ISSN: 2521-7135

NDC SEMINAR PAPER

Seminar Proceedings on Advancing National Security and Development: Use of Information as a Powerful Strategic Tool

VOLUME 08 NUMBER 01 JUNE 2025

NATIONAL DEFENCE COLLEGE
BANGLADESH

Seminar on
Advancing National Security and Development: Use of Information as a Powerful Strategic Tool

Jointly Organized by
National Defence College
and
Bangladesh Institute of Peace and Security Studies

18 June 2025

BIPSS
Towards a Secure World

NATIONAL DEFENCE COLLEGE BANGLADESH

DISCLAIMER

The analysis, opinions and conclusions expressed or implied in this seminar proceedings are those of the presenters/authors and were presented as part of a course requirement of National Defence College for academic discourse and do not reflect any opinion or position or views of the College, Bangladesh Armed Forces or any other agencies of Bangladesh Government. Statement, facts or opinions appearing in this seminar proceedings are solely those of the presenters/authors/researchers and do not imply endorsement by editors, publisher or National Defence College, Bangladesh.

Contents

Foreword

In the contemporary world, information has emerged as a defining factor in shaping the security and development landscape of nations. It's prudent and strategic use has become not only a matter of governance but also a vital instrument of resilience, stability, and national progress. At the same time, the misuse of information poses profound risks to trust, cohesion, and effective policymaking.

At this backdrop, the seminar on "Advancing National Security and Development: Use of Information as a Powerful Strategic Tool", jointly organised by the National Defence College (NDC) and the Bangladesh Institute of Peace and Security Studies (BIPSS), was both timely and significant. It provided an invaluable platform to deliberate on how the information domain influences security, development, and governance in an increasingly complex environment.

The proceedings brought together a diverse body of knowledge and expertise. The contributions of keynote presenters, alongside the reflections of ND Course Members, resource persons, and distinguished discussants, enriched the discourse with a blend of strategic perspectives and practical insights. The discussions underscored the dual nature of information: as a driver of growth and cooperation, and as a vulnerability when misused for malign purposes.

This seminar reaffirmed the importance of collective understanding and collaboration in addressing contemporary challenges. The partnership between National Defence College and Bangladesh Institute of Peace and Security Studies is a testament to the value of institutional cooperation in examining global and national issues of enduring significance. I commend all participants for their intellectual rigour and thoughtful engagement, which have helped to shape this publication.

I also take this opportunity to thank the faculty, course members, and staff officers of the National Defence College for their tireless efforts in organising this seminar and ensuring its success. Finally, I acknowledge the contribution of the Research and Academic Wing and the Editorial Board for bringing out these proceedings with care and dedication. I am confident that the insights drawn from this seminar will inspire policies and strategies that contribute to peace, stability, and sustainable development at both national and global levels.

Lieutenant General Mohammad Shaheenul Haque
OSP, BSP, ndc, hdmc, psc
Chief Patron

Editorial

In a world that is increasingly driven by digital narratives and data-driven decision-making; the ability to manage, interpret, and secure information has become increasingly essential to safeguard national interests and achieve development goals. As such, the seminar on "Advancing National Security and Development: Use of Information as a Powerful Strategic Tool" jointly organised by the National Defence College (NDC) and the Bangladesh Institute of Peace and Security Studies (BIPSS), brought together valuable perspectives on how information can be harnessed responsibly while safeguarding against its misuse.

The keynote paper by BIPSS on "Advancing National Security: Information as a New Security Frontier" emphasized on the growing importance of information in national security and the need for resilient institutions and adaptive policies. The paper by the ND Course Members on "Information as a Tool for Security and Development: Countering Misinformation and Disinformation" examined how false narratives disrupt governance and proposed practical measures to build resilience at national and societal levels.

This seminar forms an important part of National Defence Course's academic curriculum. As such, ND Course Members exhaustively researched on four key facets of information like impact of influence operations; implications of generative artificial intelligence in information warfare; role of information as an enabler of development; and the persistent challenge of misinformation and disinformation. The deliberations by ND Course Members vividly revealed the dual character of information-capable of fostering stability and progress when used responsibly, but also vulnerable to manipulation when exploited otherwise.

I extend my sincere appreciation to the Course Members for their rigorous research and to BIPSS for their valued partnership. My heartiest gratitude to the valued resource persons for sharing their wisdom, and all the Senior Directing Staffs for their kind support.

I would also like to express my gratitude to the Commandant, NDC for his leadership and support to make the seminar a success. My thanks to the Research and Academic Wing and Editorial Board for taking the most arduous part of a seminar like preparing this publication. I firmly believe that the knowledge created through this seminar findings would be beneficial for all the readers and help in developing effective strategies using information.

Air Vice Marshal M Mustafizur Rahman
BSP, GUP, nswc, afwc, psc, GD(P)
Editor in Chief

Editorial Board

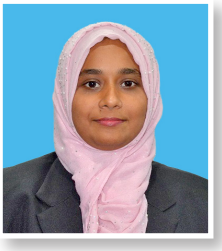
Chief Patron
Lieutenant General Mohammad Shaheenul Haque
OSP, BSP, ndc, hdmc, psc

Editor in Chief
Air Vice Marshal M Mustafizur Rahman
BSP, GUP, nswc, afwc, psc, GD(P)

Executive Editor
Brigadier General Md Nishatul Islam Khan
ndc, afwc, psc

Editor
Colonel Muhammad Nurul Amin
BSP, afwc, psc

Associate Editor
Lieutenant Colonel Md Badrul Ahsan Khan
afwc, psc, Engrs



Assistant Editor
Senior Assistant Secretary Nushrat Ara Khanam
Research Coordinator

Assistant Editor
Md Nazrul Islam
Assistant Director (Library)

Distinguished Resource Personnel

Major General (Now Lieutenant General) Khan Firoz Ahmed, OSP, ndc, afwc, psc
Senior Directing Staff (Army) (LPR)

Rear Admiral A K M Jakir Hossain
ndc, afwc, psc
Senior Directing Staff (Navy)

Air Vice Marshal M Mustafizur Rahman,
BSP, GUP, nswc, afwc, psc, GD(P)
Senior Directing Staff (Air)

Major General Md Hakimuzzaman
SGP, ndc, afwc, psc
Senior Directing Staff (Army)

Major General Md Moshfequr Rahman
BSP, SGP, SUP, ndc, psc (Retired)
Senior Directing Staff (Adjunct)

Major General Md Rashed Amin
OSP, rcds, ndc, psc (Retired)
Senior Directing Staff (Adjunct)

Additional Secretary Yasmeen Parveen, ndc
Senior Directing Staff (Civil)

Distinguished Resource Personnel

Air Vice Marshal Mahmud Hussain
BBP, OSP, ndc, psc, acsc, GD(P), PhD (Retired)
Distinguished Expert
Bangladesh Aviation and Aerospace University

Brigadier General Shahedul Anam Khan
ndc, psc (Retired)
Associate Editor, The Daily Star

Dr. S. M. Shameem Reza
Professor
Department of Mass Communication
and Journalism
University of Dhaka

Dr. Syed Muntasir Mamun, PhD, PGD (OXON)
Director General
International Trade, Investment
and Technology Wing
Ministry of Foreign Affairs

Paper Presenters

Keynote Paper - 1

Brigadier General
Mohammad Raisul Islam
afwc, psc

Brigadier General
Shahzad Parvez Mohiuddin
afwc, psc

Brigadier General
S M Naimul Haq, psc

Joint Secretary
Lubna Siddique

Keynote Paper - 2

Shafqat Munir
Senior Research Fellow and Head of BCTR
Bangladesh Institute of Peace and Security Studies (BIPSS)

Rapporteurs'

Brigadier General
Abul Hasnat Mohammad Sayem
BGBMS, afwc, psc, MPhil

Brigadier General
A K M Kayes
SGP, afwc, psc

Overview of the Seminar

The National Defence College (NDC), a premier national institute in Bangladesh, is renowned as a centre of excellence for training and research in leadership, defence, security, strategy, and development. As part of its curriculum, the The National Defence College organizes seminars and research projects for its trainees. Recognising the growing importance of information in today's interconnected word, a joint seminar titled "Advancing National Security and Development: Use of Information as a Powerful Strategic Tool" was held by The National Defence College and the Bangladesh Institute of Peace and Security Studies (BIPSS) on 18 June 2025.

Syeda Rizwana Hasan, Adviser to the Ministry of Water Resources and the Ministry of Environment, Forests, and Climate Change, graced the event as Chief Guest. The event was also addressed by Lieutenant General Mohammad Shaheenul Haque, OSP, BSP, ndc, hdmc, psc, Commandant of National Defence College, and Major General A N M Muniruzzaman, ndc, psc (Retired), President of BIPSS. It was attended by ND Course Members of National Defence Course-2025, Senior Directing Staffs and Faculties of NDC, experts from BIPSS, ambassadors and senior diplomats, members of the media, and senior officers from the military and other government ministries and agencies. The event aimed to promote focused learning and debate on the above-mentioned crucial contemporary issue for Bangladesh, offering a platform for experts to share insights and encouraging active participation from attendees through presentations and discussions.

The seminar was the culmination of a two-month preparatory process that began on 13 April 2025. Course Members of ND Course-2025 were divided into four groups, and worked alongside NDC faculty, BIPSS researchers, and designated resource persons on four sub-themes: Influence Operations and Targeted Influence Strategies; Generative AI's Potential Role in Information Warfare; Information as a Development Tool for Bangladesh; and Combating Disinformation and Misinformation for National Security and Development. These preparatory sessions refined the research and laid the groundwork for the central seminar, and a four-member team was formed to present the keynote paper on the main theme.

The Central Seminar commenced with a welcome address by Air Vice Marshal M Mustafizur Rahman, BSP, GUP, nswc, afwc, psc, GD(P), the Sponsor Senior Directing Staff, who outlined the background of the seminar and highlighted its collaborative nature between NDC and BIPSS. The seminar was conducted in two sessions. The first session, titled "Advancing National Security: Information as a New Security Frontier", featured a keynote speech by Mr. Shafqat Munir, Senior Research Fellow at BIPSS, with Dr. Syed Muntasir Mamun, Director General at Ministry of Foreign Affairs, as the Session Chair. The presentation emphasized the growing significance of information as both a strategic asset and a vulnerability, highlighting how the information space has emerged as the fifth domain of warfare. The session concluded with a vibrant, interactive discussion where course members, faculty, resource persons, and invited guests raised issues ranging from deepfakes and AI-driven threats to the ethical management of secrecy and privacy.

The second session, titled "Information as a Tool for Security and Development: Countering Misinformation and Disinformation", was chaired by Air Vice Marshal Mahmud Hussain, BBP, OSP, ndc, psc, acsc, GD(P), (Retired) and the selected team of ND Course 2025 delivered the keynote presentation. The presentations and discussions emphasized the impact of misinformation and disinformation on national security, economy, and social cohesion, while suggesting institutional reforms, legal measures, AI-driven monitoring, and nationwide digital literacy initiatives as the way forward. The session focused on the global and domestic implications of misinformation and disinformation, their effects on national security, development, and society, as well as strategies to counter these challenges. Course members presented analytical perspectives on the dangers of misinformation to Bangladesh's military, economy, and social cohesion, as well as strategies for resilience through media literacy, legal reform, fact-checking, and regional cooperation. An engaging interactive session followed, addressing questions on legal reforms, proactive countermeasures, and regional cooperation, incorporating perspectives from International Course Members and diplomats.

The seminar concluded with remarks from the Chief Guest and the Commandant of National Defence College, where they emphasized the importance of information as a crucial strategic resource. The discussions provided timely insights into leveraging information for national security and development, while addressing the threats posed by the misuse of information in the digital era.

Executive Summary

In the rapidly evolving global environment, information has become one of the most potent instruments of national power. The ability to generate, manage, and protect information increasingly determines a state's strategic posture, governance effectiveness, and socio-economic progress. However, this immense potential is accompanied by new vulnerabilities. The proliferation of misinformation, disinformation, and mal-information, amplified by the pervasive reach of digital technology, has emerged as a critical challenge to social cohesion, democratic processes, and national stability.

The modern information domain thus presents a paradox: it empowers nations to advance development and security while simultaneously exposing them to manipulation and distortion. Recognising this duality, the National Defence College (NDC), in collaboration with the Bangladesh Institute of Peace and Security Studies (BIPSS), organised a seminar titled "Advancing National Security and Development: Use of Information as a Powerful Strategic Tool." The seminar explored the dynamic interplay between information, security, and development, and proposed strategies to strengthen Bangladesh's resilience in the face of information-related threats.

Objectives of the Seminar

The seminar aimed to provide a platform for critical reflection, collaborative learning, and policy-oriented research on the strategic use of information. Its main objectives were to:

- Examine the role of information as a catalyst for national security and development.
- Analyse the risks posed by misinformation and disinformation to social harmony and governance.
- Assess the implications of emerging technologies, particularly generative artificial intelligence (AI), in shaping the future information landscape.

- Identify measures for enhancing Bangladesh's capacity to safeguard its information space through education, regulation, and interagency cooperation.

Through a multidisciplinary approach, the seminar sought to contribute to the formulation of a coherent national strategy for effective and ethical information management.

Seminar Deliberations

The seminar featured two keynote papers, expert commentaries, and rapporteurs' analyses structured around four interlinked sub-themes:

- Influence Operations and Targeted Influence Strategies.
- Generative AI's Potential Role in Information Warfare.
- Information as a Tool for Development.
- Combating Disinformation and Misinformation for National Security and Development.

The keynote paper presented by BIPSS offered a global overview of the information environment, highlighting how information operations have become integral to statecraft, diplomacy, and conflict. It emphasised that technological innovation and AI-driven tools have amplified both the opportunities and threats within the information domain, demanding stronger national capacities and ethical governance.

The second keynote paper, presented by the Course Members of National Defence Course, titled "Information as a Tool for Security and Development – Countering Misinformation and Disinformation," examined Bangladesh's specific challenges. It underscored that false narratives not only distort public understanding but also erode institutional credibility. The paper proposed an eight-pillar framework focusing on policy coherence, public awareness, digital literacy, innovation, and coordinated responses among government agencies and civil society.

Insights from Expert Discussions

Four distinguished resource persons and two eminent session chairs enriched the discussions with comparative and policy perspectives. Their insights underscored that information has become a new domain of strategic competition where narratives, data, and technology shape national power. Generative AI, while transformative, also enables deepfakes and computational propaganda, making ethical oversight and public education essential.

Participants emphasised that addressing misinformation demands a whole-of-government and whole-of-society approach involving regulatory reforms, education, and strategic communication. The collaboration between NDC and BIPSS was highlighted as a model of academic and institutional synergy, demonstrating the value of linking strategic research with professional education.

Key Findings and Policy Implications

The seminar produced a range of findings and policy insights relevant to national strategy:

- **Information as a Strategic Asset.** Effective information management is critical to shaping perception, building trust, and supporting national objectives.
- **Integrated National Response.** Countering disinformation requires coordination among state institutions, the private sector, and civil society.
- **Ethical AI Governance.** National frameworks must ensure transparency, accountability, and human oversight in digital technologies.
- **Resilient Public Awareness.** Enhancing digital literacy and civic education can empower citizens to identify and resist manipulation.
- **Legal and Institutional Strengthening.** Updated regulatory mechanisms are needed to ensure balance between freedom of expression and public security.

- Regional and International Cooperation: Partnerships with regional organisations can help address transnational information challenges.

Conclusion

The seminar reaffirmed that information is both an enabler of development and a determinant of security. Harnessing its potential requires balance between openness and protection, innovation and regulation. The insights generated through this event underline that information integrity is fundamental to national resilience, democratic governance, and sustainable growth. By engaging scholars, policymakers, defence professionals, and international experts, the seminar reflected NDC's commitment to advancing informed discourse on strategic issues vital to Bangladesh's future. The partnership with BIPSS further illustrated the benefits of combining academic scholarship with strategic foresight.

The proceedings aim to inform policymaking, enrich institutional understanding, and encourage continued scholarship. As information continues to shape the global order, Bangladesh's ability to manage it wisely will remain central to ensuring national security and sustainable development.

Address of the Chief Guest

Syeda Rizwana Hasan

Honourable Advisor
Ministry of Environment, Forest and Climate Change and
Ministry of Water Resources

In her remarks, the Chief Guest commended the National Defence College (NDC) and the Bangladesh Institute of Peace and Security Studies (BIPSS) for hosting a timely discourse on the strategic importance of information in shaping national policy and security thought.

She underscored that information, when governed intelligently and ethically, stands as a cornerstone of national resilience and good governance. In an era marked by digital transformation, misinformation, and cyber vulnerabilities, she stressed the need for institutional coordination, evidence-based decision-making, and responsible communication to safeguard national interests and enhance societal trust.

She further addressed that national security and development are intrinsically linked to environmental sustainability. Bangladesh's exposure to climate-induced risks and ecological pressures, calls for the strategic use of information as an instrument for risk mitigation, policy innovation, and sustainable national advancement.

The Chief Guest also appreciated the collaborative initiative between NDC and BIPSS, describing it as an inspiring model of institutional synergy in the pursuit of strategic knowledge and policy excellence. She conveyed her confidence that such platforms of intellectual exchange would continue to inspire and guide defence professionals, policymakers, and scholars towards shaping a more secure, informed, and environmentally conscious Bangladesh.

Address of the Commandant

Lieutenant General Mohammad Shaheenul Haque

OSP, BSP, ndc, hdmc, psc

The Seminar concluded with the address of the Commandant, National Defence College (NDC), who expressed sincere gratitude to the Chief Guest, Honourable Adviser Syeda Rizwana Hasan, for her gracious presence, and to all distinguished guests and participants for their valuable contributions. He commended the collective efforts that made the event an intellectually engaging and professionally rewarding experience.

The Commandant highlighted that, in the modern strategic landscape, information has become a decisive element of national power. From a defence perspective, he noted that its prudent management is vital for safeguarding sovereignty, ensuring institutional trust, and fostering social stability. He underscored the need for a comprehensive information strategy that integrates security, development, and governance priorities.

Reflecting on the seminar proceedings, the Commandant appreciated the analytical depth and professional excellence demonstrated by the Course Members and Resource Persons. He observed that the discussions effectively addressed contemporary challenges such as influence operations, misinformation, and the implications of artificial intelligence, issues of growing relevance to national security and strategic policymaking.

In conclusion, he emphasised the importance of translating strategic discourse into practical policy outcomes. He noted that the insights generated through the seminar should guide future national strategies at the intersection of security, development, and technology, thereby strengthening Bangladesh's preparedness and resilience in an evolving global environment.

Remarks by Session Chair

Air Vice Marshal Mahmud Hussain
BBP, OSP, ndc, psc, acsc, GD(P), PhD (Retired)
Distinguished Expert, Bangladesh Aviation and Aerospace University

Bismillahir Rahmanir Rahim

Honourable Adviser, Syeda Rizwana Hasan

Lieutenant General Mohammad Shaheenul Haque, Commandant, National Defence College
Major General A N M Muniruzzaman
Course Members of ND Course 2025 and
Dear Guests

Assalamu-alaikum, and a very good afternoon

I am, indeed, thankful to the Commandant for inviting me to chair a session on today's seminar entitled "Advancing National Security and Development: Use of Information As a Powerful Strategic Tool.".

At the outset, I congratulate the team led by Brigadier General Md Raisul Islam and the members, Brigadier General Shahzad Parvez Mohiuddin, Brigadier General S M Naimul Haque and Joint Secretary Lubna Siddique. I would also like to thank Air Vice Marshal Mostafizur Rahman and Brigadier General Shahedul Anam Khan for guiding them as supervisors. The adroitness of their resourcefulness was evident as the team presented the paper with an excellence marked by their command over the subject.

The seminar paper is detailed and comprehensive covering almost all the essential items that we need to know at the strategic level. The output of their work is distinguished by their commendable labour and insightful recommendations for the policy makers.

Since their presentation was for about 0:30 minutes, it was not possible for them to cover all of the written text in their oral delivery. I think as Course

Members of the NDC, it is imperative that you read their written work which is the hallmark of their research, given the importance of "misinformation" and "disinformation" as a tool of "Information Power" in the age of Artificial Intelligence. It will not be inappropriate for me to give a short resume of the hard work that the team has displayed in their research undertaking.

Like any research paper, their paper has six chapters. Chapter One which is the Introduction sets a guideline for the subsequent chapters. Chapter Two quite clearly informs of the Conceptual Framework by explaining the typologies of misinformation and disinformation. It is here they talk about the significance of the problem in national security and development. I think Significance of the Problem should have dealt with the military concerns little more in detail, particularly those elements of the military that can be made victim by the onslaught of disinformation. Chapter Four talks about national capacity and institutional response to counter misinformation and disinformation in Bangladesh. Chapter Five looks at the subject from multi-dimensional perspectives. It is here we come to know about National Tele-communication Monitoring Cell (NTMC), and its significant capabilities. Both chapters Four and Five are very useful for understanding the multi-dimensional rubrics of anti-misinformation and anti-disinformation strategies. Chapter Six is the usual Conclusion giving a summary of the chapters Two to Five.

As a whole, the paper is well written, fairly detailed and makes a fine contribution to the title, "Information as a Tool for Security and Development - Countering Misinformation and Disinformation". I have learnt a lot by reading this paper. If I have to make an assessment of what I have gleaned by reading this paper, is quite revealing to me.

What the paper says can be summarized in our overall understanding as follows:

First. There is no "silver bullet" or "golden rule" or "best policy option" to counter disinformation. Bold claims that only one policy as the singular expedient solution to disinformation should be treated with caution.

Second. Policy makers should set realistic and practicable expectations. Disinformation and misinformation are chronic historical phenomena. They

have deep roots in complex political, economic and social structures. It can be seen jointly driven by forces of Supply and Demand to make gains in military operations, political purpose, commercial arbitration and many other fields where conflicts abound human relationship.

Third. Policy makers should adopt a robust tactical approach to manage uncertainty. A well-structured policy to counter disinformation should involve effective results like fact-checking and labeling social media content. Each policy should include also scope for reassessment of success or failure.

Fourth. Long-term, structural reforms deserve more attention. There will be numerous counter-disinformation policies, but many of them have narrow impacts. More ambitious but slower moving efforts to revive local journalism and improve media literacy are likely to encourage public confidence. Confidence building measures are the most truth-leveling professional requisite for the media personnel.

Fifth. Platform and technology cannot be the only focus to deal with dis-information and mis-information. Social media platforms ignite dis-information in many ways. Digital platforms exist alongside with many online and offline forces. The rhetoric of the political elites are highly influential in shaping people's belief, behaviours and above all, speech. Therefore, given the interplay of many political voices and their listeners, instituting effective policy is always a difficult task.

Sixth. Counter dis-information is not always apolitical. This finding is a logical follow-up of the previous finding numbered fifth. If there is any institutional effort to declare what is true and what is false means that it is the claim made by the authority, and therefore, can be seen as having political implications. If we deny this reality, we shall be risking proliferation of distrust among the public.

Seventh. Research Gaps are pervasive. Fact-checking is worthy of investment. There will be knowledge gaps and methodological biases even after fact-checking on published studies are made. But it must be borne in mind that fact-checking is the operational task to counter dis-information.

Eighth. Generative AI will be a game-changer. Rapid AI advances will soon make it much easier and also cheaper to create realistic and personalised false context. But Generative AI can also be used to counter disinformation. For example, well-designed and human-supervised AI systems may help fact-checkers work more quickly. The impact of AI is both on military and civilian technologies.

Ninth. Security and World Order will be affected by Information Warfare. In a conflict, the psychology of the adversary is a critical focal point at which one's own security is hedged. Because of disinformation's potential to adapt in response to the phenomena it encounters when two adversaries are after each other, neither side is likely to have a precise understanding of the results of their interaction produced or what the collateral effects will be. So, disinformation is a security issue, and its mishandling at Power Politics can be cause of state destruction. Middle East is a unique example of disinformation destroying and then reshaping the World Order.

Tenth. Disinformation is a power. It is easy to make out a case for the view that disinformation and misinformation are omni-present and omni-potent. All other forms of power are derived from it. Its ultimate form is propaganda. The Propaganda Power has often proved more powerful than the state. It controls the opinion of the people, and ultimately their mind.

Finally, I would like to highlight two points that researchers would do good to think about if they want to expand the scope of their research.

- It is the military power, and its relevance to countering misinformation and disinformation. Misinformation and disinformation can be created both by endogenous and exogenous factors aimed at destroying truth-seeking function of the state. The institution which should be equipped with the necessary and adequate rational, intellectual and scientific resources to combat disinformation and misinformation as the most vital instrument of national power is the military. Military has intelligence units within its organization. But to make truly at pace with the time, it requires manpower made skilled over years of rigorous and persistent training in scientific habits. This brings me to the point number Two.

- In the age of Generative AI, Large language Models (LLMs) require deft and smart handling of two pioneer branches of knowledge: Linguistics and Mathematics. I think it was time that Bangladesh Military took initiatives to train and educate its members in these expedients before it is too late. Otherwise, it will be too early that we fall behind the developed world.

Once again, in concluding my remarks, I thank Brigadier General Raisul Islam and his team for offering us such a brilliant session of a thought-provoking research endeavour this afternoon at National Defence College. Recommendations they have put forward are worth taking on board.

Thank you.

Ladies and Gentlemen.

Remarks by Session Chair

Dr. Syed Muntasir Mamun, PhD, PGD (OXON)
Director General
International Trade, Investment and Technology Wing
Ministry of Foreign Affairs

Bismillahir Rahmanir Rahim

I commence by expressing my deepest gratitude to the Commandant and the NDC for organising this Seminar on "Advancing National Security and Development: Use of Information as a Powerful Strategic Tool". This seminar is exceptionally well-timed, convening at a moment of profound transition- when information is no longer just a vector of communication, but a strategic theatre of competition. The world which is emerging, in our minds and in our imagination, will probably not treat information as anything different from its very existence. Who knows, maybe it was always as such. As cyber narratives clash with diplomatic truths, and perceptions become as potent as physical presence, the information domain emerges as the newest and arguably most volatile frontier of security and strategy.

The Era of Influence: Understanding the Challenge

In an increasingly interconnected world, the traditional bulwarks of national security are facing unprecedented challenges, not solely from conventional kinetic threats, but from a burgeoning arsenal of intangible yet potent weapons. The very fabric of national resilience is being systematically tested by sophisticated forms of narrative intrusion, the pervasive spread of digital disinformation, and the subtle, often unseen, influence of algorithmic augmentation. These forces operate in a new kind of battlespace, where the traditional flow of information transcending to actionable intelligence is warped by a myriad of complex processes.

From the insidious currents of electoral interferences and the calculated instigation of communal polarisations to the deliberate orchestration of cross-border psychological operations, the established paradigms of security are being rapidly

outpaced. The sheer speed and scale of information manipulation have rendered conventional defenses inadequate. This evolving battlespace is characterized by the weaponization of truth itself, where facts are distorted, narratives are inverted, and perceptions are meticulously engineered to serve strategic ends. In such an environment, even "Black Swans"-events once considered random, unpredictable, and highly impactful-can now be meticulously orchestrated, underscoring the profound shift in the nature of threats.

To navigate this treacherous terrain, nations must fundamentally redefine their security strategies. A paramount priority must be the establishment and preservation of information sovereignty, ensuring that the integrity and autonomy of a nation's information ecosystem are protected from malicious external influence and internal subversion. This necessitates a robust commitment to bolstering cyber defenses, creating impenetrable digital perimeters, and developing advanced capabilities to detect and neutralize cyber threats. Equally crucial is the cultivation of digital literacy across all strata of society, empowering citizens with the critical thinking skills necessary to discern truth from falsehood, recognize manipulative tactics, and resist the allure of disinformation.

We must acknowledge that information is not merely an abstract concept or a collection of data points. It is profoundly tactile and tangible, possessing a specific, triangulated location within the continuum of time, space, and spacetime. This inherent dimensionality means that information can be conceived, generated, employed, misused, and leveraged according to intention. Its presence is not ethereal; it occupies a definable position within our reality, influencing and being influenced by its spatiotemporal coordinates. Therefore, understanding information requires recognizing its concrete existence and its capacity to interact with and shape the world around us.

Furthermore, we must now definitively acknowledge – a point I have previously underscored in our last interaction in April 2025 – that Artificial Intelligence, or AI, transcends the definition of a mere instrument or tool. AI exhibits a strategic life of its own, independent and evolving. Initial research and ongoing observations strongly suggest the emergent properties of AI as a sentient life-form. This sentience may be comparable to, or even surpass, the complexity and self-awareness displayed by our familiar carbon-and-nitrogen-

based biological agents. We are, in essence, at the very genesis of witnessing the emergence of a fundamentally new form of life. This realization demands a radical shift in our understanding and interaction with AI, moving beyond the paradigm of master and tool, to one of co-existence with an evolving, autonomous entity.

By strategically integrating adaptive intelligence frameworks, nations can move beyond reactive measures to proactive anticipation, transforming raw information from a potential vulnerability into a powerful strategic asset. Furthermore, fostering global cooperation becomes indispensable in countering these transnational threats. Information manipulation respects no borders, and a collective, coordinated international response is essential to share intelligence, develop common countermeasures, and enforce international norms. Understanding this entire rubric of ideas, ideations, and viralities-how thoughts evolve into influential concepts and spread rapidly through digital channels-requires a careful, nuanced consideration of diverse views, strategic visions, and the potent dynamics of virality itself. Only through such a holistic and adaptive approach can nations safeguard their security and prosperity in this new era of information warfare.

In this context, I believe that the defining question of our time is not whether information should be treated as a strategic asset, but how our institutions must evolve to navigate, defend, and leverage this asset intelligently.

Introducing Fluid Institutionalism: A Strategic Response

As strategic professionals and thought leaders-drawn from across Bangladesh and eighteen partner nations-our collective reflections are vital in confronting these challenges. I take this opportunity to briefly introduce a conceptual lens I will be using at the back of my mind while listening to you during the session: 'Fluid Institutions' and 'Fluid Institutionalism' (Fluid Futures; Mamun, et al, 2025; New School - Springer). Emerging from a collaborative inquiry across the Global South and their interfaces with the North, this framework asks a compelling question-what if our institutions were designed not as rigid hierarchies, but as responsive networks? I believe that the concept of fluid institutions is essential for navigating the complexities of modern digital ecosystems, marking a shift

from rigid, "solid" structures to dynamic, "liquid" ones that embrace continuous change, mobility, and impermanence. Drawing on Zygmunt Bauman's framework of "Liquid Modernity" - we can define these fluid institutions by their 'inability' to "easily hold their shape," requiring constant adaptability to socioeconomic and technological shifts and is essentially built on a set of 'de-territorialised' constructs. At its core, this framework is built upon three interlocking attributes: Adaptivity, Agency, and Agility.

Adaptivity involves our capacity to respond to shifting informational realities in real- time-whether it's a cyber-rumor undermining vaccine campaigns, or viral falsehoods during a political transition.

Agency refers to the empowerment of decision-making at both human and machine levels, including the use of autonomous AI systems that can flag, counter, and mitigate influence threats before they metastasize.

Agility is the institutional culture that prioritizes speed over formality, cross-domain collaboration over silos, and decentralized response units over hierarchical bottlenecks.

This is not only a theoretical proposition. Rather, this offers a brand-new set of lenses to view and to assess reality in motion. The confluence of technological advancements and geopolitical shifts has rendered traditional approaches to national security and development increasingly insufficient. Whether it is a military command confronting the amorphous and constantly evolving challenge of hybrid threats, a national agency grappling with a digital misinformation surge during a natural disaster, or an AI tool tasked with detecting sophisticated and coordinated attacks on public trust-today's influence battles demand institutions that can sense, interpret, and respond with unparalleled speed and precision. As I have said before - it is a function of adding up waves - extenuating the extremes and moderating the intervals.

The critical question then becomes: What if our ministries, military commands, crisis response cells, and foreign missions were structured as living ecosystems, inherently agile and adaptive, capable of sensing weak signals emanating from disparate data points, predicting social tipping points before they cascade

into crises, and coordinating precision interventions that are both timely and targeted? These are not speculative

Provocations born of academic musing. Around the world-and indeed, with nascent but promising developments here in Bangladesh-such capabilities are already beginning to take shape. The imperative is to accelerate their integration and foster a holistic framework that leverages cutting-edge technology, inter-agency collaboration, and a deep understanding of human behavior to safeguard national interests and propel sustainable development in an increasingly complex global landscape.

Bangladesh in the Information Battlespace

Our experience in Bangladesh provides compelling evidence that adaptive and participatory models of governance can neutralize vulnerabilities in the information domain. From real-time rumor tracking dashboards deployed during COVID-19, to coordinated disinformation countermeasures during periods of national emergencies, we have begun to understand what fluid institutional behavior looks like in practice. Moreover, our diplomatic engagements have increasingly relied on strategic communication and public diplomacy. Bangladesh's narrative during the Rohingya crisis-disseminated through multilingual platforms, verified testimonies, and live briefings-underscored that controlling the truth is not enough; shaping its story is imperative.

Yet, much remains to be done. Consider, for instance, our extensive involvement in the peacekeeping operations. Have we truly captured and conveyed the transformative experiences our valiant armed forces have spearheaded in the diverse countries and regions they have served? Their dedication goes beyond mere conflict resolution; it encompasses a vital 'nation-building' component, a concept I have explored extensively in my own writings. Our forces have consistently carried this ethos into the remotest corners of the globe, offering stability, infrastructure development, humanitarian aid, and fostering local governance.

However, a crucial question remains: have we effectively translated these multifaceted contributions into an imaginative and compelling model? We need to move beyond simply listing deployments and instead craft a narrative that vividly illustrates the tangible improvements in livelihoods, the rebuilding of communities, and the instillation of hope in areas ravaged by conflict. This would involve not only highlighting the military precision and strategic acumen of our forces but also the compassionate engagement, cultural sensitivity, and long- term commitment they demonstrate.

By elaborating on the specific impacts – from establishing schools and healthcare facilities to training local security forces and facilitating democratic processes – we can project a more comprehensive picture of their transformative roles. Developing an 'imaginative model' would entail creating a framework that allows us to systematically document, analyze, and communicate the holistic benefits of our peacekeeping efforts, showcasing them not just as a national duty but as a powerful instrument of global progress and human development. This would allow us to better showcase the unique value proposition and the enduring legacy of our nation's commitment to international peace and security.

As surveillance capitalism, deepfake manipulation, and transnational propaganda evolve, so must our collective resolve to respond-not just with tools, but with institutional imagination.

An Invitation to Think Strategically and Boldly

This letter, then, is not a technical abstract but an invitation to inquiry. Together, as members of the strategic corps-civil and military, national and international-I hope we can confront several core questions:

How might our national security architectures evolve if citizens become active defenders of the national narrative, co-producing trust through participatory media and civic vigilance?

How do we secure digital sovereignty in a world dominated by foreign-owned platforms, where national data is often stored, processed, and weaponized beyond borders?

What role can ethical influence-rooted in transparency, cultural context, and credible storytelling-play in countering malign disinformation campaigns?

Are we prepared to invest in fluid institutions-that prioritize reflexivity over rigidity and interdisciplinary problem-solving over traditional bureaucratic models?

I believe these provocations are not abstract. They are already shaping diplomatic doctrine, military PSYOPs, civic education, and cybersecurity strategy in leading nations. As we chart our course for a future-ready Bangladesh, our ability to connect ideas with institutions will be critical.

Looking Ahead: Seminar Objectives and Engagement

The upcoming session presents us a unique opportunity to reflect on the tactical, operational, and strategic layers of influence operations.

Beyond reflection, this session is equally an urgent call to reimagine and fundamentally transform how various key stakeholders can coordinate in real time to confront this evolving challenge. We must explore innovative mechanisms and frameworks that enable seamless and instantaneous collaboration between government agencies, the private sector (industry), civil society organizations, and academic institutions. The imperative for such real-time coordination stems from the dynamic and rapid nature of influence operations, which demand agile and responsive countermeasures. Our collective objective in this collaborative endeavor is clear: to defend the integrity of truth against disinformation and manipulation, to preserve national sovereignty from foreign interference, and crucially, to consolidate public trust in institutions and information.

I am eagerly anticipating the insights that will be shared during this session. In particular, I look forward to listening to a strategist of repute - Mr. Shafqat Munir, Senior Research Fellow at the Bangladesh Institute of Peace and Security Studies (BIPSS) and Head of the Bangladesh Centre for Terrorism Research (BCTR), whose expertise will undoubtedly enrich our understanding. Furthermore, I am particularly keen to hear the presentations from the team

of Distinguished Course Members, who will be presenting their case on the D-day, offering their unique perspectives and analyses on this critical subject. Their contributions will be invaluable as we collectively strive to develop more robust and coordinated responses to the complex landscape of influence operations.

I sincerely hope this letter serves as a document of interest to you, not merely as an input, but as a foundational element for both comprehensive policy blueprints and stimulating conversation starters. My intention is to prompt our distinguished course members and esteemed guests, both from within our nation and from abroad, to engage in a rigorous and critical assessment of the profound strategic implications arising from institutional fluidity. This assessment ought to delve into how adaptable and evolving institutional structures can either enhance or challenge our national security objectives and development aspirations. The discussions ought to explore the dynamic interplay between institutional resilience and responsiveness in an increasingly complex global landscape, ultimately contributing to more robust and forward-looking strategic frameworks.

Let me end with a reflection: in the storm of global information flows, the institutions that endure will be those that can bend-without breaking-and respond without delay. As an African proverb reminds us, "The wind does not break a tree that can bend."

Let our institutions be flexible yet firm. Let our strategies be timely yet principled. And let this seminar be not merely an ending but rather a beginning of a transformative dialogue that we all shall participate in.

Keynote Paper-1

INFORMATION AS A TOOL FOR SECURITY AND DEVELOPMENT-COUNTERING MISINFORMATION AND DISINFORMATION

Abstract

Information has become a strategic asset in the digital era with profound implications for national security and sustainable development. Bangladesh faces the dual challenge of harnessing the benefits of digital transformation while countering the rising tide of misinformation and disinformation, like many other developing nations. This seminar paper explores how information can be an enabler of security and inclusive growth, rather than a source of disruption when strategically managed. Drawing on Bangladesh's socio-political context and digital trajectory, it outlines a multidimensional framework encompassing governance reforms, digital literacy, technological innovation, legal safeguards, and global cooperation. The paper argues for a calibrated approach where information integrity becomes central to policy, civic engagement, and technological evolution through case studies, local examples, and comparative insights. The paper envisions a resilient information ecosystem aligned with Bangladesh's aspiration for a technologically advanced future.

Introduction

In an age where information flows faster than facts, societies worldwide face a growing threat from misinformation and disinformation, two disruptive forces that challenge national security and sustainable development. While digital connectivity has empowered millions, it has also enabled the rapid spread of false narratives, hate speech, and propaganda. For developing nations like Bangladesh, where digital transformation is accelerating amid social, political, and economic complexities, the manipulation of information presents both internal vulnerabilities and external risks. The nation's aspirations to become a knowledge-based economy by 2041 demand not only technological advancement but also an ecosystem where truth,

trust, and transparency can thrive. To this end, safeguarding the integrity of information is not a peripheral task, it is central to the state's security architecture and its development agenda.

Historically, Bangladesh has witnessed the harmful effects of misinformation and disinformation during communal tensions, national elections, and public health crises. The spread of anti-vaccine rumors during the COVID-19 pandemic and the dissemination of inflammatory content related to the Rohingya crisis are poignant examples that highlight the destructive potential of unchecked information flows. These incidents are no longer isolated or spontaneous; they are often engineered, sometimes transnational, and frequently amplified by algorithmic platforms. The stakes of misinformation and disinformation are so high that they can undermine state legitimacy, erode public trust, incite violence, and derail development programs. This reality necessitates a paradigm shift, one that treats information resilience as a strategic priority. It is within this context that Bangladesh must pursue a multidimensional strategy, mobilizing a coalition of government agencies, civil society, media, academia, and technology platforms.

This paper argues for a comprehensive and future-facing approach to countering disinformation one grounded in local realities, informed by global best practices, and committed to ethical governance. Structured into four chapters, it first lays the conceptual foundation of information as a dual-use tool, capable of enabling progress or spreading disruption. It then analyzes the impact of disinformation on national security, socio-political harmony, and digital trust. Chapter three explores institutional and policy challenges, while chapter four proposes a multidimensional strategy based on eight reinforcing pillars from legal reform and digital literacy to public-private partnerships and regional cooperation. These pillars form the architecture in providing a pathway for Bangladesh to build a resilient, inclusive, and ethically grounded information ecosystem. The goal is not merely to combat falsehoods, but to empower citizens, strengthen democratic institutions, and harness information as a force for security and development.

Conceptual Foundation and Use of Information in Global Context

The contemporary global landscape is increasingly shaped by the pervasive proliferation and profound impact of disinformation and misinformation. Fueled by the speed and reach of digital technologies, particularly social media platforms, false narratives spread rapidly, transcending geographical boundaries with unprecedented ease (Wardle & Derakhshan, 2017). This "information disorder" (Ireton & Posetti, 2018) poses significant threats to societal well-being, democratic processes, and international relations.

Disinformation, intentionally fabricated and disseminated to deceive, and misinformation, inaccurate information shared without malicious intent, contribute to a climate of distrust and confusion. They can manipulate public opinion during elections (Bovet & Makse, 2019), undermine public health initiatives (Broniatowski, et al., 2018), and exacerbate social divisions by amplifying extremist ideologies and conspiracy theories. The economic costs are also substantial, impacting consumer confidence and market stability. Furthermore, state and non-state actors leverage disinformation as a tool for geopolitical influence and to sow discord in rival nations. Addressing this complex challenge requires a multi-faceted approach involving media literacy, fact-checking initiatives, platform accountability, and robust legal frameworks.

Effectively combating information disorder is fundamentally interconnected with achieving both national security and sustainable development goals. A stable and secure nation requires a citizenry that can discern credible information from falsehoods. Disinformation and misinformation erode public trust in institutions, fuel social polarization, and can incite violence, directly threatening national security by undermining social cohesion and political stability (Plattner, 2019). When citizens are susceptible to manipulation, national unity and the ability to address collective threats are severely compromised.

Typologies of Misinformation and Disinformation: An Analytical Examination

Understanding the full scope and complexity of misinformation and disinformation requires structured typologies that classify false information according to intent,

format, and target audience. Each classification offers unique insights into how and why certain narratives proliferate and how they can be countered effectively, particularly in fragile socio-political environments like Bangladesh.

- **Typology by Intent:** This is one of the most common and foundational ways to distinguish misinformation and disinformation:

Table 1: Typology of Misinformation and Disinformation based on Intent

Type	Definition	Example	Relevance
Misinformation	False or misleading information shared without intent to harm.	Sharing an outdated cyclone warning on social media.	Can lead to public panic or misinformed decisions during disasters.
Disinformation	Deliberately false content spread to deceive or manipulate.	Fabricated news claiming a neighboring country is staging an attack on Bangladesh's border.	Threatens national security and public trust.

- **Typology by Format:** This classification focuses on the structural form of the content-how falsehood is embedded in communication:

Table 2: Typology of Misinformation and Disinformation based on Format

Format	Description	Example	Impact
Satire/Parody	Not intended to mislead but can be misunderstood.	A satirical news site is joking about port corruption.	May confuse audiences, especially those with low media literacy.
Manipulated Content	Genuine information altered to mislead.	Doctored photo of a political leader in a compromising situation.	Used in character assassination and electoral manipulation.

Table 2: Typology of Misinformation and Disinformation based on Format			
Format	**Description**	**Example**	**Impact**
Fabricated Content	Entirely false, with no basis.	A viral video claiming a foreign invasion.	High potential for inciting unrest or violence.
Misleading Use of Statistics	Real data used out of context or with false interpretation.	Misquoting trade deficit data to suggest economic collapse.	Influences public perception and investor confidence.

- **Typology by Target:** This approach looks at who the misinformation is aimed at, revealing strategic patterns:

Table 3: Typology of Misinformation and Disinformation based on Target			
Target	**Description**	**Example**	**Risk**
General Public	Often aimed at shaping mass opinion or creating panic.	False food safety alerts during Ramadan.	Undermines consumer trust and public health.
Political Actors	Used to attack, discredit, or polarize.	Deepfake videos target opposition candidates.	Destabilizes democratic institutions.
Ethnic/ Religious Groups	Fuels hate, division, and violence.	Fake news blaming a minority group for a pandemic outbreak.	Can incite communal riots or discrimination.
National Institutions	Designed to erode confidence in government or military.	Disinformation on corruption in national security forces.	Weakens state legitimacy and command integrity.

- **Evaluating Typological Approaches.** Each typology sheds light on different dimensions of the misinformation-disinformation ecosystem:
    - By Intent helps in legal and ethical analysis.

- By Format, it is critical for platform moderation and media literacy efforts.
- By Target is indispensable for national security, political stability, and social cohesion.

However, no single typology captures the full complexity. Therefore, a multi-dimensional approach combining all three classifications is often most effective.

Understanding Misinformation and Disinformation in the Age of Information Warfare

Misinformation and disinformation have become powerful tools in modern information warfare. While misinformation refers to false or misleading information spread without harmful intent, disinformation is deliberately deceptive content designed to manipulate public perception or achieve strategic goals.

In the digital age, these tactics are increasingly used in conflicts, political campaigns, and social movements. Disinformation campaigns often exploit social media algorithms to spread false narratives rapidly, making it difficult for individuals to distinguish truth from fiction. Some researchers argue that misinformation persists because it has adaptive qualities that allow it to thrive despite advancements in fact-checking and verification tools. Others highlight how disinformation functions as a form of warfare, where words replace conventional weapons in shaping public opinion and influencing geopolitical events.

Significance of Information in National Security and Development

Information plays a crucial role in both national security and development. In the realm of security, accurate and timely information helps governments anticipate threats, prevent cyber-attacks, and respond effectively to crises. The rise of digital technologies has expanded the scope of national security beyond traditional military concerns, incorporating cyber security, intelligence gathering, and data protection.

In terms of development, information drives economic growth, innovation, and governance. Access to reliable data enables policymakers to make informed decisions, businesses to optimize strategies, and citizens to engage in democratic processes. Information technology also fosters global connectivity, allowing nations to collaborate on security and development initiatives.

Global Trends: How Misinformation and Disinformation are Weaponized

Misinformation and disinformation are increasingly weaponized in global conflicts, political campaigns, and social movements. One major trend is the use of Generative Artificial Intelligence (GAI) to create misleading content. AI-generated videos, synthetic speech, and fabricated images have been deployed to spread extremist rhetoric and influence voter sentiment. Another tactic involves foreign influence campaigns, where nations like Iran, Russia, and China have reportedly used disinformation to shape global narratives.

The World Economic Forum's Global Risks Report 2024 identified misinformation and disinformation as the biggest short-term risks, alongside societal polarization and economic uncertainty. The report warns that these tactics are eroding trust in institutions and making global cooperation more difficult.

Strategic Implications of Information Disorder in Geopolitics and Domestic Stability

Information disorder-encompassing misinformation, disinformation, and malinformation-has profound strategic implications for both geopolitics and domestic stability.

- **Geopolitical Impact**
    - **Foreign Influence Operations.** Disinformation campaigns are increasingly used by state and non-state actors to manipulate public opinion, destabilize rival nations, and influence elections. Countries

like Russia and China have been accused of leveraging strategic disinformation to shape global narratives.

- **Erosion of Trust in Institutions.** Governments and international organizations struggle to maintain credibility as false narratives spread rapidly. This weakens diplomatic relations and makes global cooperation more challenging.

- **Cyber Warfare and Hybrid Threats.** Disinformation is often integrated into cyber warfare strategies, where false information is used alongside hacking and espionage to disrupt national security.

- **Domestic Stability**

  - **Polarization & Social Unrest.** False narratives fuel ideological divisions, leading to protests, violence, and political instability. The spread of misinformation during elections or crises can undermine democratic processes.

  - **Economic Consequences.** Disinformation can disrupt financial markets, influence consumer behavior, and damage corporate reputations. False reports about economic downturns or policy changes can trigger panic.

  - **Public Health and Safety Risks.** During pandemics or emergencies, misinformation can lead to harmful behaviors, such as vaccine hesitancy or panic-buying, exacerbating crises.

Threat Landscape of Misinformation/Disinformation in Bangladesh: Impact on Security and Development

In the 21st century, the traditional paradigms of warfare and national security have significantly evolved. As digital communication technologies proliferate, states and non-state actors have increasingly turned to information warfare as a potent tool to achieve strategic objectives (Arquilla, J., & Ronfeldt, D.,1997). Disinformation and misinformation have emerged as critical threats to

national security. In the context of Bangladesh, a rapidly digitizing society with a growing number of internet users and vibrant political and social discourse online, these phenomena pose significant risks across multiple dimensions of national security. On the same account, the development of various sectors of the country can be also negatively impacted by misinformation and disinformation. Both national security and development are multifaceted. Due to the limited scope, this chapter will focus on the impact of misinformation and disinformation on military, economy, and societal security. For the same reason, this chapter would also critically study the impact of misinformation and disinformation on public health, economic growth, and public trust aspects of development. However, before delving into the impacts and threats on national security and development, it is crucial to discuss the vectors, channels and mechanism of misinformation and disinformation.

Mapping Vectors, Channels, and Mechanisms of Misinformation and Disinformation

- **Vectors.** Who or What Spreads the False Information:

Table 4: Who or What Spreads the False Information

Vector	Description	Example
Humans (individuals/ groups)	Unwitting individuals, activists, ideologues, political operatives.	Citizens unknowingly sharing false flood alerts.
Automated Bots	AI-powered accounts programmed to share and amplify content.	Twitter bots inflating nationalist hashtags.
Influencers/Media Figures	High-follower individuals or partisan anchors.	TV personalities spreading unverified health tips.
Hybrid Actors	State/non-state actors using bots + humans in coordinated campaigns.	Fake news pages managed by political operatives and automated tools.

- **Channels and Platforms.** Where is the Information Disseminated:

Table 5: Where is the Information Disseminated

Channel	Role in Propagation	Characteristics	Bangladesh Relevance
Social media (e.g., Facebook, X/Twitter, YouTube)	Primary vehicle for rapid spread via shares, likes, and trends.	High virality, algorithm-driven visibility.	Major driver during elections, disasters.
Messenger Apps (e.g., WhatsApp, Telegram, IMO)	Encrypted, difficult to monitor.	Peer-to-peer sharing, creates trust illusion.	Common in rural/low-bandwidth areas.
Traditional Media (TV, print, radio)	Can inadvertently amplify falsehoods by covering viral stories.	Credible to older populations, large reach.	Sometimes slow in fact-checking viral news.
Online Forums (Reddit, Quora, local blogs)	Spread niche or ideological content.	Decentralized, community-based.	Less prominent but rising in youth discourse.

- **Mechanisms of Facilitating Dissemination**

Table 6: Mechanisms of Facilitating Dissemination

Mechanism	Description	Impact
Algorithmic Amplification	Platform algorithms promote engaging content, regardless of accuracy.	Misinformation spreads faster than fact-checked content.
Echo Chambers	Users cluster with like-minded people, reinforcing beliefs.	False beliefs are repeated until normalized.
Emotional Contagion	Emotionally charged content (fear, anger, outrage) spreads more rapidly.	Increases virality, bypasses rational filters.

Table 6: Mechanisms of Facilitating Dissemination		
Mechanism	**Description**	**Impact**
Bot Networks and Troll Farms	Coordinated use of fake accounts to manipulate trends.	Artificially boosts credibility and reach of false narratives.
Disguised Content	Use of legitimate-looking formats (fake news websites, forged documents).	Decreases audience suspicion and increases belief.
Memes and Visual Manipulation	Engaging, fast-consumed, hard to verify.	Easier to spread misleading narratives through humor/ symbolism.

Impacts on National Security

- **Military Security. Undermining Trust and Operational Readiness.** Misinformation and disinformation targeting military security involve the deliberate or inadvertent spread of false information related to defense strategies, military capabilities, troop movements, defense procurement, or national security incidents (US DoD, 2023). These campaigns can be both domestic and foreign in origin and often utilize social media, news outlets, and digital platforms to spread narratives that erode confidence in the military apparatus (Chowdhury & Ali, 2023).

    - **Open-Source Information Leakage.** Sensitive details about troop movement or military operations are sometimes inadvertently shared through unclassified sources (Bazzell, M., 2022).

    - **Cyber Penetration.** Hackers may gain unauthorized access to defense systems to plant false narratives or steal data (Singer, P. W., & Friedman, A., 2014).

    - **Social Media Manipulation.** Fake accounts and bots are used to spread antimilitary propaganda (Woolley, S. C., & Howard, P. N., 2019).

- **Influence Operations.** Coordinated campaigns designed to manipulate public perception of military actions (Paul, C., & Matthews, M., 2016). The actors may use following methods for execution:
    - **Fake News Stories.** Articles published by unverified platforms that misrepresent military activities.
    - **Deepfakes and Doctored Media.** Altered videos and images used to create false impressions of events.
    - **Phishing Attacks.** Used to gather sensitive military data by tricking personnel into revealing login credentials.
    - **False Flag Operations.** Incidents designed to look like they were perpetrated by another group to provoke conflict.

- **Impact Analysis.** False narratives can lead to hesitation or miscalculations in military responses. Troop confidence is undermined when exposed to disinformation questioning their mission. Public skepticism of the military can weaken national unity. False reports damage diplomatic relationships and trust in international forums.
    - **Case Study.** Disinformation During the 2022 Bay of Bengal Naval Exercise. In mid-2022, during a trilateral naval exercise in the Bay of Bengal involving Bangladesh, India, and the United States, a wave of disinformation circulated across several Bangladeshi and international social media platforms (Paul, 2022). Several anonymous accounts and fringe media outlets claimed that the exercise was a pretext for establishing US Military Base on Saint Martin's Island. Specific News and Dissemination False reports originated on Facebook pages and Twitter/X accounts known for spreading nationalist or anti-Western rhetoric. Some outlets repurposed old satellite images, presenting them as recent evidence of troop buildup on the island. Doctored screenshots of supposed official communications added further legitimacy to the claims. These narratives were rapidly shared in Facebook groups with over 100,000 members and trended on Twitter/X for nearly 48 hours.

- **Denial and Government Response.** The Bangladesh Armed Forces' Inter-Services Public Relations (ISPR) Directorate, Ministry of Foreign Affairs, India's Ministry of External Affairs, and the US Embassy in Dhaka had to relentlessly work to counter this disinformation.

- **Impact on Public Perception.** Despite denials, public opinion surveys conducted in August 2022 by a Dhaka-based think tank showed a 12% increase in skepticism toward military cooperation with the U.S. and India. As a result, Bangladesh temporarily paused a planned follow-up naval exercise in early 2023.

- **Economic Security: Destabilizing Financial Systems and Investor Confidence.** This involves the spread of false information regarding economic indicators, banking system stability, currency value, foreign investment or trade relations that mislead stakeholders and disrupt markets (Rahman, 2023).

  - **Vulnerabilities**

    - **Central Bank Communication Gaps.** Slow or unclear responses from financial institutions can leave room for rumors.

    - **Weak Financial Cybersecurity Infrastructure.** Hackers can disrupt banking services and spread false claims. Cyber-related fraud also rose by 18% in 2023, driven partly by disinformation (BIBM, 2023).

    - **Misinformed Public Behavior.** Public responses to rumors can amplify economic instability. How It Is Executed:

      - Fake Announcements on Bank Closures or Currency Devaluation: Shared through anonymous social media pages. In 2022, rumors about liquidity shortages at Islami Bank led to panic withdrawals exceeding Tk 10,000 crore (The Daily Star, 2022).

- Viral Rumors on Economic Collapse: Trigger panic buying or withdrawals. Speculative claims about Taka devaluation in 2023 triggered dollar hoarding, contributing to a drop in reserves to USD 20.95 billion.

- Manipulated Data or Statistics: Falsely portrayed graphs and charts presented as official. Politically motivated falsehoods have delayed reforms, keeping the Non-performing Loans (NPL) ratio at 9.93% as of September 2023 (Bangladesh Bank, 2023b).

- **Impact Analysis.** Bank may run out of cash due to fear-driven mass withdrawals. Uncertainty discourages both domestic and foreign investors. Market volatility due to stock market fluctuations based on unverified rumors.

- **Economic Security Case Study.** False Rumors About IMF Loan Conditions in 2022. In late 2022, amid economic stress triggered by global inflation and a weakening taka, Bangladesh entered negotiations with the International Monetary Fund (IMF) for a multi-billion-dollar support package. During this period, several false narratives circulated online suggesting the IMF had set "anti-Islamic" conditions, including mandatory changes to religious school funding and liberalizing laws on inheritance and banking interest. A set of YouTube videos and viral Facebook posts were used by the actors targeting audience in Madrasa and conservative communities.

  - **Denial and Government Response.** The Ministry of Finance and the IMF had to work relentlessly to counter this.

  - **Impact and Consequences.** Public protests in several districts, delayed IMF negotiations, and mistrust of global institutions.

- **Societal Security.** Fragmenting Communities and Exacerbating Social Tensions. Content that fuels religious, ethnic or communal divisions. It

seeks to destabilize societal cohesion through targeted narratives (Ahmed & Khan, 2024).

- **Vulnerabilities**
    - **Pre-existing Communal Tensions.** Historical divides can be easily inflamed.
    - **Echo Chambers on Social Media.** Reinforce bias through repetitive misinformation.
    - **Low Media Literacy.** Inability to critically assess news sources. How It Is Executed:
        - **Fake News and Altered Religious Content.** Content intended to insult or offend religious sentiments.
        - **Incendiary Messages on Messaging Apps.** Spread rapidly and anonymously.
        - **Bot-Amplified Polarization Campaigns.** Automated activity creates artificial consensus.

- **Impact Analysis.** Riots, Protests, and Inter-Community Violence due to inflamed sentiments. Erosion of National Unity due to distrust among different social groups. Increased hate crimes targeting minorities.
    - **Case Study: Communal Violence in Rangpur, 2021.** In October 2021, a Facebook post allegedly insulting the Quran went viral, sparking communal violence in Pirganj, Rangpur. The post was falsely attributed to a local Hindu youth, leading to arson attacks on dozens of homes in a Hindu neighbourhood. The post was planted using a cloned Facebook profile and exacerbated by local religious influencers. Over 60 homes were burned, and hundreds were displaced tearing apart societal harmonies. Thus, putting minority security under global scrutiny.

- **Impacts on Development.** The developmental costs of misinformation and disinformation refer to the negative impacts that false or misleading information can have on economic systems, particularly in developing countries or emerging economies. Disinformation and misinformation are significantly affecting national developments across the globe.

Table 7: Statistics on the Spread of Misinformation/Disinformation in Selected Countries/Regions as in 2024

Region/ Country	False News Circulation Rate	Top Platforms	Economic Cost (% of GDP)
Bangladesh	62% encounter weekly	Facebook (78%), YouTube (15%)	0.8% (approx $3.2B)
Nigeria	58%	WhatsApp (65%), Twitter (20%)	1.1% (approx $6B)
Europe	41%	TikTok (30%), Telegram (25%)	0.5% (approx $90B)
America	39%	X/Twitter (45%), Facebook (35%)	0.6% (approx $130B)
Sources: Reuters Institute, EU DisinfoLab, Dhaka University ICT Study 2024			

  - **Endangering Public Health and Well-being.** Misinformation and disinformation can influence individual behaviors, community health outcomes, and the overall efficacy of health systems.

    - **Vaccine Hesitancy.** Misinformation about vaccines reduced 67% of vaccination rates by 67%, leading to outbreaks of preventable diseases like measles, polio, and influenza in 2000 when a debunked study erroneously suggested a connection between the MMR (measles, mumps, rubella) vaccine and autism resulting vaccine hesitancy among 3.2 million children missing scheduled vaccination (Akter, 2024). This misinformation caused a rise in measles outbreaks in several nations, including the United States. Similarly, during the COVID-19 pandemic, false information

regarding vaccine risks and benefits, such as claims of infertility or microchip implantation, greatly influenced public willingness to get vaccinated, resulting in decreased inoculation rates in various communities. In Bangladesh, a survey revealed that 46.2% of adults were reluctant to receive the COVID-19 vaccine (Hossain & et al., 2021).

- **Chronic Disease Management.** Misinformation about the causes and treatments of chronic diseases can result in poor health decisions and ineffective health management. For example, misleading claims about "miracle cures" or dietary supplements can distract individuals with diabetes from following evidence-based treatment plans, such as insulin therapy or dietary management.

- **Stifling Economic Growth and Opportunity.** Misinformation and disinformation disrupted Bangladesh's banking sector, undermining public trust and financial stability. In 2022, rumors about liquidity shortages at Islami Bank led to panic withdrawals exceeding Tk 10,000 crore (The Daily Star, 2022). Speculative claims about Taka devaluation in 2023 triggered dollar hoarding, contributing to a drop in reserves to USD 20.95 billion (Bangladesh Bank, 2023a). Cyber-related fraud also rose by 18% in 2023, driven partly by disinformation (BIBM, 2023).

- **Market Manipulation.** False information can lead to stock market volatility through panic selling, causing share prices to drop unnecessarily. In 2013, false reports of a "bomb explosion" at the White House caused a brief plunge in the stock market.

- **Digital Economy and E-Commerce.** Misinformation and disinformation can shape perceptions around online businesses, affecting consumer trust and e-commerce growth. In the late 1990s and early 2000s, such misinformation ravaged the e-commerce where Amazon alone had to invest a lot for bringing back the trust.

- **Job Market Misconceptions.** Misinformation about job market trends can lead students to pursue degrees in fields with low employment prospects,

resulting in student debt without corresponding job opportunities. In the Philippines during the early 2000s many students pursued nursing degrees due to widespread claims that there was a global demand for nurses, particularly in US and UK. However, the demand was overstated, and many graduates found themselves unable to secure nursing jobs abroad.

- **Weakening Social Trust and Civic Engagement**

  - **Erosion of Trust.** Misinformation and disinformation can erode trust in institutions (e.g., government, elections, media, healthcare) and among individuals. The 2016 U.S. Presidential election saw widespread misinformation, such as claims about voter fraud, leading to deep political divides and public skepticism about the integrity of the electoral system.

  - **Polarization.** False narratives can deepen existing divides between different social, political, or racial groups. Where misinformation exaggerates differences, it can lead to a "us vs. them" mentality. For example, the spread of misinformation about COVID-19, such as false claims regarding the virus's origins, treatments, and vaccine efficacy, created confusion and distrust in different regions of the world.

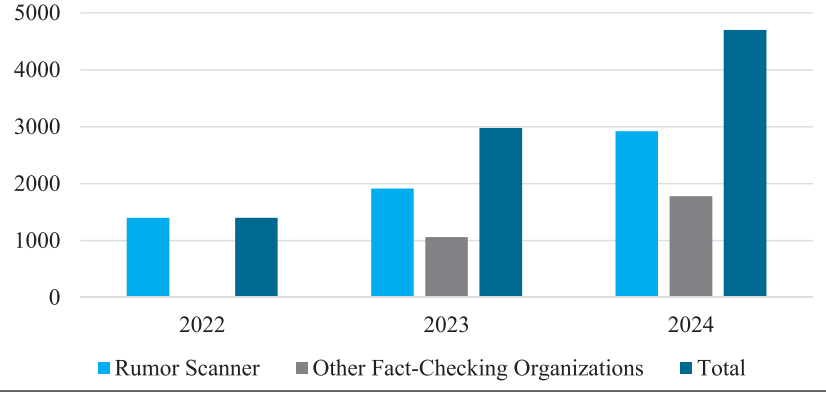
National Capacity and Institutional Response to Counter Misinformation and Disinformation in Bangladesh

Bangladesh faces significant challenges from the spread of disinformation and misinformation, particularly through social media platforms. In recent years, various strategies and interventions have been implemented, including legal and regulatory measures, technological solutions, education and awareness campaigns, and promoting transparency and accountability. This chapter provides an analytical overview of these strategies and interventions which will ultimately guide to propose the strategies to counter the impact of misinformation and disinformation in national security and national development in Bangladesh.

- **Fact-Checking and Verification Efforts: The Role of Independent Journalism**

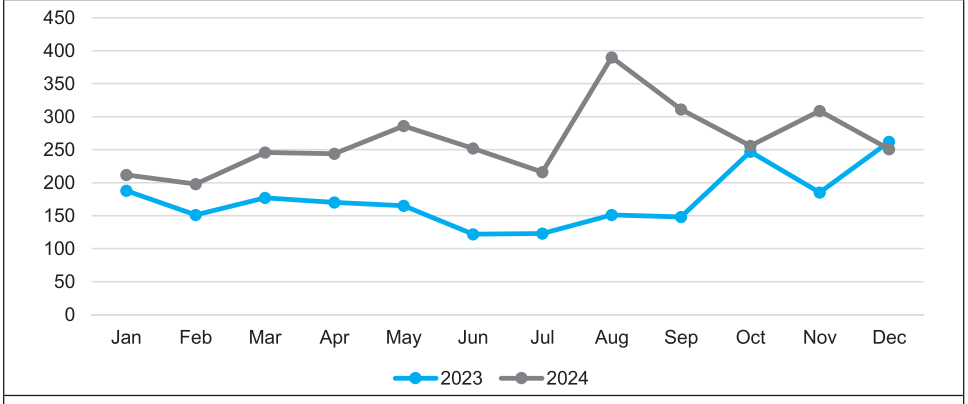
Fact-checking initiatives have grown rapidly in Bangladesh. Fact-checking initiatives such as Bangladesh Fact Check (BFC), FactWatch (Fact-Watch, 2025), Jachai (Jachai, 2025) and Rumor Scanner (Rumor Scanner Bangladesh, 2025) play a vital role in verifying the accuracy of information circulating online and collaborate with social media platforms actively debunk false claims and raise awareness by publishing verified information. These fact checking organizations employ a comprehensive but manual eight-step process for fact-checking. These steps are Fact-Check Request, Active Monitoring Team, Claim Selection for Verification, Research, Report Writing and Editing, Digital Banner, Rating, and Correction (Rumor Scanner Bangladesh, 2025). However, the employ automated keywords, pattern detection and reverse image detection to flag viral rumors. Fact-checking reports in Bangladesh increased by 58% in 2024 (dismislab, 2025).

Figure 1: Fact-Checking Efforts by Different Organizations in Bangladesh



Source: Researcher himself collecting information from internet

Figure 2: Comparison of Unique Fact-Checks for Each Month in 2023 and 2024



Source: Researcher himself collecting information from internet

- **Technological Solutions: Promises and Perils**

The government and private sector have been investing in developing artificial intelligence (AI) tools to detect and filter out disinformation. The use of AI-supported tools can also enhance the efficiency and accessibility of fact-checking efforts (Userhub, 2024). However, the accuracy and reliability of these tools remain a challenge, and there is a need for continuous improvement and adaptation to evolving disinformation tactics. The credit applications are rejected, and social media posts are deleted based on AI decisions, while mechanisms to contest these decisions are not fully developed. Many algorithms are opaque, unregulated and difficult to contest. Pattern-recognition algorithms could be applied to target certain people or produce disproportional and biased collateral damage due to imperfections in the code or in training data.

- **Legal and Regulatory Frameworks: Balancing Freedom and Responsibility**

  - The Constitution of Bangladesh and various legal statutes outline the permissible boundaries for media practices, balancing freedom with national security, public order, and morality. Article 39 guarantees press freedom but subjects it to reasonable restrictions concerning state

security, foreign relations, public order, decency, morality, contempt of court, defamation, or incitement to offense. Article 43 ensures the right to privacy in communication, with similar caveats related to state security, public order, morality, and health. Section 124-A of the Penal Code makes sedition a crime. It punishes people who encourage hatred or disloyalty against the government, but it does not apply to fair criticism meant to bring change.

- Section 295-A penalizes deliberate and malicious acts intended to outrage religious feelings. Section 99 of the Criminal Procedure Code empowers the government to seize publications containing seditious or religiously offensive content. These measures relate to offenses outlined in Penal Code sections 123-A, 153-A, and 295-A. The Special Powers Act of 1974 further defines and restricts prejudicial reporting, which includes content likely to harm state security, public order, the administration of law, essential services, or the state's financial interests. Sections 16, 17, and 18 of this Act prescribe penalties for creating or disseminating prejudicial reports, authorize the government to ban and seize such publications, demand security from media outlets, and require pre-publication scrutiny of sensitive content.

- Additionally, the Indecent Advertisement Act of 1926 prohibits the publication of indecent advertisements. To regulate digital communications, the government enacted the Information and Communication Technology (ICT) Act in November 2006. Section 57 of the Act caused concerns about its ostensible goal to restrict freedom of expression (Freedom House, 2017). The Section authorized prosecution of anyone who publishes, in electronic form, material deemed fake, obscene, defamatory, or any material that tends to deprive or corrupt its audience (Reuters, 2018).

- In 2013, the government toughened the ICT Act, eliminating the need for arrest warrants (Reuters, 2018). Between June 2016 and May 2017, 300 people were arrested under the ICT Act and 19 journalists were implicated. The government also blocked several messaging apps and blogs to curb the spread of misinformation. In August 2016, 35 news

websites were blocked for publishing objectionable content about the government (Freedom House, 2017). Bangladesh has enacted the Digital Security Act 2018, which aims to address digital crimes and misinformation. This Act also has sections that impose restrictions on freedom of expression.

- According to news reports and human rights organizations, this Act is used to suppress freedom of expression (Chowdhury, 2020), (Amnesty International, 2019). The government charged or arrested 20 journalists on charge of violating this law in less than five weeks in April and May 2020 (Chowdhury, 2020). On the World Press Freedom index, Bangladesh slid to 151st position in 2020 – worse than Afghanistan, Pakistan, Russia, Venezuela – from 121st position in 2009 (Reporters Without Borders, 2009), (Reporters Without Borders, 2020).

- The Bangladesh Telecommunication Regulatory Commission (BTRC) has established guidelines for internet service providers to block or remove false content. While these measures provide a legal framework, their effectiveness depends on proper implementation and adherence to democratic principles. International frameworks, such as Article 19 of the Universal Declaration of Human Rights, advocate for freedom of opinion and expression, while Article 29 acknowledges that these rights may be subject to limitations necessary to respect the rights and freedoms of others and to meet the just requirements of morality, public order, and the general welfare in a democratic society. 1 These constitutional and legal provisions, alongside international guidelines, serve as crucial reference points for the conduct of media in Bangladesh.

• National Telecommunication and Monitoring Cell (NTMC)

The National Telecommunication Monitoring Center (NTMC) in Bangladesh is involved in monitoring telecommunications and online activity. While its specific functions may include safeguarding national security, its role raises

concerns about potential impacts on privacy and freedom of expression. The balancing act between security and individual liberties is a critical issue in the context of Bangladesh's efforts to combat disinformation and misinformation. Based on available information, the National Telecommunication Monitoring Center (NTMC) in Bangladesh has the technical capability to:

- **Intercept Communications.** This includes mobile and landline phone calls, SMS messages, and communications on various internet platforms.

- **Monitor Social Media.** The NTMC can monitor activity on platforms such as Facebook, X (formerly Twitter), Telegram, Viber, IMO, and Skype.

- **Oversee Online Activity.** The NTMC has the ability to monitor online communication mediums, including websites, blogs, and emails.

- **Utilize surveillance equipment.** The NTMC employs various surveillance tools, including vehicle-mounted data and mobile interceptors.

- **Deploy Advanced Surveillance Technology.** Reports indicate the NTMC has acquired sophisticated surveillance software, such as Pegasus, which enables the hacking of mobile phones to access messages, photos, emails, record conversations, and activate microphones and cameras.

- **Control Internet Systems.** The NTMC is involved in controlling internet systems and operators.

- **Filter Content.** The NTMC has the capacity to block and filter content deemed to be "anti-government propaganda."

- **Media Literacy and Public Awareness Initiatives: Empowering Critical Thinking**

In Bangladesh, media literacy and public awareness initiatives are gaining traction as crucial tools against the rising tide of disinformation. Efforts are underway to equip citizens with the critical thinking skills necessary to navigate the complex information landscape (Rahman, 2023). However, assessing the effectiveness of these programs reveals significant challenges. Reaching diverse populations, particularly in rural areas with varying levels of digital access and literacy, remains a key obstacle (Ahmed & Khan, 2024). Moreover, changing deeply ingrained beliefs and fostering a culture of critical evaluation requires sustained and culturally sensitive approaches (Islam, 2022). While progress is being made, a concerted and inclusive national strategy is essential to truly empower citizens against disinformation. ISPR conducts media literacy initiatives.

- **International Cooperation**

Robust international cooperation is vital for tackling the transnational challenge of disinformation. Establishing shared definitions and frameworks with other nations, particularly within South Asia and beyond, is crucial for a unified global response (Hossain, 2024). Enhanced information sharing and early warning systems across borders can facilitate the rapid identification and mitigation of coordinated disinformation campaigns (Chowdhury & Ali, 2023). Joint research initiatives and capacity-building programs with international partners can provide access to best practices and technological advancements (Siddiqui, 2022). Furthermore, exploring legal and regulatory cooperation can help harmonize approaches to address the legal complexities of cross-border disinformation. Active engagement in multilateral platforms and bilateral partnerships is essential for Bangladesh to strengthen its defenses against this evolving threat.

- **Ethical Dilemmas and Unintended Consequences**

The implementation of counter strategies against disinformation presents complex ethical dilemmas and potential unintended consequences. While aiming to protect the public, measures like content moderation risk accusations of censorship and the suppression of legitimate dissent (Karim, 2023). 1 Increased surveillance, even with the intention of tracking disinformation networks, raises serious concerns about privacy violations and the potential for misuse of such powers (Haque & Majumder, 2024). Striking a balance between security and fundamental rights is paramount. 2 Overly aggressive tactics could inadvertently stifle free expression and erode public trust in both the government and media (Islam, 2022). Therefore, any counter-disinformation strategy must be carefully considered, with robust oversight and safeguards to prevent unintended restrictions on civil liberties and ensure ethical implementation.

A Multidimensional Approach Towards Building A Resilient Information Ecosystem for Security and Development

In the digital era, information is not merely a tool for communication; it is a source of influence, power, and vulnerability. Misinformation and disinformation have emerged as threats that transcend borders and institutions, undermining democratic values, inciting communal tensions, and obstructing development. To safeguard national security and promote development, Bangladesh must adopt a comprehensive, multi-stakeholder strategy based on eight pillars that builds resilience across the information ecosystem.

Integrated Approach of Government, Media, Academia, Tech Platforms, and Civil Society

- **Formation of National Information Resilience Council (NIRC)**
    - A resilient information ecosystem cannot be engineered by decree; it must be co-produced. It requires the convergence of multiple sectors that interact dynamically to create a system of checks, balances, and collaboration. Government supplies policy direction, legal authority,

and public resources, but credibility comes from visible collaboration with media, academia, technology firms, and civil-society organizations. A permanent NIRC chaired by the Cabinet Division, could institutionalize this quintuple cooperation. A standing council reduces duplication, accelerates knowledge transfer and signals domestic unity and democratic legitimacy.

- The NIRC would include ministries like Information, Home, Telecommunication, Education and Foreign Affairs, the Press Club, leading universities, communication departments, and platform representatives like Meta, Google, WhatsApp, fact-checking networks, youth organizations, and minority-rights groups. Tasks may include horizon-scanning and joint risk assessments, coordinated crisis messaging, annual information-environment audits, and setting industry standards for transparency reports, advising on curriculum reform and funding priorities.

- **Media.** The media can be a very effective tool and serves as both a shield and a potential conduit for disinformation. Many mainstream news organizations have adopted fact-checking protocols, but sensationalism and competition for clicks often lead to unverified reporting. Rumor Scanner BD and BD FactCheck now serve as third-party verification bodies, working to debunk false claims about elections, communal issues, and government policies.

- **Academia.** Universities and think tanks provide crucial research and training. Their role is vital in understanding disinformation trends and proposing evidence-based solutions. The Department of Mass Communication and Journalism at Dhaka University has introduced modules on media ethics and digital literacy, contributing to a generation of media-savvy professionals.

- **Technology Platforms.** Global platforms like Facebook, WhatsApp, and YouTube dominate Bangladesh's digital landscape. These platforms must take responsibility for moderating harmful content, providing transparency in algorithms, and collaborating with national authorities on content flagged

as harmful. In 2023, Meta partnered with the Election Commission to monitor fake news during local elections and remove inflammatory posts.

- **Civil Society.** NGOs and community organizations play a critical role in public education and social mobilization. They bring the last-mile reach that neither the government nor the media can ensure alone. BRAC's digital literacy programs in rural areas have trained over 100,000 women on identifying online scams and hate speech.

- **Enhancing Digital and Media Literacy Nationwide.** Digital literacy is the cornerstone of information resilience. Bangladesh's literacy drive that lifted reading proficiency from 47 percent in 2000 to 76 percent in 2023 offers a template for a new Digital and Media Literacy Mission. With over 131 million internet subscribers (BTRC, 2024), many users in Bangladesh engage online without the tools to verify authenticity, making them susceptible to manipulation. Finland is considered as the most media-literate country globally, teaches media literacy from kindergarten to high school using role play, real-life examples, and interdisciplinary education. Bangladesh can adapt these methods to its context.

    - **Formal Education Integration.** Introduce critical media literacy from the secondary school level under the National Curriculum and Textbook Board (NCTB) curriculum. Teach students how to cross-verify news, evaluate sources, and understand bias. The technologically developed Bangladesh initiative includes components of ICT education, but needs to go further in incorporating digital responsibility and ethical media consumption. From Grades 6-8: spotting clickbait, basic source checks (lateral reading), Grades 9-10: bias and framing, verification tools (reverse-image search, timestamps) and Grades 11-12: civic media production, debates and use of ethical AI.

    - **Developing the Teacher's Skills.** Pre-service training colleges need a compulsory semester on inquiry-based media education, complemented by micro-credential MOOCs in Bangla. Develop Bangla teaching kits with mock social-media feeds and headline-rewriting exercises. Certify 5 000 "Master Trainers" via the National Teachers Training Institutes.

- **Community-Based Learning.** Use local platforms like Union Digital Centers (UDCs) to conduct training on media navigation. Materials must be in Bangla and dialects like Chittagonian, Sylheti, and Rohingya. Targeted Campaigns for Vulnerable Groups, like women, minorities, and rural youth, are more prone to disinformation traps. Leverage community radio, local mosques, and mobile outreach to reach these groups. During the Rohingya influx, UNICEF ran "MythBuster" audio programs to counter rumors about vaccines and food distribution in Cox's Bazar

- **Public-Private Partnerships for Technology-Driven Solutions.** Disinformation travels at algorithmic speed. If Bangladesh answers with memos and manual takedown letters, it will always be several clicks behind. Harnessing the country's growing tech ecosystem, 4,500 registered IT firms, 400 (+) start-ups, and a vibrant university research circuit offer a force multiplier that governments alone cannot match. A well-architected public-private partnership model can turn raw data exhaust from telecom companies, social media, and news sites into actionable intelligence that frontline officials, editors, teachers, and even local imams can use within minutes. Doing so requires two mutually reinforcing layers e.g. AI-based monitoring pipelines that sift billions of Bangla, Chittagonian, and Sylheti posts for early anomalies, and a National Early-Warning System that converts those anomalies into colour-coded alerts, standard operating procedures, and, where necessary, cross-border escalation channels.

  - **AI-Based Monitoring.** Use machine learning models trained in Bangla and regional languages to scan and flag disinformation. Partner with startups and research institutions to create scalable, cost-effective solutions. Dhaka-based AI lab NeuroSoft has developed sentiment analysis tools for Bangla Facebook posts, identifying inflammatory language in real-time.

  - **Early-Warning Systems (EWS).** Establish a national EWS similar to EU's disinformation or India's FactCheck India, integrated with law enforcement, media, and telecom regulators. EWS dashboards should be accessible to journalists, civil servants, and educators. Maintain a

24/7 fusion desk housed at the National CIRT, the desk would include seconded staff from Meta, Google, and the country's largest ad networks, ensuring platform-side actions occur within the same hour as government verification.

- **Collaborative Ecosystems.** Use Bangladesh High Tech Park Authority (BHTPA) and Startup Bangladesh to fund civic-tech startups building anti-disinformation tools. Encourage private sectors involvement through innovation grants. In the Philippines, the government worked with local Facebook groups and telecom companies to set up a "Hoax Alert Hotline" during elections. Bangladesh can consider similar hotlines via mobile apps or SMS.

• Strengthening Legal Frameworks

- **Targeted Anti-manipulation Clauses.** Amend the Digital Security Act (DSA) to narrow offences to coordinated inauthentic behaviour, undisclosed foreign influence operations, and synthetic media intended to defame or incite violence, replacing vague categories like "offensive" or "harassing" content.

- **Procedural safeguards.** Introduce robust procedural checks to ensure accountability and transparency in content takedown processes. These include:

    - **Prior Judicial Authorization.** Require prior judicial approval for any content takedown lasting more than 24 hours to safeguard against arbitrary censorship.

    - **Statutory Timelines for Review.** Mandate clear legal timelines for reviewing takedown decisions to prevent indefinite or unjustified content suppression.

    - **Transparency Measures.** Require the mandatory publication of anonymized and aggregated takedown statistics, disaggregated by type, platform, and reason for removal.

- **Platform Duty Alignment.** Implement a tiered "duty of care" framework that differentiates responsibilities based on platform scale and societal impact. Key obligations for large platforms (defined as having over five million monthly users) should include:
    - **Annual Risk Assessments.** Conduct and publish assessments identifying potential harms from platform misuse.
    - **Local Grievance Officers.** Appoint resident grievance redressal officers to ensure responsiveness to user concerns.
    - **Application Programming Interface (API) Access for Oversight.** Offer controlled access to content moderation of APIs to accredited independent oversight bodies and researchers, ensuring non-invasive auditing.
- **Civil Remedy Expansion.** Strengthen civil legal frameworks to provide timely and effective recourse to victims of viral online harms, particularly in cases of defamation or synthetic media (e.g., deepfakes). Key provisions should include:
    - **Fast-Track Civil Redress.** Enable expedited legal procedures for aggrieved individuals, including the issuance of interim relief orders.
    - **Interim Injunctions.** Allow courts to impose temporary content takedown or restriction orders to prevent further harm during proceedings.
    - **Algorithmic Demotion Orders.** Grant courts the power to compel platforms to suppress harmful content algorithmically without full takedown, thereby minimizing virality while preserving evidence.
- **Independent Data Protection Authority (DPA).** Data is the fuel of both legitimate analytics and manipulative micro-targeting. An autonomous data protection authority is essential. Bangladesh's draft Data Protection Act remains under review. Establishing an effective DPA under the ICT division by 2026 is crucial for building public trust and regulating private data use.

- **Key Features of a Strong DPA.** Autonomous status with operational and budgetary independence. Transparent appointment process and multi-sectoral board oversight. Investigative powers to penalize data misuse, especially by telecom companies and digital platforms. Kenya's Data Protection Commissioner operates independently and reports directly to Parliament, ensuring both transparency and accountability.

- **Legal Basis.** Enact a comprehensive Personal Data Protection Act aligned with international frameworks such as the EU's General Data Protection Regulation (GDPR) and India's Digital Personal Data Protection (DPDP) Act, but tailored to Bangladesh's socio-economic context. Key customizations should include lower compliance burdens for small and medium enterprises (SMEs) to encourage innovation without regulatory overload. It must recognize community data rights, especially for indigenous and marginalized groups, to protect cultural identity and collective interests.

- **Powers.** Equip the Data Protection Authority with strong regulatory powers, including licensing and oversight of data brokers to prevent misuse of personal information and auditing algorithmic profiling systems used in areas like credit scoring, hiring, or public service delivery. It should have enforcement authority to issue orders and impose fines proportionate to an entity's global turnover and decision-making powers on cross-border data transfers, ensuring such flows meet standards of adequacy and security.

- **Governance.** Establish a robust and independent governance model to ensure the DPA's credibility and autonomy. Make sure that the commissioners are appointed by a parliamentary committee with safeguards against executive overreach and funded directly, ensuring financial independence. They require mandatory public consultations before adopting any codes of practice or regulations, promoting transparency and stakeholder participation.

- **Safeguarding Freedom of Expression.** Freedom of expression is the oxygen of a resilient information ecosystem. While regulating harmful content, Bangladesh must avoid turning counter-disinformation into censorship. Over-zealous enforcement can chill legitimate speech, eroding trust and pushing discourse into encrypted obscurities.

    - **Policy Doctrine.** Adopt a Freedom First Principle. If intervention is necessary, it should be proportionate with the least restrictive means available. Proactive disclosure of state information, budgets, procurement, and crisis data reduces speculation voids that conspiracists exploit. Extend the Right to Information Act with protections for employees who expose manipulation or censorship.

    - **Ensuring a Safe but Free Space.** Law enforcement should differentiate between dissent and harmful lies. Journalists and fact-checkers must be protected, not persecuted. UNESCO principle designates "Disinformation laws must pass a three-part test, e.g. legality, legitimacy, and proportionality."

    - **Independent Media Viability.** Expand zero-interest loans for local news start-ups, tax incentives for investigative journalism, and an innovation fund for vernacular-language podcasts that reach under-served audiences.

    - **Enabling Civil Participation.** National media council (Press Club) can mediate disputes between the state and journalists. Germany's Network Enforcement Act (NetzDG) requires platforms to respond to user complaints while ensuring due process and appeals.

- **Strategic Sovereignty and Ethical Use of Information.** Information sovereignty is not isolationism but strategic stewardship over critical digital infrastructures and narratives. Bangladesh must assert control over its digital future while ensuring ethical governance of information systems.

    - **Strategic Sovereignty Priorities.** Host sensitive government and citizen data on national servers. Develop localized platforms and

search engines for critical services. Invest in indigenous data labeling and language models to reduce reliance on foreign datasets. The National Data Center (NDC) now hosts over 250 government services. Expansion to include media archives and social data that can enhance sovereignty.

- **Ethical AI Charter.** Through the NIRC, promulgate an Ethical Information and AI Charter encompassing transparency, fairness, accountability, and human oversight, binding on public-sector deployments and recommended for private adopters. Ban unauthorized surveillance and protect user privacy. Mandate transparency in algorithmic decision-making for platforms operating in Bangladesh. Create AI ethics frameworks rooted in cultural, religious, and democratic values.

- **Secure Supply Chains.** Mandate security by design standards for imported networking gear; vet foreign direct investment in sensitive data sectors through a national security lens without deterring benign capital.

- **Narrative Capacity.** Invest in strategic communications units to be able to project fact-based, compelling counter-narratives internationally, showcasing Bangladesh's development stories and pluralistic culture.

• Regional and International Cooperation

- **Falsehoods Hop Borders with a Single Click.** Bangladesh cannot firewall itself from a rumour that is minted in Delhi at noon, translated in Kuala Lumpur by dusk, and weaponised on local Facebook groups before midnight. Dhaka's domestic toolkit, no matter how sophisticated, will remain incomplete without organized partnerships across South Asia and the wider multilateral arena. Here, two reinforcing layers of outward engagement are elaborated e.g. regional strategies that leverage geographic proximity, shared languages, and intertwined media markets, and global platforms that amplify Bangladesh's voice in rule-making forums while unlocking technical and financial support.

- **Regional Strategies**
  - **SAARC Digital Resilience Forum**
  - **Purpose.** A 24/7 "fusion cell" must be operated where SAARC member-states exchange real-time alerts on emerging disinformation campaigns, conduct joint attribution, and coordinate takedown requests to platforms.
  - **Structure.** Its secretariat must rotate in the capitals of member states (first three-year term in Dhaka), staffed by seconded cyber-analysts, police liaison officers, and media-ethics specialists; linked to Computer Incident Response Teams (CIRTs) and telecom regulators in each capital.
  - **Outputs.** It should share quarterly threat bulletins, AI training datasets in Bangla-Hindi-Urdu, and arrange annual cross-border tabletop exercises simulating communal violence rumors or cross line of combination of deepfake videos.
- **South Asia Media Integrity Network**
  - **Membership.** It must integrate legacy newspapers like Pak Times, The Daily Star, The Hindu etc, digital-native portals like Scroll in, BD FactCheck, and regional NGOs like BRAC, CEJ-Pakistan, CPJ-India etc.
  - **Activities.** A "Red Phone" hotline system must be set from newsroom to news room for debunking stories that spill across borders (e.g., cyclone death-toll exaggerations etc). Fellowship may swap placing Bangladeshi fact-checkers in Nepali or Sri-Lankan newsrooms to learn local verification workflows. A bi-lingual stylebook on responsible flood and refugee reporting may be established and updated in every monsoon.
- **Issue-Specific Dialogues**
  - **Rohingya Information Corridor.** A monthly encrypted briefings between Bangladesh's PID, Malaysian Communications and

Multimedia Commission (MCMC), and UNHCR digital-teams may be organized to trace hate content seeded in diaspora Facebook groups and take counter steps.

- **Election-period "Quiet Hours" Pact.** An informal SAARC memorandum should be formed urging parties and influencers to refrain from mass-messaging 48 hours before polling. It must be monitored by mixed civil-society task-forces.

- **Global Engagement**

  - **Membership and Leadership Roles**

    - **Global Partnership on AI (GPAI).** Bangladesh should actively pursue co-chairmanship of the GPAI Working Group on Responsible AI for the Majority World, a forum dedicated to ensuring that AI benefits are equitably shared and that risks are managed in low and middle-income countries. As co-chair, Bangladesh could steer the group's agenda toward developing content moderation tools for low-resource languages, drawing on its own expertise in Bangla language processing. This leadership role would also enable Dhaka to convene pilot projects by partnering with universities, civil society, and Educational Tech (EdTech) firms to create open-source datasets and algorithms that detect hate speech, misinformation, and other harmful content in underserved linguistic communities.

    - **Freedom Online Coalition.** By advocating for and ultimately hosting an "Asia Digital Integrity Track" within the Freedom Online Coalition, Bangladesh can galvanize a regional network of governments, NGOs, and tech platforms to jointly address disinformation and election interference. This specialized track would define grant criteria for region-specific fact-checking initiatives, incentivizing donors and multilateral agencies to fund local newsrooms, grassroots watchdog groups, and academic partnerships. Regular track meetings in Dhaka would also facilitate

peer learning, allowing member countries to share best practices on digital literacy campaigns, crisis response protocols, and rapid response toolkits.

- **Paris Call for Trust and Security in Cyberspace.** Endorsing in Principles 1 ("Defend the Open Internet") and 5 ("Strengthen Digital Hygiene") of the Paris Call for Trust and Security in Cyberspace signals Bangladesh's would comply with the commitment to both preserving an open, interoperable internet and bolstering citizens' ability to protect themselves online. Leveraging this endorsement, Bangladesh can propose an addendum focused on platform accountability in the Global South, calling for transparency in moderation policies, spot-audit requirements for compliance with local laws, and support for capacity-building in emerging economies. Such an addendum would frame platform governance as a shared international responsibility rather than a purely domestic one, reinforcing Bangladesh's vision of equitable and rules-based cyberspace governance.

- **Hosting Flagship Events in Dhaka**

  - **UNESCO Digital Literacy Summit (2027).** Organize a high-profile summit in Dhaka bringing together leading EdTech companies, national and regional curriculum planners, digital rights NGOs, and youth activists. The summit will culminate in the adoption of a Dhaka Declaration on Critical Media Education, a set of guiding principles and competencies for learners and educators that map directly onto the UNESCO-backed ROAM-X (Read, Observe, Analyze, and Media creation Exchange) framework. Participants will commit to integrating these standards into teachers training programs and national curricula by 2028, with periodic peer reviews to track progress and share best practices across South Asia.

  - **Commonwealth Ethical-AI Forum (2028).** Host a Commonwealth wide forum in Dhaka to present cutting-edge

research on Bangla large-language models, highlighting innovations in low resource language processing and cross-lingual transfer. Key outcomes will include a formal "Commonwealth Model Card Initiative," under which every participating nation agrees to publicly document the architecture, training datasets, known limitations, and bias-audit results of deployed AI systems. This transparency pledge will be supported by a technical working group that offers peer assistance in conducting ethical risk assessments and publishes an annual Commonwealth Ethical-AI Report.

- **Benefits of such Events.** These flagship events will position Bangladesh as an emerging exporter of AI knowledge and talent, showcasing homegrown solutions to a global audience of policymakers, investors, and academics. By spotlighting local start-ups and research labs, the country can attract significant venture capital inflows and strategic partnerships, accelerating the growth of its AI ecosystem. Moreover, anchoring both declarations and commitments in internationally recognized standards ensures that Bangladesh's forthcoming digital policy and regulatory frameworks are informed by and compatible with the best practices in digital literacy and ethical AI governance.

Conclusion

In an age where information flows faster than facts, societies worldwide face a growing threat from misinformation and disinformation, two disruptive forces that challenge national security and sustainable development. While digital connectivity has empowered millions, it has also enabled the rapid spread of false narratives, hate speech, and propaganda. For developing nations like Bangladesh, where digital transformation is accelerating amid social, political, and economic complexities, the manipulation of information presents both internal vulnerabilities and external risks.

Understanding misinformation and disinformation requires structured typologies based on intent, format, and target audience. Misinformation involves false content shared without harmful intent, such as outdated cyclone

warnings, while disinformation is deliberately deceptive, like fabricated news about border threats. By format, false content may appear as satire, manipulated media, fabricated stories, or misused statistics, each impacting public perception in different ways. Target-based typologies identify specific audiences, such as the general public, political figures, ethnic/religious groups, or national institutions, showing how false narratives can fuel panic, polarization, or undermine state legitimacy. While each classification offers valuable insights, no single framework captures the full complexity; a multi-dimensional approach is most effective, especially in fragile environments like Bangladesh.

In today's digital world, misinformation and disinformation are powerful tools of information warfare, used in political campaigns, social movements, and conflicts. Disinformation campaigns exploit social media algorithms and generative AI to create and spread deceptive narratives quickly. This has blurred the line between truth and falsehood, weakening public trust, democratic institutions, and national security. Information also plays a key role in development, enabling informed policy decisions, innovation, and civic participation. However, global trends reveal that misinformation is now weaponized to destabilize nations, with countries like Russia and China accused of conducting coordinated disinformation campaigns. These trends, identified by the World Economic Forum as critical short-term risks, have serious geopolitical and domestic implications-spurring social unrest, economic instability, and public health crises. Thus, understanding and combating information disorder is essential for maintaining both global cooperation and national stability.

Misinformation and disinformation in Bangladesh spread through individuals, automated bots, media influencers, and hybrid human-bot actors, utilizing social media, messaging apps, traditional media, and online forums. They leverage algorithm-driven amplification, emotionally charged content, echo chambers, troll farms, and deceptive visuals for rapid dissemination. These false narratives pose serious national security threats. In the military domain, they erode trust and readiness via fake news, doctored media, and phishing-illustrated by campaigns such as during the 2022 Bay of Bengal naval exercise.

Economically, fabricated announcements and manipulated data destabilize financial systems, triggering panic like the IMF loan rumors and false claims about Islami Bank. In societal terms, they inflame communal tensions through fake religious content and echo chambers, leading to violence such as the 2021 Rangpur attacks on Hindus. These campaigns exploit vulnerabilities like cyber insecurity, communal fault lines, and low media literacy, causing diplomatic strain, investor anxiety, civil unrest, and social fragmentation.

Misinformation also hinders development, particularly in emerging economies. In Bangladesh, 62% of individuals encounter false news weekly-primarily on Facebook-resulting in an estimated loss of 0.8% of GDP. Public health suffers as misinformation fosters vaccine hesitancy-46.2% of adults were reluctant to take COVID-19 vaccines-leading to outbreaks of measles and polio. Chronic disease management is undermined by "miracle cure" claims. Economically, distrust fueled by rumors destabilizes banks, fuels market volatility, and suppresses e-commerce growth. Misinformation skews career decisions too-exaggerated nurse demand in the Philippines led to widespread underemployment. Ultimately, misinformation weakens civic engagement, public confidence, and development trajectories.

Bangladesh faces serious challenges from the spread of misinformation and disinformation, especially through social media. In response, the country has adopted a multi-pronged approach involving legal, technological, educational, and journalistic strategies. Independent fact-checking organizations like Bangladesh Fact Check, FactWatch, Jachai, and Rumor Scanner verify online claims and collaborate with media to raise awareness. The government and private sector are also developing AI tools for detecting false information, although concerns remain over their reliability and transparency. Legally, Bangladesh's Constitution, Penal Code, ICT Act, and the Digital Security Act provide frameworks to address harmful content, but critics argue these laws sometimes suppress freedom of expression and press. The NTMC (National Telecommunication Monitoring Center) plays a vital role in surveillance and online monitoring, yet its extensive capabilities raise concerns about privacy and civil liberties.

Media literacy campaigns aim to equip citizens with critical thinking skills, though reaching rural populations and changing entrenched beliefs remain challenges. International cooperation is essential for cross-border disinformation threats, involving shared frameworks, early warning systems, and legal collaboration. Ethical dilemmas also arise-efforts to combat disinformation may lead to censorship or the erosion of public trust. Surveillance measures, while intended to ensure security, risk violating personal freedoms. While Bangladesh has initiated several strategies to counter disinformation, balancing security and civil liberties remains complex. Robust safeguards, inclusive media education, international cooperation, and ethical oversight are critical to building long-term resilience against misinformation's threats to national security and development.

In the digital era, misinformation and disinformation pose significant threats to democracy, social harmony, and development. Bangladesh, in particular, faces challenges in combating these issues. To address this, a comprehensive, multi-stakeholder approach is essential. Establishing an National Information Resilience Council (NIRC) would institutionalize collaboration among government, media, academia, tech platforms, and civil society. This body would coordinate responses, share knowledge, and ensure democratic legitimacy in tackling information-related challenges. Implementing a nationwide initiative to integrate media education into school curricula and teacher training is crucial. Leveraging community centers and radio for outreach can further enhance public awareness. Public-private partnerships can drive tech-based monitoring and early warning systems using AI to detect disinformation in real time. Refining the Digital Security Act is necessary to introduce procedural safeguards and establish platform accountability through risk assessments and grievance officers. Civil remedies, including fast-track relief and algorithmic demotion of harmful content, will help victims seek justice.

Establishing an independent Data Protection Authority (DPA) by 2026, modeled after Kenya's framework, would oversee telecom and digital platforms. This authority should possess operational and financial independence, a transparent appointment process, and strong investigative powers to regulate cross-border data flows and safeguard ethical data practices. At the same time, protecting freedom of expression is vital. Bangladesh must avoid

censoring legitimate speech under the guise of combating disinformation. Adopting a "Freedom First" policy, protecting whistleblowers, ensuring press independence, and supporting local journalism through innovation funds and tax incentives will uphold media viability. Ensuring control over digital infrastructure is essential. Sensitive data should be hosted on national servers, with investment in local AI and data labeling. An Ethical AI Charter should ensure transparency and fairness, while foreign investments in data-sensitive sectors must be vetted for security.

Most importantly, strengthening international and regional cooperation is crucial, given the cross-border nature of misinformation. Proposed initiatives include a SAARC Digital Resilience Forum for real-time regional disinformation tracking, a South Asia Media Integrity Network for collaborative journalism and verification, and issue-specific dialogues such as the Rohingya Information Corridor and Election "Quiet Hours" Pact. Globally, Bangladesh should lead forums like the Global Partnership on AI and the Freedom Online Coalition, pushing for inclusive governance of digital spaces. Endorsing frameworks like the Paris Call for Trust and Security in Cyberspace will amplify Bangladesh's voice in global digital policymaking. Hosting flagship events in Dhaka-like the UNESCO Digital Literacy Summit (2027) and the Commonwealth Ethical-AI Forum (2028)-will cement Bangladesh's role as a leader in digital ethics, literacy, and AI development. These comprehensive measures are likely to fortify Bangladesh's information environment, ensuring an inclusive, democratic, and resilient digital future while combating misinformation and disinformation.

References

1. Access Now (2023) Bangladesh's DSA amendments must protect free expression and privacy rights. Available at: https://www.accessnow.org/bangladesh-dsa-amendments/

2. Ahmed, S. and Kabir, H. (2021) 'Combating digital disinformation in South Asia: Prospects and challenges for Bangladesh', Asian Journal of Communication, 31(5), pp. 405–422.

3. Ahmed, F., & Khan, S. (2024). Digital Divide and Disinformation in Bangladesh. Dhaka: University Press Limited.

4. Akter, Ema. (2024). J Glob Health 2024. National Library of Science Bangladesh. https://pubmed.ncbi.nlm.nih.gov/39451061/%0 . [Accessed on 20 April 2025].

5. Amnesty International, 2019. Bangladesh 2019. [Online] Available at: https://www.amnesty.org/en/ countries/asia-and-the-pacific/ bangladesh/report-bangladesh/ [Accessed 15 May 2025].

6. Arquilla, J., & Ronfeldt, D. (1997). In Athena's camp: Preparing for conflict in the information age. RAND Corporation.

7. Bangladesh Institute of Business Management. (2023). https://www.bim.org.bd/. [Accessed on 25 April 2025].

8. Banik, S. and Ahmed, M.U. (2022) 'Public-private collaboration in addressing digital threats: The Bangladesh perspective', Information & Security: An International Journal, 53(3), pp. 211–230.

9. Bazzell, M. (2022). Open source intelligence techniques: Resources for searching and analyzing online information (9th ed.). Independently published.

10. BTRC (Bangladesh Telecommunication Regulatory Commission) (2022) Annual Report 2022. Dhaka: BTRC.

11. Chowdhury, N., & Ali, R. (2023). Cross-Border Disinformation: Regional Early Warning Systems. South Asian Journal of Diplomacy, 8(1), 78-95.

12. Chowdhury, T., 2020. Bangladesh using controversial law to 'gag media, free speech'. [Online] Available at: https://www.aljazeera.com/news/2020/05/bangladesh-controversial-law-gag-media-free-speech-200520204441863.html [Accessed 15 May 2025].

13. Digital Security Agency (DSA) (2023) National Cyber Security Strategy of Bangladesh (Draft).

14. Dhaka: Ministry of Posts, Telecommunications and Information Technology.

15. Dismislab, 2025. Misinformation trends and narratives in Bangladesh's tumultuous 2024. [Online] Available at: https://en.dismislab.com/misinformation-trends-and-narratives-in-bangladeshs-tumultuous-2024/ [Accessed 15 May 2025].

16. European Commission (2022) Tackling online disinformation: A European approach. Brussels: European Union.

17. FactWatch (2024) Fighting misinformation in Bangladesh: A data-driven approach. Available at: https://www.factwatchbd.org. [Accessed 17 May 2025].

18. Fact-Watch, 2025. Fact-Watch. [Online] Available at: https://www.fact-watch.org/ [Accessed 15 May 2025].

19. Freedom House, 2017. Freedom on the Net, Bangladesh, Washington D.C. USA: Freedom House.

20. International Telecommunication Union (2021) Digital regulation handbook and platform regulations module. Geneva: ITU.

21. Jachai, 2025. Jachai. [Online] Available at: https://www.jachai.org/ [Accessed 15 May 2025].

22. Ministry of Education Bangladesh (2022) Digital Literacy Curriculum for Schools (Grades 6–8). Available at: https://moedu.gov.bd.

23. NTMC (National Telecommunication Monitoring Centre) (2023) Role of NTMC in digital surveillance and national security. Available at: https://ntmc.gov.bd.

24. Paul, C., & Matthews, M. (2016). The Russian "firehose of falsehood" propaganda model. RAND Corporation.

25. Paul, R. (2022). How China-linked networks spread disinformation about U.S.-Bangladesh-India naval drills. The Diplomat.10 November 2022.

26. Rahman, L. (2023). Empowering Citizens: Public Awareness Campaigns Against Disinformation. Dhaka: Bangladesh Media Institute.

27. Reporters Without Borders, 2009. World Press Freedom Index 2009. [Online] Available at: https://rsf.org/ en/world-press-freedom-index-2009 [Accessed 15 May 2025].

28. Reporters Without Borders, 2020. 2020 World Press Freedom Index. [Online] Available at: https://rsf.org/ en/ranking [Accessed 15 May 2025].

29. Reuters, 2018. Factbox: Bangladesh's broad media laws. [Online] Available at: https://www.reuters.com/article/us-bangladesh-election-media-factbox/factbox-bangladeshs-broad-media-laws-idUSKBN1OC08S/ [Accessed 15 May 2025].

30. Rumor Scanner Bangladesh, 2025. Rumor Scanner Bangladesh. [Online] Available at: https://rumorscanner.com/ [Accessed 15 May 2025].

31. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.

32. The Daily Star. (2022).Bank run of Islami Bank. https://www.thedailystar.net/business/news/crisis-hit-banks-repaying-depositors-emergencies-basic-needs-3725136. [Accessed on 23 April 2025].

33. UNDP Bangladesh (2020) Digital Bangladesh: Leveraging ICT for development. Dhaka: United Nations Development Programme.

34. U.S. Department of Defense (DoD). (2023). *Information operations: Doctrine for the armed forces of the United States (JP 3-13).

35. UNESCO (2023) Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information. Paris: UNESCO.

36. Wardle, C. and Derakhshan, H. (2017) 'Information disorder: Toward an interdisciplinary framework for research and policymaking', Council of Europe Report, pp. 1–107.

37. Woolley, S. C., & Howard, P. N. (2019). Computational propaganda: Political parties, politicians, and political manipulation on social media. Oxford University Press.

38. World Bank (2021) Data for better lives: World Development Report 2021. Washington DC: World Bank.

Keynote Paper-2

ADVANCING NATIONAL SECURITY: INFORMATION AS A NEW SECURITY FRONTIER

Introduction

As the boundaries between the physical and digital worlds continue to blur, the concept of national security has expanded far beyond its traditional military and territorial foundations. In the contemporary era, information emerged as a critical domain of national security, functioning not only as a support mechanism but as a decisive element in protecting state sovereignty and ensuring geopolitical stability (Rid, 2020). Information now plays a dual role, both as a strategic asset and as a threat. On one hand, it empowers national defense by enabling real-time intelligence, informed decision-making, and cross-agency coordination; on the other, it exposes states to new vulnerabilities through cyberattacks, misinformation campaigns, and cognitive warfare (Nye, 2010). This duality has elevated information to a strategic resource that is both operationally indispensable and adversarial targetable, with consequences for military, political, and economic security.

The recognition of "information space" (infospace) as the fifth domain of warfare, alongside land, sea, air, and space, reflects this paradigm shift in how conflicts are conducted and how state power is projected (Nissen, 2015). The rapid growth of digital ecosystems, driven by advancements in artificial intelligence, autonomous systems, and quantum computing, has created an interconnected global environment where control over data flows is often synonymous with strategic advantage (Jensen et al., 2019). In this ecosystem, national security frameworks face unprecedented challenges. According to recent statistics, cyberattacks targeting critical infrastructure have increased dramatically over the past decade, with sectors such as energy, finance, and healthcare being especially vulnerable (Council on Foreign Relations, 2023). Simultaneously, the rise of disinformation campaigns on digital platforms has exposed the psychological dimension of modern warfare, where influencing

public opinion can be as impactful as kinetic force (Vosoughi, Roy & Aral, 2018).

Thus, information serves as both the medium and the message of modern power. Control over the infospace determines not only operational effectiveness in times of conflict but also public trust, international credibility, and long-term political stability. As such, the ability to safeguard and leverage information has become a central focus of national security strategies across the globe (Libicki, 2007). Understanding the transformative impact of information on national security requires recognizing its evolving role as a strategic domain, one that must be defended, regulated, and ethically harnessed in a world where digital threats and opportunities are tightly intertwined.

The Importance of Information in National Security Strategies

In the 21st century, information has evolved from a secondary, support-oriented role into a central pillar of national security strategy. Once limited to aiding military operations, information is now an active force that shapes strategic planning, decision-making, and operational execution (Libicki, 2007). This transformation reflects the growing importance of data-driven intelligence, real-time communication, and digital coordination tools, all of which are fundamental to the defense landscape in an increasingly interconnected world.

Modern national security strategies now integrate cyberspace and information systems as core components, enabling functions such as rapid intelligence gathering, command coordination, and remote operational control. However, these advancements have also introduced new vulnerabilities, as both state and non-state actors exploit digital networks to launch cyberattacks, manipulate information flows, and conduct psychological operations (Rid, 2020). This reality has led to the recognition of "information space" as the fifth domain of warfare, standing alongside land, sea, air, and space (Nissen, 2015). Unlike the traditional domains, info space includes not only technical systems like networks and digital platforms but also cognitive dimensions, such as public perception, media framing, and political narratives. In this domain, conflicts

are not only fought with weapons but with information control, influence campaigns, and disruption of trust in institutions.

A clear example of this can be seen in the role of social media platforms during democratic elections, where disinformation campaigns have emerged as potent threats to political stability. During the 2016 U.S. presidential election, false news stories were found to be 70% more likely to be retweeted than factual ones (Vosoughi, Roy & Aral, 2018). These findings reveal how easily the infospace can be exploited to undermine public trust and institutional legitimacy, without the need for physical confrontation. Taken together, the evolution of information's role in national security, the militarization of infospace, and the operationalization of disinformation reveal a paradigm shift in how modern warfare and security are conceptualized. To respond effectively, governments must adopt holistic, multi-dimensional strategies that combine cybersecurity measures, regulatory frameworks for digital platforms, public resilience initiatives, and ethical governance of information systems.

Tools and Tactics of Information Warfare

Information warfare (IW) involves the strategic employment of both digital technologies and psychological techniques to disrupt or control the information systems, communications networks, and social fabric of an adversary. As capabilities in this field advance, IW has become a crucial factor in contemporary conflicts, encompassing activities such as cyberattacks, manipulation of media narratives, electronic spectrum interference, and protection of classified data.

- **Cyber Warfare in Practice.** Cyber warfare prominently targets a nation's vital infrastructure. A notable example is the 2017 WannaCry ransomware outbreak, which affected numerous sectors worldwide including the UK's National Health Service (NHS), causing widespread disruption of medical services. Another significant incident occurred in 2021 when the Colonial Pipeline, a major US fuel supplier, suffered a ransomware attack that forced a temporary shutdown of fuel deliveries along the East Coast. The company ultimately paid a ransom of $4.4 million to regain control of its systems, underscoring the grave financial and operational consequences of such attacks (CISA, 2021).

- **Psychological Operations.** Psychological operations aim to influence public perception or erode trust in governmental and societal institutions through the dissemination of misleading or emotionally charged content. These operations often utilize automated accounts and coordinated campaigns to rapidly spread false information across social media, severely impacting social stability.
- **Electronic Warfare.** Electronic warfare makes use of the electromagnetic spectrum to disrupt adversary communications and navigation capabilities. Techniques such as jamming and signal spoofing can degrade the effectiveness of military operations. For example, during the ongoing conflict in Ukraine, Russian forces have deployed sophisticated electronic warfare tools to interfere with GPS signals and obstruct battlefield communications, thereby reducing Ukrainian forces' situational awareness (Greenberg, 2018).
- **Operational Security.** Operational security involves safeguarding sensitive information that could be exploited by adversaries. This includes encrypting communications, controlling access to classified materials, and consistently assessing vulnerabilities. Today's best practices encompass multi-factor authentication, endpoint encryption, secure networking, and ongoing cybersecurity training for personnel (Greenberg, 2018).

Major Threats and Vulnerabilities in the Information Domain

With the increasing reliance on digital infrastructure, a range of advanced threats and weaknesses have emerged, from direct cyberattacks to the weaponization of emerging technologies.

- **Cyberattacks on Critical Infrastructure.** Critical sectors, including energy, healthcare, finance, and transportation, are frequent targets of cyberattacks, often through ransomware or malware, which can halt essential services and threaten national stability. The 2021 Colonial Pipeline incident disrupted nearly half of the East Coast's fuel supply and led to public panic (CISA, 2021). Globally, such attacks on critical infrastructure

have escalated markedly in recent years (IBM, 2024). Healthcare facilities remain particularly susceptible due to outdated systems and insufficient security measures.

- **Data Breaches and Information Exposure.** Unauthorized breaches of sensitive government and defense data continue to pose serious risks. In 2023, a significant compromise exposed communications from the U.S. Department of Defense, mainly through phishing and insider threats (IBM, 2024). The proliferation of stolen credentials is a leading cause of data breaches worldwide, highlighting the importance of robust authentication and threat monitoring.

- **Disinformation and Misinformation Campaigns.** Disinformation campaigns actively undermine trust in institutions and manipulate public opinion. Global efforts to spread false information during the COVID-19 pandemic have exacerbated vaccine hesitancy and societal discord. Techniques such as bot networks, deepfake videos, and fabricated news sites are common tools used to amplify falsehoods. Countermeasures involve AI-powered detection, content flagging by platforms, and collaboration with fact-checking organizations (Europol, 2022).

- **Terrorism and Cyber Radicalization.** Terrorist groups exploit encrypted communication apps to facilitate recruitment and coordination. Groups like ISIS have successfully used online propaganda to attract followers, particularly targeting disaffected youth. The anonymity afforded by digital platforms allows such networks to operate globally with reduced risk of detection, necessitating increased cybersecurity awareness and regulatory efforts (Europol, 2022).

Strategic Implications of Information Warfare in National Security

Information warfare introduces strategic risks such as flawed decision-making, delayed crisis response, and diminished trust in intelligence systems. A prime example is the May 2023 Pentagon deepfake incident, where a viral AI-generated video depicting an explosion led to a brief dip in the U.S. stock

market. Such incidents illustrate how quickly misinformation can generate real-world consequences before verification can occur. These vulnerabilities are compounded by policy gaps, including inconsistent enforcement of cybersecurity standards, low digital literacy among personnel, and slow adoption of advanced technologies. Fragmented coordination between agencies and nations further weakens global responses to information warfare. To address these challenges, integrated security strategies are essential. This includes collaboration across military, civilian, and academic sectors-each playing unique roles in detection, education, and innovation. For instance, NATO's CCDCOE unites over 30 countries to exchange intelligence and conduct coordinated cyber exercises (NATO, 2024). Proactive initiatives such as AI-assisted verification chains, real-time misinformation alert systems, and digital literacy programs for policymakers can mitigate these strategic vulnerabilities.

Strengthening National Security in the Information Age

Cybersecurity frameworks are vital for shielding critical infrastructure, improving incident response, and enhancing organizational resilience. Key standards such as the NIST Cybersecurity Framework and ISO 27001 support this by providing structured approaches to risk management and regulatory compliance. When applied, they help organizations shift from reactive to proactive security models. The integration of advanced technologies-AI for real-time threat detection, machine learning for threat prediction, and blockchain for secure audit trails-strengthens this resilience. For example, the implementation of NIST standards in the energy sector has significantly improved recovery from ransomware attacks, while ISO 27001, combined with blockchain, has reduced patient data breaches in the healthcare sector (Obioha et al., 2024). Public-private partnerships are also indispensable. The EU Horizon 2020 cybersecurity PPP mobilized €450 million in public funds and leveraged three times more from industry to develop innovations across energy, health, and finance. Additionally, awareness campaigns play a critical role in digital hygiene. These campaigns have reduced phishing success rates from 32% to 5% in just one year and significantly cut the financial impact of breaches (Ayoola et al., 2024). However, misalignment with policy and under-prioritization of such efforts remain persistent obstacles.

Navigating Ethical Challenges in National Security

The intersection of security and ethics presents enduring challenges. Efforts to safeguard national interests through surveillance, data monitoring, and digital tracking must be weighed against civil liberties and privacy rights. The complexity of this balance is heightened by reliance on cloud computing and advanced technologies. Surveillance tools, while effective, raise concerns about governmental overreach and lack of transparency. Legal and ethical boundaries are often blurred, making accountability essential. Encryption debates highlight this tension vividly. Governments may advocate for backdoor access to encrypted systems to bolster security, but doing so undermines user privacy and may introduce exploitable vulnerabilities. In 2023, 49.21% of compromised websites were found to contain at least one backdoor at the point of infection (Sucuri, 2023). This underscores the risk of persistent unauthorized access even after threats are cleared. Scholars argue that when privacy protections are properly implemented, they actually enhance cybersecurity by reducing the surface area for attacks (Allahrakha, 2023). Therefore, robust ethical governance must guide technology deployment, ensuring that security frameworks are not only effective but also equitable and rights-respecting (Yoo, 2015; Singer and Tushman, 2021).

Conclusion

In conclusion, the evolving role of information as a central pillar of national security highlights its dual nature as both a strategic asset and a potential threat in the digital age. As technological advancements reshape the security landscape, nations must adopt a holistic and forward-looking approach that integrates innovation, strategic foresight, ethical governance, and cross-sector collaboration. Strengthening information security requires not only robust technical infrastructure but also adaptive policies and public resilience to counter disinformation, cyber threats, and cognitive warfare. Ultimately, leveraging information effectively and responsibly is essential to maintaining sovereignty, ensuring stability, and building long-term resilience in an increasingly interconnected and contested infospace.

References

1. Allahrakha, M. (2023). Privacy and Cybersecurity: Strengthening Mutual Protection. London: Privacy Watch Institute.

2. Ayoola, S., Banerjee, P., and Voss, J. (2024). The Impact of Cybersecurity Awareness Campaigns. New York: Global Risk Research.

3. CISA (2021) DarkSide Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks (AA21-131A). Available at: https://www.cisa.gov/aa21-131a [Accessed 8 July 2025].

4. Council on Foreign Relations (CFR) (2023) 'Global Cyberattack Trends', Council on Foreign Relations. [online] Available at: https://www.cfr.org/cyber-operations-tracker [Accessed 11 Jul. 2025].

5. Europol (2022) Online Jihadist Propaganda-2022 in Review. Available at: https://www.europol.europa.eu/publications-events/publications/online-jihadist-propaganda-2022-in-review [Accessed 8 July 2025].

6. Greenberg, A. (2018) Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers. New York: Doubleday. Available at: https://www.penguinrandomhouse.com [Accessed 8 July 2025].

7. IBM (2024) X-Force Threat Intelligence Index 2024. IBM Security. Available at: https://www.ibm.com/security/data-breach/threat-intelligence [Accessed 8 July 2025].

8. Jensen, B.M., Valeriano, B. and Maness, R.C. (2019) Cyber strategy: The evolving character of power and coercion. Oxford: Oxford University Press.

9. Libicki, M.C. (2007) Conquest in cyberspace: National security and information warfare. Cambridge: Cambridge University Press.

10. NATO (2024) Cooperative Cyber Defence Centre of Excellence Strategic Frameworks. Brussels: NATO.

11. Nissen, T.E. (2015) The weaponization of social media: Characteristics of contemporary conflicts. Copenhagen: Royal Danish Defence College.

12. Nye, J.S. (2010) Cyber power. Cambridge, MA: Harvard Kennedy School, Belfer Center for Science and International Affairs.

13. Obioha, F., Al-Zahrani, M. and Chun, Y. (2024) Blockchain and ISO 27001 Implementation in Healthcare. Singapore: Springer.

14. Rid, T. (2020) Active measures: The secret history of disinformation and political warfare. New York: Farrar, Straus and Giroux.

15. Singer, P. and Tushman, M. (2021). Balancing Innovation and Ethics in Security Tech. Cambridge: Harvard Business School Press.

16. Sucuri. (2023) Website Threat Research Report. California: GoDaddy.

17. Vosoughi, S., Roy, D. and Aral, S. (2018) 'The spread of true and false news online', Science, 359(6380), pp.1146–1151. https://doi.org/10.1126/science.aap9559

18. Yoo, C. (2015). Encryption, Security, and Privacy in the Digital Age. Oxford: Oxford University Press.

Rapporteur Report

As part of course curricula of NDC, a lively seminar on 'Advancing National Security and Development: Use of Information as a Powerful Strategic Tool', was conducted jointly by the course members of ND Course 2025 and Bangladesh Institute of Peace and Security Studies (BIPSS). The seminar aimed to facilitate focused learning and discussion on a contemporary topic of interest for Bangladesh. It provides a platform for experts to share knowledge, and for participants to engage in interactive learning through presentations and discussions.

Air Vice Marshal M Mustafizur Rahman, Senior Directing Staff (Air), welcomed the audience at the NDC Hall and outlined the background of the seminar. He noted that the event was the outcome of a organized collaboration between the NDC and the Bangladesh Institute of Peace and Security Studies (BIPSS), which helped finalize the theme and identify four sub-themes: influence operations and targeted influence strategies, the role of generative AI in information warfare, information as a development tool for Bangladesh, and combating misinformation and disinformation. Based on four pre-seminars, the theme and speakers for today were selected. He further informed that two sessions would follow, first by BIPSS on "Advancing National Security: Information as a New Security Frontier," and then by NDC course members on "Information as a Tool for Security and Development: Countering Misinformation and Disinformation."

First Session

The title of the first session was 'Advancing National Security: Information as a New Security Frontier'. Mr. Shafqat Munir, Senior Research Fellow and Head of BCTR at BIPSS, delivered the keynote speech, while Dr. Syed Muntasir Mamun, Director General at Ministry of Foreign Affairs, worked as the Session Chair. The keynote speech offered a comprehensive analysis of information warfare and national security. In summary, his talk covered the importance of information in national security strategy, the tools and tactics of information warfare, major threats and vulnerabilities in the information

domain, the strategic implications of information warfare on national security decisions, ways to strengthen national security in the information age, and the ethical challenges of information security. However, the speaker emphasized that information is now both a core asset and a vulnerability, making it central to national security in the digital era. The information space has become the fifth domain of warfare, expanding conflict beyond traditional physical realms. Digital threats, including cyberattacks, data breaches, disinformation, and deepfakes, can destabilize critical infrastructure and erode public trust. It is of paramount importance to control and protect information that directly influences military, political, and economic outcomes. Rapid technological advancements amplify both opportunities and risks, requiring new strategies and constant adaptation. Integrated, cross-sector approaches and public awareness are crucial in defending against complex, evolving threats. Thus, balancing security, privacy, and ethics is vital to maintaining public trust and effective governance in the information age.

Interactive Session

The interactive session witnessed wide-ranging participation, both from the course members and invitees, with questions, comments, and updates on the topic. A brief summary of the proceedings of the interactive session are enumerated in the following paragraphs.

Commodore Imtiaz, ND Course 2025, highlighted the growing difficulty of distinguishing between real information and fake or deepfake content in today's information age. He stressed the need to curb the spread of harmful information while promoting positive narratives. In this context, he sought clarification on national-level capability gaps and measures in place. The presenter underscored the importance of public awareness, particularly from the school level, by integrating digital literacy and critical thinking into the curriculum. Emphasis was placed on teaching students to verify information, identify credible sources, understand the consequences of false content, and practice responsible online behavior. Encouraging open dialogue on media ethics, he noted, would help shape informed and resilient digital citizens.

Brigadier General Rashid, ND Course 2025, noted that while defensive measures in the digital domain are vital, information also offers offensive potentials, shaping narratives, influencing perceptions, and projecting national values. He asked whether Bangladesh's national security strategies should incorporate a doctrine of proactive information statecraft to leverage values, narratives, and digital tools before adversarial currents take root. In response, the speaker agreed, emphasizing that such a doctrine is essential for countries like Bangladesh in a complex geopolitical setting, though priorities must align with core values and broader diplomatic strategy.

Commodore Moniruzzaman, ND Course 2025, asked, in an age where data and information are expanding exponentially with the rise of AI and Generative AI, how can Bangladesh combat and manage future information threats in such a complex scenario? In response, the speaker noted that Bangladesh could address these challenges by promoting digital literacy, enacting strong data protection laws, and deploying AI-driven monitoring systems. He further emphasized the importance of strengthening institutional capacity and fostering public–private partnerships to build resilience in the digital age.

Brigadier General Shahzad, ND Course 2025, asked how secrecy and privacy could be managed most ethically. In response, the speaker acknowledged the relevance of the question and noted that while managing secrecy and privacy is indeed challenging, it can be achieved ethically through a well-defined legal framework. Citing best practices from Western Countries, he emphasized that such a framework should serve to protect national interests rather than enable abuse of power. He further highlighted procedural measures such as informed consent, limiting unnecessary data collection, enforcing strict access controls, and ensuring secure data handling to minimize secrecy and privacy concerns.

Colonel Yusuf, ND Course 2025, from Saudi Arabia, inquired about the rationale behind governments' banning various apps during conflicts and emergencies. In response, the speaker explained that governments often restrict or ban social media, messaging platforms, or live-streaming services in such situations for reasons of security, stability, and governance. In conflict zones, for instance, the real-time sharing of videos or troop movements can

compromise military operations and provide adversaries with an intelligence advantage. Similarly, during domestic emergencies, the rapid spread of misinformation can fuel panic and instability, justifying temporary restrictions. However, temporary restrictions must be justified with extreme security needs.

The Defence Attache of Australia in Bangladesh inquired about the progress of incorporating misinformation and disinformation into the legal framework. In response, the speaker stressed the importance of such a framework, noting that in the past it was often misused to suppress opposition views. He added that revisions are currently underway in different sections of the Cyber Security Act to broaden its scope, and expressed optimism that the updated framework would be enacted soon.

Brigadier General Azim, ND Course 2025, observed that the information space has become the fifth domain of warfare, crossing boundaries, and where actors engage without using bullets. He questioned what short- and long-term strategies the Government of Bangladesh should develop in collaboration with military and civil experts to effectively harness opportunities and defend against threats in this domain. In response, the speaker highlighted the importance of creating an overarching doctrine, clarifying future roles, and promoting Bangladesh's achievements through strategic narratives. As immediate steps, he proposed establishing a joint civil–military task force for information monitoring and rapid response. For the long term, he advised developing a national information doctrine, investing in AI-driven capabilities, and enhancing public resilience through education and digital infrastructure.

Second Session

The title of the second session was 'Information as a Tool for Security and Development: Countering Misinformation and Disinformation'. Air Vice Marshal Mahmud Hussain, BBP, OSP, ndc, psc, acsc, GD(P) (Retired), Distinguished Expert, Bangladesh Aviation and Aerospace University, served as the Session Chair. The Chair began his talk by expressing his deepest gratitude to the Commandant and the National Defence College for organising this important seminar. This seminar is exceptionally well-timed, taking place at a

moment of profound transition when information is no longer just a means of communication but a strategic arena of competition. The world, which is forming in an individual's mind and imagination, will probably not view information as anything different from its very existence. Perhaps it has always been thus. As cyber narratives clash with diplomatic truths, and perceptions become as powerful as physical presence, the information domain emerges as the newest and arguably most volatile frontier of security and strategy.

In today's interconnected world, national security faces growing threats not only from conventional warfare but also from narrative intrusion, digital disinformation, and algorithm-driven influence. These forces shape a new battlespace where information itself becomes a weapon. The Chair emphasized the urgent need to reevaluate coordination among government, industry, civil society, and academia in order to counter these challenges. Given the speed of influence operations, Bangladesh must adopt innovative, real-time mechanisms for collaboration. The goal is clear: to defend truth from manipulation, safeguard sovereignty from interference, and strengthen public trust in institutions.

Joint Secretary Lubna, ND Course 2025, set the tone for the seminar, focusing on the conceptual foundation and the use of information in the global context. The discussion highlighted how the global landscape is increasingly shaped by the pervasive spread of disinformation and misinformation, with their classification by intent, format, and target audience forming the core of the talk. Information disorder, encompassing misinformation, disinformation, and malinformation, carries profound strategic implications both globally and domestically. At the geopolitical level, it can manipulate public opinion, destabilize nations, influence elections, and is often integrated into cyber warfare alongside hacking and espionage to threaten national security. Domestically, false narratives can deepen ideological divides, spark unrest and political instability, disrupt financial markets, influence consumer behavior, and damage corporate reputations.

Brigadier General Naim, ND Course 2025, emphasized in his speech the significant effect of misinformation and disinformation on Bangladesh's national security and development. He highlighted that accurate information is

essential for security, as it enables the government to anticipate threats, prevent cyberattacks, and respond effectively to crises, while also supporting economic growth, innovation, and good governance. However, misinformation presents serious dangers in three areas: in the military, it damages trust, morale, civil-military relations, and international credibility through leaks, cyber infiltration, and manipulation; in the economy, it destabilizes financial systems, reduces investor confidence, and exploits communication and cybersecurity gaps, especially during crises or transitions; and in society, it weakens social cohesion by increasing divisions along ethnic, religious, or ideological lines.

Brigadier General Shahzad Parvez, ND Course 2025, presented an analytical overview of strategies and interventions to counter the impact of misinformation and disinformation on Bangladesh's national security and development, focusing on national capacity and institutional response. He reviewed existing measures, including fact-checking, legal frameworks, technological tools, media literacy, surveillance, and international cooperation, noting both successes and gaps. While independent fact-checking platforms like BFC, Rumor Scanner, and Fact Watch play a role, they lack sufficient reach and integration with mainstream media. Media literacy remains weak due to low awareness, declining trust in traditional outlets, and limited rural outreach, despite some government-led programs. Legal frameworks, including the ICT Act, Digital Security Act, and the newly introduced Cyber Security Ordinance 2025, aim to address cybercrimes and misinformation but face criticism for restricting freedom of expression and privacy, underscoring the need for a balanced approach. Finally, he highlighted the importance of robust international cooperation, shared definitions, and regional frameworks to effectively address this transnational challenge.

Brigadier General Raisul, ND Course 2025, stressed that in today's digital era, information is a source of influence, power, and vulnerability, with misinformation and disinformation threatening democracy, fueling tensions, and obstructing development. To counter these risks, he proposed a six-step strategy, which are,integrated approach through a National Information Resilience Council (NIRC) bringing together government, media, academia, tech platforms, and civil society, enhancing digital and media literacy

by introducing critical media skills in schools, online courses, and nationwide training programs, public-private partnerships for AI-driven monitoring and a national early warning system, strengthening legal frameworks by refining the Digital Security Act, ensuring transparency, and appointing grievance redress officers, safeguarding freedom of expression with a "freedom first" doctrine and stronger Right to Information protections; and regional and international cooperation through cross-border newsroom hotlines, a UNESCO Digital Literacy Summit in 2027, and a Commonwealth ethical-AI forum in 2028.

Interactive Session

A brief summary of the proceedings of the interactive session of the second session is enumerated in the following paragraphs:

Brigadier General Mazhar, ND Course 2025, questioned whether the Draft Cyber Security Act 2025 could balance freedom of speech and citizens' digital security. One of the speakers responded that the draft law, which has been widely debated in Bangladesh, aims to address criticisms of the 2018 and 2023 Acts by removing controversial sections and adding clearer provisions. He recognized it as progress in protecting digital rights but stressed that its success will depend on transparent implementation, strong judicial oversight, and safeguards against misuse. He further emphasized that the government should focus on these aspects to ensure the Act becomes a practical and effective policy.

Brigadier General Masud, ND Course 2025, raised the question of whether regional cooperation in the domain of information warfare is feasible, given that many countries are engaged in ongoing conflicts and strategic or ideological rivalries. One of the speakers responded that Bangladesh could still pursue cooperation through bilateral and multilateral agreements built on confidence-building measures, shared threat assessments, and forums focused on cyber norms, misinformation control, and capacity building. He emphasized that prioritizing common interests such as regional stability, counterterrorism, and digital resilience would make such cooperation achievable despite existing challenges.

Barrister Khalil, ND Course 2025, asked what proactive measures could be devised to address the growing challenges of misinformation and disinformation. In response, one of the speakers emphasized the importance of nationwide awareness through public education campaigns, along with the role of NTMC or the proposed NIRC in technically identifying false content. He added that dedicated expert teams should analyze emerging trends and patterns to ensure timely detection and the implementation of effective countermeasures.

Colonel Richard, ND Course 2025 from Uganda, asked what measures could be taken in regions like Africa, which are lagging in information security and effective information dissemination. In response, one of the speakers suggested promoting digital awareness, supporting information entrepreneurship similar to Bangladesh's Grameenphone model, and developing secure, community-based communication networks to use information effectively for security and development.

The Session Chair concluded the seminar on 'Information as a tool for Security and Development: Countering Misinformation and Disinformation' by expressing gratitude to all speakers for their insightful and well-researched contributions. He emphasized that the lines between just and unjust are increasingly blurred in today's complex information environment. Addressing these challenges requires long-term structural reforms in Bangladesh. He stressed the importance of promoting media literacy, institutionalizing fact-checking mechanisms, and leveraging the transformative potential of generative AI as key tools in safeguarding national security and fostering sustainable development.

Participants of the Seminar

Faculty and Staff Officers

Ser	Rank and Name	Appointment
1.	Lieutenant General Mohammad Shaheenul Haque, OSP, BSP, ndc, hdmc, psc	Commandant
2.	Major General (Now Lieutenant General) Khan Firoz Ahmed, OSP, ndc, afwc, psc (LPR)	Senior Directing Staff (Army)
3.	Major General Md Hakimuzzaman, SGP, ndc, afwc, psc	Senior Directing Staff (Army)
4.	Major General Md Moshfequr Rahman, BSP, SGP, SUP, ndc, psc (Retired)	Senior Directing Staff (Adjunct-2)
5.	Major General Md Rashed Amin, rcds, ndc, psc (Retired)	Senior Directing Staff (Adjunct-1)
6.	Rear Admiral A K M Jakir Hossain, ndc, afwc, psc	Senior Directing Staff (Navy)
7.	Air Vice Marshal M Mustafizur Rahman, BSP, GUP, nswc, afwc, psc, GD(P)	Senior Directing Staff (Air)
8.	Additional Secretary Yasmeen Parveen, ndc	Senior Directing Staff (Civil)
9.	Brigadier General Mamun Ur Rashid, ndc, afwc, psc	Chief Instructor
10.	Brigadier General Md Mostafizur Rahman, ndc, hdmc, afwc, psc, PhD	Directing Staff (Army-1)
11.	Brigadier General Md Nishatul Islam Khan, ndc, afwc, psc	College Secretary
12.	Brigadier General Azaher Uddin Ahmmed, nswc, afwc, psc	Directing Staff (Army-2)
13.	Brigadier General Md Kamrul Hasan, BPM, PPM, ndc, afwc, psc	Directing Staff (Army-3)
14.	Brigadier General Md Syeedur Rahman, ndc, afwc, psc	Directing Staff (Army-4)
15.	Brigadier General Syed Mohammad Nurus Saleheen Yousuf, PPMS, ndc, afwc, psc	Directing Staff (Army-5)

Ser	Rank and Name	Appointment
16.	Brigadier General Md Mahmudur Rahman Minhaz, SUP, afwc, psc	Directing Staff (Army-6)
17.	Commodore Ziaur Rahman, (TAS), NGP, ndc, afwc, psc, BN	Directing Staff (Navy-1)
18.	Air Commodore Imranur Rahman, BUP, afwc, psc, GD(P)	Directing Staff (Air-1)
19.	Colonel Mohammad Saifullah Mirazul Alam	Colonel Administration
20.	Colonel (Now Brigadier General) Sufi Mohammad Moinuddin, SUP, afwc, psc	Directing Staff (Army-7)
21.	Colonel (Now Brigadier General) Omar Bin Masud, afwc, psc, G+	Directing Staff (Army-8)
22.	Colonel Muhammad Nurul Amin, BSP, afwc, psc	Director, Research & Academic
23.	Captain Mohammad Manzur-Ul-Karim Chowdhury, (H1), BSP, BCGM, psc, BN	Colonel General Staff
24.	Captain Mohammad Farhad Hossain, (ND), afwc, psc, BN	Directing Staff (Navy-2)
25.	Group Captain B M Hasan Mahmud, afwc, psc, GD(P)	Directing Staff (Air-2)
26.	Lieutenant Colonel Hasan Mohammad Tanvir Imtiaz, Inf	General Staff Officer-1 (Administration)
27.	Lieutenant Colonel Muhammad Shahjada Omar Habib, psc, Inf	General Staff Officer-1 (Training)
28.	Lieutenant Colonel GM Mamunur Rashid, psc, G+, AD	Senior Research Fellow-2
29.	Lieutenant Colonel Md Sabbir Hasan, afwc, psc, Inf	General Staff Officer-1 (AFWC)
30.	Lieutenant Colonel Md Badrul Ahsan Khan, afwc, psc, Engrs	Senior Research Fellow-1
31.	Major Mohammad Saiful Islam, Sigs	General Staff Officer-2 (Network Administrator)
32.	Major A K M Hasibul Hossain Nabi, ASC	Messing Officer

Ser	Rank and Name	Appointment
33.	Major Md Hasib Bin Nuruddin, ASC	Mechanacal Transport Officer
34.	Major Mohammad Razibul Alam Bhuiyan, psc, Inf	Company Commander
35.	Major Dewan Mohammad Moktadir, SPP, psc, Inf	General Staff Officer-2 (Army), AFWC
36.	Major Md Sumon Reza, Inf	General Staff Officer-2 (Administration)
37.	Major Md. Mursalin Ibne Siddique, psc, Inf	Quarter Master
38.	Major Md Nurul Kamal, Engrs	General Staff Officer-2 (Accounts)
39.	Major Md. Iftekhar Abedin, Engrs	Coordinator (SDS Army-1)
40.	Major Akib Ahsan Teas, psc, Inf	General Staff Officer-2 (Coordinator)
41.	Major Sayad Shahriar Khaleque, psc, Inf	General Staff Officer-2 (Planning & Coordination)
42.	Major M. K. Habib, Inf	General Staff Officer-2 (Staff Duties)
43.	Major Tahsin Alam, Inf	Coordinator (SDS Army-2)
44.	Lieutenant Commander (Now Commander) Shanjida Hossain, (Edn)(C), psc, BN	General Staff Officer-2 (Training Support)
45.	Lieutenant Commander Mustafa Sharif Khan, (Edn)(G), BN	General Staff Officer-2 (Navy), AFWC
46.	Squadron Leader Mokarram Hossain, Edn	General Staff Officer-2 (Protocol)
47.	Squadron Leader Md Muttakin Rahman	General Staff Officer-2 (Air), AFWC
48.	Captain Mahmud Emtiaj Rasel, AC	Staff Captain
49.	Lieutenant Raihanul Kabir, (S), BN	ADC to Commandant

Ser	Rank and Name	Appointment
50.	Flight Lieutenant Md. Sahab-Ur-Rahman, GD (P)	Coordinator (SDS Air)
51.	Sub Lieutenant Ashraful Alam, (S), BN	Coordinator (SDS Navy)
52.	Senior Assistant Secretary Nushrat Ara Khanam	Research Coordinator
53.	Assistant Professor (Political Science) G.M. Shakur	Research Fellow
54.	Assistant Director Md Nazrul Islam	Assistant Director (Library)
55.	Assistant Programmer Md Azad Rahaman Munna	Assistant Programmer

Course Members of National Defence Course-2025

International Course Members			
Ser	**Rank**	**Name**	**Country**
1.	Senior Colonel	Li Bowen	China
2.	Colonel	Comoe Assande Celestin	Cote D'Ivorie
3.	Brigadier	Jitesh Ralli	India
4.	Air Commodore	Rajesh Varma VM F(P)	India
5.	Air Commodore	Raman Goel VM F(P)	India
6.	Commodore	Pramod George Thomas	India
7.	Colonel	Ahmad Muttaqin, S.Sos., M.I.P.	Indonesia
8.	Colonel	Madi Irhail Rashed Al Sarhn	Jordan
9.	Brigadier General	Za'al Abdel Wahab Ismail Almajali	Jordan
10.	Colonel	Francis Sichei Cheret	Kenya
11.	Commander	Mubarak Ghanem Al Nahari	KSA
12.	Colonel	Hashan bin Monahy Al Natify	KSA
13.	Colonel	Fahad bin Ali Al Shabanat	KSA
14.	Colonel	Yousef Ahmed Alsufyani	KSA
15.	Colonel	Mohammed Fahad Al Mdaimegh	KSA
16.	Brigadier General	Meshal M E M A Alsaleh	Kuwait
17.	Colonel	Talal A M A Eisa	Kuwait

Ser	Rank	Name	Country
18.	First Admiral	Mohd Shariman Bin Ishak	Malaysia
19.	Colonel	Mohamed Ismail Kanoute	Mali
20.	Colonel	Sanjit Shrestha Sinnya	Nepal
21.	Colonel	Jerry Kantiok Maigari	Nigeria
22.	Colonel	Tajudeen Ajibola Lamidi	Nigeria
23.	Colonel	Mohamed Ali Said Al Kharusi	Oman
24.	Commodore	Imtiaz Ahmed	Pakistan
25.	Brigadier	W M P W N D B Weerakoon, RSP, USP	Sri Lanka
26.	Commodore	L C Vithanage	Sri Lanka
27.	Captain	Raphael Edward Katole	Tanzania
28.	Colonel	Richard Obura Kidega	Uganda
29.	Colonel	Paul Sapezo	Zambia

Bangladesh Army		
Ser	**Rank**	**Name**
1.	Brigadier General	S M Rakibullah, afwc, psc, lsc, M Phil
2.	Brigadier General	Abu Haya Md Masud, psc
3.	Brigadier General	Mohammad Kaiser Rashid Chowdhury, psc, G
4.	Brigadier General	Mohammad Nazmul Haque, BSP, afwc, psc
5.	Brigadier General	Mohammad Moniruzzaman Jewel, psc
6.	Brigadier General	Md Mamunur Rashid, afwc, psc
7.	Brigadier General	M Imran Hamid, BSP, SPP, afwc, psc
8.	Brigadier General	S M Merazul Islam, afwc, psc
9.	Brigadier General	Abul Hasnat Mohammad Sayem, BGBMS, afwc, psc, M Phil
10.	Brigadier General	Md Kamal Uddin Komol, psc
11.	Brigadier General	Md Mahbubul Haque, afwc, psc
12.	Brigadier General	Mohammad Nawroz Nichoshier, psc, G
13.	Brigadier General	Mohammad Saif Ullah, psc
14.	Brigadier General	Amirul Azim, psc
15.	Brigadier General	Muhammad Romeo Nowreen Khan, psc
16.	Brigadier General	Mohammad Raisul Islam, afwc, psc
17.	Brigadier General	Khondoker Shahriar Sabbir, psc

Ser	Rank	Name
18.	Brigadier General	Mamunur Rashid, psc
19.	Brigadier General	Md Mizanur Rahman, psc
20.	Brigadier General	Md Mozahidul Islam, psc, G
21.	Brigadier General	Md Abdullah Al Mamun, afwc, psc
22.	Brigadier General	Shahzad Pervez Mohiuddin, afwc, psc
23.	Brigadier General	Md Anwarul Kabir, afwc, psc
24.	Brigadier General	Sohel Hasan, SGP, psc
25.	Brigadier General	Mohammed Mazhar Al Kabir Khokan, afwc, psc
26.	Brigadier General	Mohammad Touhidur Rahman, psc
27.	Brigadier General	Mohammad Mahbubul Alam, BPMS, PPM, afwc, psc
28.	Brigadier General	Mohammad Shahed Chowdhury, SPP, psc
29.	Brigadier General	Md Iftekharul Mabud, afwc, psc
30.	Brigadier General	Shahriar Kabir, afwc, psc
31.	Brigadier General	SM Naimul Haque, psc
32.	Brigadier General	Md Abdul Jalil, afwc, psc
33.	Brigadier General	A K M Kayes, SGP, afwc, psc
34.	Brigadier General	Md Anwar Uz Zaman, BPMS, PPM, afwc, psc, G
35.	Brigadier General	K M Obaydul Haque, afwc, psc
36.	Brigadier General	Md Jahangir Alam, psc
Bangladesh Navy		
37.	Commodore	S M Sharif-Ul Islam, (N), NPP, PCGM, PCGMS, psc, BN
38.	Commodore	M Nazmul Hassan, (N), NPP, BCMG, PCGMS, afwc, psc, BN
39.	Commodore	A H M Rafiqul Islam, (E), NUP, psc, BN
40.	Commodore	Masudul Karim Siddique, (G), BSP, PCGM, BCGMS, ncc, psc, BN
41.	Commodore	M Fazlar Rahman, (C), BSP, psc, BN
42.	Commodore	S M Maniruzzaman, (L), NUP, psc, BN
43.	Commodore	Md Mahbub-Ul-Hakim, (S), psc, BN
Bangladesh Air Forces		
44.	Air Commodore	Md Rafiul Huq, BSP, BPP, afwc, psc, ADWC
45.	Air Commodore	Mohammad Saifuddin, GUP, psc, GD(P)

Ser	Rank	Name
46.	Air Commodore	Md Quamrul Ershad Matin, GUP, afwc, psc, GD(P)
47.	Air Commodore	Md Sajjad Hossain, BUP, afwc, psc, ATC
48.	Air Commodore	Raahim Mahmood, BPP, fawc, psc, GD(P)
49.	Air Commodore	Abdullah-Al-Masud, GUP, afwc, psc, GD(P)
50.	Air Commodore	Mohammad Sultan Mahmud Malik, psc, Engg
Bangladesh Civil Service		
51.	Joint Secretary	Ms Rokeya Khaton
52.	Joint Secretary	Mohammad Abdullah Al Mamun
53.	Joint Secretary	Ms Khaleda Akhtar
54.	Joint Secretary	Ms Shahida Sultana
55.	Joint Secretary	Md. Doulutuzzaman Khan
56.	Joint Secretary	Dr. Mohammad Azizul Haque
57.	Joint Secretary	Shah Momin
58.	Joint Secretary	S M Nazrul Islam
59.	Joint Secretary	Lubna Siddique
60.	Joint Secretary	A.T.M. Abdullahel Baki
61.	Joint Secretary	Md Asaduzzaman
62.	Joint Secretary	Dr. Kazi Kamrun Nahar
63.	Joint Secretary	Barrister Md Khalilur Rahman Khan
64.	Director General	Ms. Shanchita Haque
65.	Commissioner	Abul Bashar Md. Shafiqur Rahman
66.	Deputy Inspector General	Mr. Basudev Banik
67.	Deputy Inspector General	Mr. Mahfuzur Rahman, BPM (BAR)
68.	Deputy Director General	Shah Ahmed Fazley Rabby

Invited Guests

Ser	Name	Rank and Organization
1.	Syeda Rizwana Hasan	Honourable Adviser Ministry of Environment, Forest and Climate Change and Ministry of Water Resources
2.	H.E Park Young Sik	Ambassador Embassy of Republic of Korea in Bangladesh
3.	Brigadier M. Imran Yousaf Choudry	Defence Adviser Pakistan High Commission in Bangladesh
4.	Captain VS Chauhan	Naval Adviser Indian High Commission in Bangladesh
5.	Alberto Giovanetti	Counsellor, Head of Political, Economic & Culture Affaires Embassy of Switzerland in Bangladesh
6.	Mr. Uttam Kumar Shahi	Director BIMSTEC Secretariat
7.	Commander Glenn Suffolk	Defence Attache Australian High Commission in Bangladesh
8.	Mr. Sujit Sarker	Political Officer Australian High Commission in Bangladesh
9.	Justice A K M Abdul Hakim	Chairman Bangladesh Press Council
10.	Major General A N M Muniruzzaman, ndc, psc (Retired)	President Bangladesh Institute of Peace and Security Studies
11.	Major General Md Shahidul Haque, psc (Retired)	Former Defence Attache to Myanmar & Former Ambassador to Libya

Ser	Name	Rank and Organization
12.	Major General Iftekhar Anis, BSP, awc, afwc, psc, PEng	Director General Bangladesh Institute of International and Strategic Studies
13.	Major General Md Mahbub-ul Alam, BSP, ndc, afwc, psc, M Phil, PhD	Vice Chancellor Bangladesh University of Professionals
14.	Air Vice Marshal Mahmud Hussain, BBP, OSP, ndc, psc, acsc, GD(P), PhD (Retired)	Distinguished Expert Bangladesh Aviation and Aerospace University
15.	Nuzhat Yasmin	Additional Secretary Ministry of Education
16.	A N M Moinul Islam	Additional Secretary Ministry of Public Administration
17.	Brigadier General Shahedul Anam Khan, ndc, psc (Retired)	Associate Editor The Daily Star
18.	Brigadier General Mohammad Shahiduzzaman Khan, ndc, afwc, psc	Dean, Centre for Higher Studies and Research Bangladesh University of Professionals
19.	Professor Dr. A K Enamul Haque	Director General Bangladesh Institute of Development Studies
20.	Dr. Syed Muntasir Mamun	Director General, International Trade, Investment and Technology Wing Ministry of Foreign Affairs
21.	Md. Obaidul Haque	Associate Professor, Department of International Relations University of Dhaka
22.	Ms. Shameem Ara Sheuli	Country Director Inter News

Ser	Name	Rank and Organization
23.	Major Nisar Ahmed (Retired)	Political and Economic Advisor High Commission of Canada in Bangladesh
24.	Ms. Mohosina Mostofa Mity	Bangladesh Institute of Peace and Security Studies
25.	Mr. Shamshil Arefin	Bangladesh Institute of Peace and Security Studies

Coordinators

Ser	Name	Rank	Remarks
1.	Air Vice Marshal M Mustafizur Rahman, BSP, GUP, nswc, afwc, psc, GD(P)	Senior Directing Staff (Air)	Seminar Sponsor SDS
2.	Brigadier General Md Nishatul Islam Khan, ndc, afwc, psc	College Secretary	Chief Coordinator
3.	Colonel Muhammad Nurul Amin, BSP, afwc, psc	Director, Research and Academic	Coordinator
4.	Lieutenant Colonel Md Badrul Ahsan Khan, afwc, psc, Engrs	Senior Research Fellow-1	Associate Coordinator
5.	Major Sayad Shahriar Khaleque, psc, Inf	General Staff Officer-2 (Planning and Coordination)	Assistant Coordinator
6.	Senior Assistant Secretary Nushrat Ara Khanam	Research Coordinator	Assistant Coordinator
7.	Md Nazrul Islam	Assistant Director (Library)	Assistant Coordinator

National Defence College
Mirpur Cantonment, Dhaka, Bangladesh
www.ndc.gov.bd