



## **Military and Modern Warfare**

Strategic Shifts, Technological Innovations, and Bangladesh's Security Challenges

*Mohammad Fakhru Salam*

22 May 2026

<https://doi.org/10.36304/ExpwMCUP.2026.06>

**Abstract:** Modern warfare is undergoing a profound transformation driven by the convergence of autonomous systems, electronic warfare, and data-intensive operations. For Bangladesh, situated in the strategically contested Bay of Bengal, managing the protracted Rohingya crisis and facing escalating climate vulnerabilities, these shifts present immediate and complex security challenges. This article argues that Bangladesh must adopt an agile, human-centered, and technology-enabled security posture, operationalized through a "Defend-Deter-Protect" framework. Human-centered security is defined as

---

Dr. Mohammad Fakhru Salam is an associate professor in the Department of Political Studies at Shahjalal University of Science and Technology, Bangladesh. His research interests include foreign policy, geopolitics, security studies, political sociology, and governance in South Asia. His recent scholarship examines strategic competition in the Indo-Pacific, Bangladesh's foreign policy challenges, military transformation, and the implications of emerging technologies for modern warfare and national security. Dr. Salam has also published on environmental governance, political ecology, and community participation, with a broader focus on state, power, and development in Bangladesh. <https://orcid.org/0000-0002-6135-678>. The views expressed in this article are solely those of the author. They do not necessarily reflect the opinions of Marine Corps University, the U.S. Marine Corps, the Department of the Navy, or the U.S. government.

prioritizing civilian protection, disaster resilience, and livelihood stability alongside conventional defense objectives. Drawing on a qualitative synthesis of recent strategic and policy literature (2023–25), the study analyzes three interrelated dimensions: evolving patterns of modern warfare, technological innovations reshaping operational environments, and Bangladesh’s emerging security challenges. It demonstrates that effective security for Bangladesh lies not in high-cost, platform-centric modernization, but in cost-effective, scalable capabilities including unmanned systems, maritime domain awareness, counterunmanned aircraft systems, cyber resilience, and climate security integration. The article concludes by proposing a prioritized and resource-sensitive policy roadmap that enhances strategic autonomy through diversified partnerships and strengthened domestic capacity, offering a pragmatic pathway for small-state security in the Indo-Pacific.

**Keywords:** Bangladesh, modern warfare; drones, electronic warfare, Indo-Pacific, Bay of Bengal, climate security, Rohingya, counterunmanned aircraft systems, replicator

The global order lacks a central authority, prompting nations to prioritize their security, often leading to mistrust and conflicts.

~ Al Amin<sup>1</sup>

## **Introduction**

Bangladesh faces a rapidly evolving and deeply entangled security environment shaped by three converging pressures: intensifying great power competition in the Indo-Pacific, the rapid diffusion of disruptive military

technologies, and escalating nontraditional threats, including climate disasters and protracted displacement crises. Positioned along the Bay of Bengal and adjacent to the instability in Myanmar, Bangladesh must simultaneously navigate maritime insecurity, humanitarian vulnerability, and strategic competition among larger powers. These pressures are not abstract; they are lived realities that increasingly blur the boundaries between defense, development, and human survival.

At the same time, the character of warfare is undergoing a profound transformation. A decade of uninterrupted growth pushed global military spending to \$2.718 trillion USD in 2024, marking the sharpest rise in decades.<sup>2</sup> However, rising expenditure alone does not capture the scale of change. Conflicts from Ukraine to the Red Sea and across the Indo-Pacific reveal a battlespace shaped by autonomous systems, electronic warfare, real-time data networks, and commercial satellite infrastructures. Low-cost technologies such as first-person-view (FPV) drones now produce disproportionate battlefield effects, compressing innovation cycles and redefining the cost logic of war. These developments are rapidly diffusing into regions like South Asia, where fragile borders, dense coastal zones, and climate vulnerabilities amplify their impact.

For Bangladesh, this evolving landscape presents a critical strategic dilemma. The country's security agenda is already stretched by cross-border spillovers from Myanmar, rising maritime insecurity in the Bay of Bengal, and the long-term management of nearly 1 million Rohingya refugees. In such a context, reliance on traditional, platform-centric models of military modernization is increasingly inadequate.

This article argues that Bangladesh must instead adopt an agile, human-centered, and technology-enabled security posture, operationalized through a “Defend–Deter–Protect” framework. Human-centered security, as used here, prioritizes the protection, resilience, and well-being of individuals and communities measured through disaster response effectiveness, civilian protection, livelihood security, and equitable resource allocation rather than focusing exclusively on state-centric military metrics. This conceptualization shifts the focus from the accumulation of hardware to the outcomes that security policies produce in people’s lives.

Within this framework, *defense* is understood not merely as territorial protection but as the resilience of critical infrastructure and digital systems; *deterrence* is grounded in cost-effective and scalable capabilities that raise the threshold of aggression without triggering destabilizing arms races; and *protection* places civilian security, climate adaptation, and social stability at the center of national security strategy. Crucially, technological modernization is not treated as an end but is evaluated in terms of its contribution to these human-centered outcomes, whether in reducing civilian vulnerability, improving disaster response, or safeguarding coastal livelihoods. By doing so, the apparent tension between technological advancement and human security is resolved through an integrated and outcome-oriented approach.

The analysis proceeds in four stages. It first develops a streamlined theoretical framework that brings together technological transformation, the security dilemma, and human-centered security. It then examines the strategic and technological shifts reshaping contemporary warfare before situating these dynamics within Bangladesh’s specific security challenges.

The article concludes by advancing a policy roadmap that prioritizes cost-effective, scalable, and context-sensitive capabilities such as uncrewed systems, maritime domain awareness, counterunmanned aircraft systems (UAS) architecture, resilient communications, and climate-security preparedness while leveraging Bangladesh's Indo-Pacific Outlook (2023) to maintain strategic autonomy through diversified partnerships and strengthened domestic capacity.<sup>3</sup>

In an era in which security is increasingly defined by the ability to manage complexity rather than accumulate power, Bangladesh's future lies in building a security architecture that is not only technologically adaptive but fundamentally anchored in the protection and resilience of its people.

### **Theoretical Framework**

This study adopts an integrated theoretical framework to analyze Bangladesh's evolving security challenges within the broader transformations of contemporary warfare and the Indo-Pacific strategic environment, aiming to inform both scholarly understanding and policy guidance. Rather than assembling multiple theories in parallel, the framework is deliberately streamlined around three analytically complementary lenses: technological transformation, the security dilemma in a small-state context, and human-centered security. This approach enhances conceptual clarity while ensuring direct alignment with the article's central argument.

The first lens focuses on technological transformation, drawing on insights from the literature on the revolution in military affairs and network-centric warfare. Contemporary conflicts increasingly reflect a shift from

platform-centric models toward information-dominant, networked operations in which battlefield effectiveness depends on integrating sensors, decision-making systems, and precision-strike capabilities. Autonomous systems, artificial intelligence (AI), and electronic warfare have compressed decision cycles and expanded the battlespace into cyber and cognitive domains. For Bangladesh, these developments do not imply the need for full-spectrum technological parity with major powers. Rather, they highlight the strategic value of cost-effective, scalable, and adaptive capabilities, particularly uncrewed systems, maritime surveillance technologies, and resilient communication infrastructures. In this sense, technological transformation is not treated as a driver of militarization but as a means of enhancing operational efficiency within resource constraints.

The second lens is grounded in the concept of the security dilemma, which underscores how efforts by one state to enhance its security can inadvertently generate insecurity among others. In the Indo-Pacific, where strategic competition among India, China, and the United States continues to intensify, Bangladesh operates within a structurally constrained environment defined by asymmetric power relations. For a small state, large-scale military expansion risks provoking regional suspicion and escalation, while insufficient investment in security capabilities exposes critical vulnerabilities. Bangladesh's strategic behavior can therefore be understood as a cautious and prudent adaptation, seeking to avoid entrapment in great power rivalry while maintaining regional stability. This approach aims to foster confidence and strategic restraint among regional actors, reassuring security analysts and policymakers of Bangladesh's responsible posture.

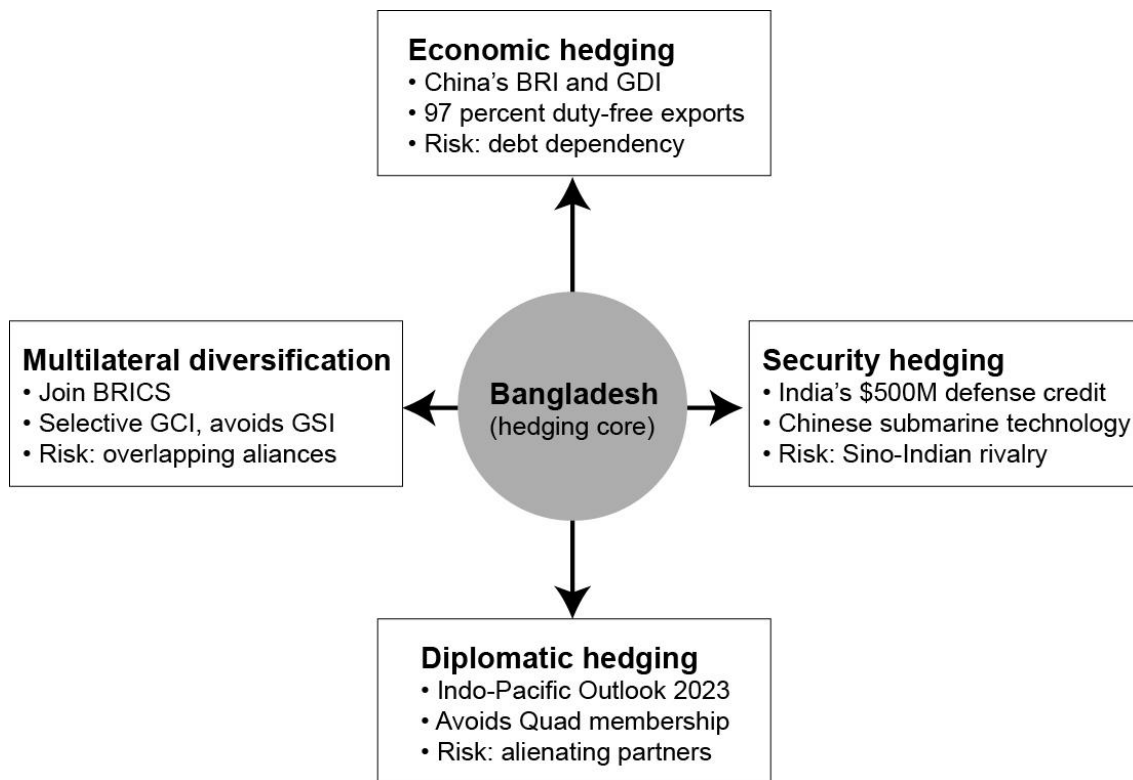
The third and central lens is human-centered security, which expands the scope of security beyond territorial defense to include the protection and resilience of individuals and communities. Building on the definition established in the introduction, this study treats human-centered security as the primary evaluative criterion for assessing technological and strategic choices. In Bangladesh, this perspective is particularly salient, as external threats, climate-induced disasters, protracted displacement, maritime livelihood vulnerabilities, and internal governance challenges shape the country's security landscape. Security policy, therefore, must be evaluated in terms of its capacity to reduce civilian vulnerability, strengthen disaster response and recovery, sustain fragile livelihood systems, and ensure equitable allocation of limited resources.

Within this framework, technological modernization is not treated as an end in itself. Rather, it is assessed by its contribution to human-centered outcomes, such as enhancing disaster preparedness, improving maritime governance, and protecting vulnerable populations. This perspective underscores technology as a tool for societal resilience, reassuring policymakers and analysts that technological progress serves the broader goal of societal stability and security.

Taken together, these three lenses generate a coherent analytical proposition. Bangladesh's security strategy aims to balance technological adaptation, strategic restraint, and human-centered resilience to promote regional stability and shared security in a resource-constrained, geopolitically competitive environment. This integrated framework directly informs the article's proposed Defend-Deter-Protect model, ensuring that each policy recommendation supports regional peace, technological feasibility, and

human security outcomes. The following sections build on this framework to examine the changing character of warfare, the diffusion of emerging technologies, and their implications for Bangladesh’s evolving security posture.

**Figure 1.** Bangladesh’s hedging strategy in the Indo-Pacific security environment



Source: courtesy of the author, adapted by MCUP.

Taken together, these perspectives suggest that Bangladesh’s security strategy must carefully balance technological adaptation with human-centered security imperatives. While technological modernization remains essential, it is not approached here as an end or as a mere accumulation of hardware. Instead, technological capabilities are assessed by the outcomes they produce, particularly their ability to reduce civilian vulnerability,

strengthen disaster response, and sustain maritime and coastal livelihoods. In this way, the apparent tension between military modernization and human-centered security is not only reconciled but reframed, positioning technology as a means to enhance societal resilience rather than a symbol of state power.

### *Methods*

This policy-oriented synthesis integrates secondary evidence with theory-driven analysis to inform policymakers and scholars about Bangladesh's security environment, relying on a qualitative, interpretive approach grounded in political science and security studies, using document analysis, scholarly literature, and policy discourse to examine Bangladesh's evolving security environment in depth.

The analysis draws on a wide range of contemporary sources, including global defense assessments from the Stockholm International Peace Research Institute, the Indigenous Peoples Rights International, the International Institute for Strategic Studies, and the Center for Strategic and International Studies; military innovation reports from the U.S. Department of Defense, the North Atlantic Treaty Organization, and the U.S. Defense Innovation Unit; and regional think-tank outputs from the Bangladesh Institute of International and Strategic Studies, the Bangladesh Institute of Peace and Security Studies, and the North South University Center for Peace Studies. These are complemented by recent peer-reviewed scholarship on modern warfare, small-state security, and Indo-Pacific geopolitics, as well as credible journalistic reporting from sources such as Reuters, the Associated Press, and *The Daily Star*. To foster confidence in the findings, the study

prioritizes materials published between 2023 and 2025, ensuring relevance and timeliness in capturing recent strategic shifts.

The analytical process unfolds in three interrelated stages. It begins by mapping global transformations in the character of warfare and the diffusion of emerging technologies. It then situates these developments within the evolving Indo-Pacific strategic order, before turning to Bangladesh's specific security challenges and policy responses. This structured approach aims to reassure the audience of the comprehensive and thoughtful nature of the analysis, which is interpreted through an integrated theoretical lens that brings together technological transformation, the security dilemma in a small-state context, and human-centered security.

Rather than seeking causal generalization through quantitative measurement, the study employs a theory-informed interpretive approach that connects global trends to Bangladesh's national and regional realities. This approach is particularly well suited to capturing the complex interplay among emerging technologies, great power competition, and nontraditional security threats, while ensuring that the analysis remains both policy-relevant and grounded in Bangladesh's lived security experiences.

### **Strategic Shifts in the Character of War, 2023–2025**

The character of modern warfare has undergone a profound transformation, shifting from a platform-centric to a network-centric and people-intensive model. Military effectiveness now depends less on the sheer scale of hardware and more on integrating rapid, multidomain kill chains that connect sensors, shooters, and decision makers in real time. However, despite the increasing role of advanced technologies, the “people layer” continues to

determine outcomes. Dispersed small units, empowered noncommissioned officers, and civilian technologists capable of rapidly adapting commercial innovations such as drones, AI systems, and autonomous platforms are now critical to battlefield success.<sup>4</sup> At the same time, ubiquitous intelligence, surveillance, and reconnaissance (ISR) capabilities, combined with the proliferation of low-cost precision-strike systems have placed unprecedented pressure on supply chains and operational logistics. In Ukraine, for example, FPV drones costing as little as \$500 USD have successfully destroyed assets worth millions, demonstrating how the cost-exchange ratio heavily favors attackers.<sup>5</sup> These dynamics force militaries to adopt more agile strategies, including deception, decoys, dispersion, and rapid signature management to maintain survivability in contested environments.

Electronic warfare has further reshaped the modern battlespace, emerging as the new form of “artillery” capable of jamming global navigation satellite systems (GNSS), spoofing communications, and disrupting command-and-control structures. The conflict in Ukraine highlights that electronic warfare fratricide, where friendly systems unintentionally disrupt each other, is now a real operational risk, demanding disciplined spectrum management and doctrinal adaptation.<sup>6</sup> Understanding these risks is essential for strategic planning, as they directly influence operational effectiveness and risk mitigation measures. Beyond terrestrial domains, commercial space constellations such as Starlink have become central to resilient beyond-line-of-sight communications and ISR redundancy.<sup>7</sup>

However, this growing reliance on private providers raises critical concerns about data sovereignty, legal liabilities, and escalation dynamics, requiring states to establish contingency plans for network disruptions. This

dependency influences strategic resilience and necessitates clear policies for maintaining operational continuity. Additionally, the contemporary security environment is increasingly characterized by a hybrid-gray continuum, where coercion below the threshold of conventional warfare has become normalized. States now face constant low-intensity pressures, whether through maritime harassment in disputed waters, cyber campaigns aimed at disrupting infrastructure, or information operations that influence public opinion. In smaller nations like Bangladesh, this changing nature of conflict requires a more holistic approach to security that balances investment in hard military capabilities, including counterdrone systems and resistant communications, with an emphasis on diplomatic, legal, and informational means to ensure that they can manage within the new nature of conflict.

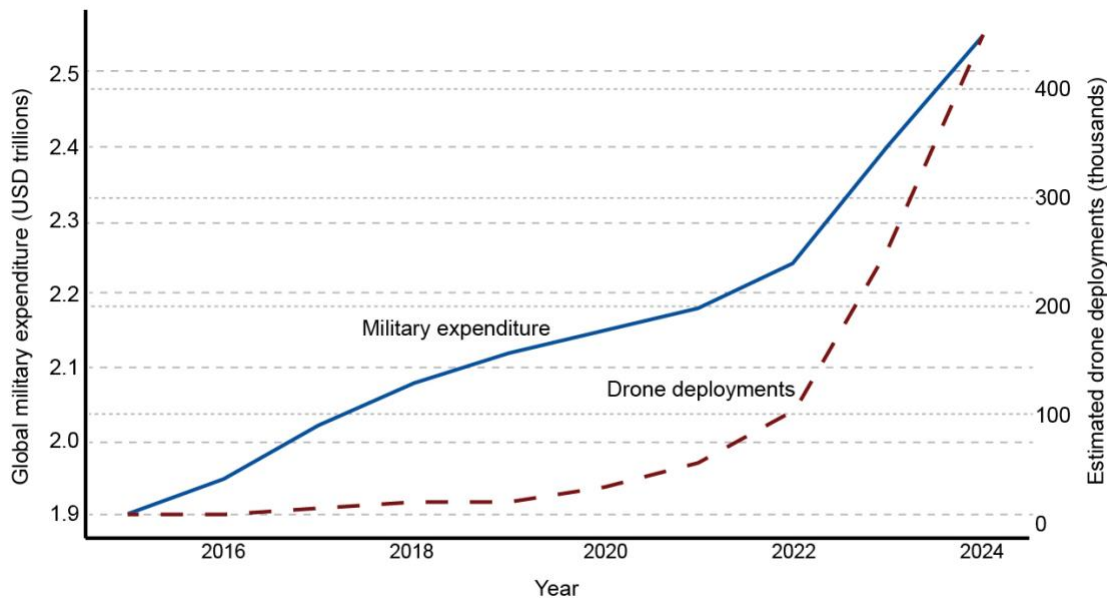
### **Technological Innovations Reshaping Operations**

The modern battlespace is undergoing radical change due to the accelerated adoption of uncrewed and autonomous systems across the air, land, sea, and undersea domains. The proliferation of low-cost uncrewed aerial vehicles (UAVs), such as small quadcopters used for reconnaissance and long-range, one-way attack drones, has transformed operational concepts and military doctrines worldwide. Mass and attainability are becoming key priorities in Western militaries as they move beyond a few expensive, bespoke systems to thousands of cheap, easily replaceable autonomous platforms that can scale up quickly in contested environments.<sup>8</sup>

Lessons from recent conflicts highlight three critical operational imperatives. First, sustainment over sophistication has become central, as battlefield success now relies less on technologically “exquisite” systems and

more on industrial scalability, repairability, and continuous software updates to ensure rapid adaptation against evolving threats.<sup>9</sup> Second, an effective response to drone threats requires a layered counter-UAS architecture that integrates electronic warfare capabilities, kinetic interceptors, camouflage, decoys, and tactical innovations, rather than relying on a single “silver bullet” solution.<sup>10</sup> Third, autonomous platforms achieve their full potential only when integrated into kill-web networks, sophisticated systems linking sensors, shooters, and decision makers that significantly amplify the range, speed, and precision of conventional fires.

**Figure 2.** Global military expenditure and the proliferation of autonomous systems, 2015–24



Source: courtesy of the authors, adapted by MCUP.

Alongside autonomous systems, AI has emerged as a decisive enabler of modern military operations, transforming how forces process, manage,

and act on battlefield information. AI supports the triage of sensor data, autonomous target recognition, optimized route planning, and real-time spectrum management, enabling militaries to operate at machine speed. However, maintaining human-on-the-loop oversight remains critical to ensure accountability and preserve legally auditable chains of decision making, particularly as autonomous operations expand. The challenge lies in ensuring continuous model updates that can outpace adversaries' adaptive tactics while maintaining reliability and operational control during contested conditions. Complementing AI, electronic warfare has emerged as a central pillar of survivability and dominance, enabling forces to jam GNSS links, spoof communications, and degrade adversary command-and-control structures. As evidenced in Ukraine, electronic warfare is reshaping tactics, forcing militaries to adopt strict emissions discipline, agile spectrum maneuvering, and fallback communications strategies designed to maintain operational continuity during network disruption or GNSS denial.<sup>11</sup>

**Table 1.** Key technological innovations in modern warfare, 2023–25

<b>Technology</b>	<b>Operational use</b>	<b>Cost implications</b>	<b>Relevance for Bangladesh</b>
<b>Uncrewed aerial systems</b>	Reconnaissance, loitering munitions, strike operations	First-person-view drones ≈ \$500 USD versus traditional missiles ≈ \$1 million+ USD	Affordable surveillance and counterterror operations
<b>Autonomous underwater vehicles</b>	Subsurface monitoring, mine detection	≈ \$50,000–200,000 USD per unit	Enhances Bay of Bengal maritime security
<b>Electronic warfare</b>	Global Positioning System jamming, communications disruption, spectrum dominance	Relatively low cost but technology-intensive	Needed for counterdrone operations and intelligence, surveillance, and

<b>Technology</b>	<b>Operational use</b>	<b>Cost implications</b>	<b>Relevance for Bangladesh</b>
			reconnaissance resilience
<b>Artificial intelligence for command and control and targeting</b>	Sensor fusion, route planning, predictive analytics	Mostly software-based, scalable	Key for optimizing coastal and border defenses
<b>Cyber and information operations</b>	Protecting operational technology/information technology infrastructure and combating disinformation	Rising investment, critical for digital sovereignty	Crucial for protecting ports, telecommunications, and power grids

Source: courtesy of the author.

While hypersonic weapons dominate strategic discourse, their prohibitive cost and limited deployment suggest that militaries will continue to prioritize layered, integrated air-defense systems to counter diverse aerial threats, including drones, cruise missiles, and long-range precision fires. The combination of point-defense counter-UAS capabilities and wide-area sensor networks is increasingly critical for maintaining effective airspace security. Simultaneously, the growing convergence of operational technology and information technology across ports, energy grids, and telecommunications networks has elevated cybersecurity and information operations to strategic priorities. Protecting critical infrastructure now demands rigorous cyber hygiene, proactive vulnerability assessments, and robust consequence management frameworks. Equally significant is the role of narrative control, as adversaries increasingly exploit disinformation campaigns to undermine public confidence and destabilize societies during crises and disasters. In this interconnected environment, modern warfare is defined as much by autonomy, spectrum dominance, and digital resilience as by traditional

firepower. For smaller states like Bangladesh, these transformations necessitate adopting adaptive, cost-effective, and layered security strategies that integrate technological innovation with human-centric defense policies to ensure operational competitiveness and long-term resilience.

### **Propaganda, Digital Influence, and Political Warfare in the Indo-Pacific Security Environment**

Information warfare is no longer peripheral to security; it directly shapes public trust, crisis response, and social stability, making it integral to the “Protect” pillar of this framework. In the digital era, the terrain of conflict has expanded far beyond conventional battlefields into the domains of information, cognition, and perception. Across the Indo-Pacific, where strategic rivalries intersect with fragile state structures, propaganda and political warfare amplified by digital platforms and AI have emerged as central instruments of power projection, emphasizing the critical role of security professionals and policymakers in managing these challenges.

The rapid diffusion of AI, autonomous systems, and ubiquitous digital platforms has transformed the speed and scale at which narratives are constructed, contested, and weaponized. Information has become a strategic resource capable of shaping public opinion, influencing policy decisions, and redefining the outcomes of conflict. In this evolving landscape, influence operations are continuous, often operating below the threshold of conventional confrontation, requiring constant vigilance from security professionals and policymakers.

For Bangladesh, these dynamics are particularly consequential. As a strategically located state at the intersection of the Bay of Bengal and the

wider Indo-Pacific, it is increasingly exposed to digitally enabled influence operations. The expansion of digital connectivity has created new opportunities for economic integration, yet it has also introduced vulnerabilities to cyber disruption, disinformation, and AI-generated manipulation. Recognizing these risks is essential for safeguarding security, which now requires protecting informational integrity and societal resilience beyond territorial defense.

### **The Indo-Pacific Context and Bangladesh's Strategic Posture**

The Sino-Indian rivalry in the Indo-Pacific, intensified by Ladakh border clashes, China's Belt and Road Initiative, and the Quadrilateral Security Dialogue among Australia, India, Japan, and the United States, has elevated Bangladesh's strategic importance. Beijing's investments in Chattogram, Payra, and submarine bases fuel India's concerns over encirclement, while India leverages its \$500 million USD defense credit line and naval cooperation to retain influence. Bangladesh's location along the Bay of Bengal places it at the intersection of competing maritime strategies, making balanced engagement with both actors essential for safeguarding sovereignty, economic interests, and regional stability.<sup>12</sup>

Bangladesh's Indo-Pacific Outlook emphasizes an open, rules-based order, economic connectivity, maritime security, and strategic autonomy, eschewing bloc politics while deepening cooperation on capacity-building.<sup>13</sup> This policy of equidistance diplomacy enables Bangladesh to engage multiple security and technology partners without compromising development priorities. Bangladesh's Forces Goal 2030 military modernization blueprint has expanded service capacities, though its scope remains a subject of

ongoing debate amid shifting domestic politics.<sup>14</sup> Bangladesh's maritime jurisdiction, as reflected in the map above, extends deeply into the Bay of Bengal, constituting ocean territory roughly 80 percent the size of its landmass. While the blue economy offers opportunities in fisheries, maritime trade, and offshore resources, it faces significant security challenges such as piracy, illegal fishing, marine pollution, and gaps in maritime domain awareness, which threaten sustainable development and regional stability.<sup>15</sup> Addressing these threats requires targeted maritime security measures and regional cooperation.

### **Bangladesh's Evolving Security Challenges**

Bangladesh's security environment requires coordination with regional and international stakeholders, including neighboring countries, the Association of Southeast Asian Nations, and United Nations agencies, to effectively address humanitarian, maritime, climatic, and internal challenges. The country currently hosts nearly 1 million Rohingya refugees in Cox's Bazar and on Bhasan Char, making it one of the world's largest and most protracted refugee crises.<sup>16</sup> However, persistent funding shortfalls have significantly curtailed essential services, including education, healthcare, and food security, exacerbating protection risks and social vulnerabilities.<sup>17</sup> The situation is further complicated by the escalation of violence in Myanmar, where clashes between the military junta and ethnic armed organizations have periodically spilled across the Naf River, with audible shelling reported in Teknaf in 2024.<sup>18</sup> These dynamics demand a comprehensive, whole-of-government approach that integrates strengthened border security, humanitarian coordination, and sustained regional diplomacy to manage

both immediate crises and long-term stability, involving key regional and international partners.

Beyond its borders, Bangladesh faces mounting maritime security challenges in the Bay of Bengal, where piracy and armed robbery incidents spiked sharply in 2024, particularly around Chattogram and other coastal waters, straining the operational capacities of the Bangladesh Navy and Coast Guard.<sup>19</sup> The bay remains a critical conduit for narcotics trafficking, human smuggling, and illicit trade, while increasing climate-induced disruptions, such as extreme weather events, further complicate interdiction efforts and search-and-rescue operations.<sup>20</sup> With Bangladesh's blue economy ambitions heavily reliant on maritime trade, fisheries, and offshore energy exploration, ensuring maritime domain awareness and robust law enforcement mechanisms has become inseparable from safeguarding economic and environmental sustainability. This focus aims to inspire confidence in the audience about Bangladesh's proactive approach to maritime security and economic resilience.

Climate-related security threats pose another significant challenge, with Cyclone Remal (May 2024) devastating 3.7–3.8 million people and destroying approximately 150,000 homes, underscoring the deep interlinkages between disaster management and national security.<sup>21</sup> The *National Adaptation Plan of Bangladesh (2023–2050)* identifies climate resilience, disaster risk reduction, and infrastructure protection as central national priorities.<sup>22</sup> The armed forces play an increasingly vital role in anticipatory action, including emergency evacuations, airlift operations, engineering support, and communications recovery, demonstrating how military capacity is becoming a cornerstone of climate-security preparedness.

This highlights the importance of collective effort and shared responsibility in addressing climate threats.

Internal stability is further challenged by violent extremism and governance-driven unrest. Since 2016, security forces have degraded several organized jihadist networks, but residual risks remain, particularly from splinter factions like Neo-Jama'atul Mujahideen Bangladesh and their cross-border linkages with transnational extremist groups.<sup>23</sup> At the same time, student-led protests in 2024 revealed how governance crises can escalate into broader internal security challenges, straining law enforcement and institutional cohesion.<sup>24</sup> Looking ahead, future threats are expected to involve a hybrid mix of online radicalization, organized criminal networks, political instability, and external provocations, necessitating integrated counterterrorism strategies that combine technological surveillance, cross-border intelligence sharing, and community-based resilience frameworks.

### **A Bangladesh Roadmap: Defend, Deter, Protect, 2025–2030**

#### *From Capability Accumulation to Human-Centered Outcomes*

The proposed roadmap reorients Bangladesh's security strategy away from platform-centric accumulation toward an outcome-based approach, evaluating capabilities by their contribution to human-centered security. Rather than pursuing prestige-driven modernization or costly replication of major power models, this framework emphasizes investments that are cost effective, scalable, and capable of enhancing societal resilience. Within this logic, an agile security posture is understood as the capacity of state institutions to anticipate, absorb, and adapt to multidomain threats in real time. Such agility is not an abstract ideal but can be observed through

measurable indicators, including response time during crises, the effectiveness of civilian protection, the redundancy of critical systems, and the speed of recovery following disruption.

Within this broader orientation, the “Defend” pillar prioritizes protecting Bangladesh’s territorial, maritime, and digital domains through layered, distributed systems that are both affordable and adaptable. Maritime domain awareness emerges as a critical component, requiring the integration of coastal radar systems, automatic identification systems, and UAV-based surveillance to monitor illegal fishing, piracy, and gray-zone activities in the Bay of Bengal. At the same time, cybersecurity and digital sovereignty must be strengthened through institutional capacity-building under Bangladesh’s Cyber Security Act (2023), including expanding national computer emergency response mechanisms, conducting systematic audits of critical infrastructure, and developing robust public-private resilience frameworks. Looking forward, the development of satellite-enabled surveillance, whether through a modest national program or shared regional access, offers a strategic pathway to reduce dependence on external intelligence sources while enhancing maritime awareness and disaster monitoring. Taken together, these measures strengthen strategic autonomy by enabling Bangladesh to retain greater control over information and surveillance capabilities.

The “Deter” pillar shifts attention to the need for cost-effective, asymmetric capabilities that raise the threshold for aggression without triggering destabilizing arms-race dynamics. For a small state operating within a competitive Indo-Pacific environment, deterrence must be achieved through efficiency rather than scale. This requires the development of a

layered counter-UAS architecture that combines electronic warfare measures, kinetic interception, and passive techniques such as camouflage and decoys to protect critical assets, including military installations, refugee camps, and essential infrastructure. Investment in electronic warfare capabilities further enhances this deterrent posture by enabling low-cost disruption of adversary communications and navigation systems. At the same time, prioritizing distributed and attritable systems, particularly scalable drone fleets, ensures a favorable cost-exchange ratio, allowing Bangladesh to offset resource constraints while maintaining operational effectiveness. In this context, deterrence is not built on expensive platforms but on adaptability and resilience. By emphasizing defensive and asymmetric tools, this approach also mitigates the security dilemma, reducing the likelihood that Bangladesh's modernization efforts will provoke regional escalation.

At the core of the framework lies the "Protect" pillar, which anchors security policy in the lived realities of citizens and communities. This pillar directly operationalizes human-centered security by focusing on protecting vulnerable populations and strengthening societal resilience. In the context of the Rohingya crisis, this requires the deployment of surveillance technologies, early warning systems, and coordinated civil-military mechanisms to prevent infiltration, trafficking, and violence within refugee settlements. More broadly, climate-security integration becomes a central priority, with the armed forces playing an expanded role in anticipatory disaster response, emergency logistics, evacuation operations, and post-disaster reconstruction. Equally important is protecting livelihoods, particularly in coastal and maritime regions where fisheries, ports, and fragile

ecosystems underpin economic survival. Here, integrated maritime enforcement and environmental monitoring can help reduce vulnerability while sustaining long-term economic stability. The effectiveness of this pillar can be measured through tangible outcomes, including reduced disaster response times, improved civilian protection, and minimized disruption to livelihoods.

Given Bangladesh's fiscal and institutional constraints, the success of this roadmap depends not only on what is implemented but also on how it is sequenced. A phased approach is therefore essential. In the short term, priority should be given to deploying counter-UAS systems, strengthening cyber resilience, and modernizing disaster response capabilities, as these offer immediate, high-impact returns. In the medium term, investments should expand toward maritime domain awareness, the development of electronic warfare capabilities, and the strengthening of institutional coordination mechanisms. During the longer term, more resource-intensive initiatives such as developing satellite capabilities and integrating advanced AI-enabled systems can be pursued as foundational capacities mature.

To support this prioritization under real budgetary constraints, table 2 provides a comparative assessment of key security investments, evaluating them on cost, strategic impact, and their contribution to human-centered security outcomes. In doing so, the roadmap translates abstract strategic principles into a practical decision-making framework, ensuring that Bangladesh's security investments remain both effective and sustainable in an increasingly complex security environment.

**Table 2.** Cost-benefit and strategic prioritization of security investments in Bangladesh

Capability	Cost level	Strategic impact	Human security contribution	Implementation priority
First-person-view/tactical drones	Low	High (intelligence, surveillance, and reconnaissance as well as deterrence)	Enhances surveillance, disaster mapping, and border monitoring	<b>High (immediate)</b>
Counterunmanned aircraft systems	Medium	High (critical protection)	Protects refugee camps, infrastructure, and civilian zones	<b>High (immediate)</b>
Electronic warfare	Medium	High (asymmetric advantage)	Disrupts hostile systems with minimal collateral risk	<b>High (short term)</b>
Cybersecurity infrastructure	Medium	Very high (system resilience)	Protects financial systems, telecommunications, and public services	<b>Very high (immediate)</b>
Maritime domain awareness	Medium	Very High (economic and security)	Secures fisheries, trade routes, and coastal livelihoods	<b>Very high (short/medium term)</b>
Disaster response logistics	Medium	Very high (climate security)	Direct civilian protection, rapid recovery capacity	<b>Critical (immediate)</b>
Corvettes/large naval platforms	Very high	Medium	Limited direct civilian impact	<b>Low (deferred)</b>
Fighter aircraft expansion	Very high	Medium	Minimal human security return	<b>Low (deferred)</b>
Satellite capability (national/shared)	High (initial)	Very high (long-term autonomy)	Improves disaster warning, maritime monitoring	<b>Medium/long term</b>

Source: courtesy of the author.

This table illustrates that Bangladesh’s optimal strategy is to prioritize low- and medium-cost, high-impact capabilities that directly enhance civilian

protection and resilience, while deferring capital-intensive platforms with limited human-security returns.

### **Strategic Autonomy through Selective Partnerships**

Bangladesh's evolving security strategy requires an integrated approach that balances defense, deterrence, and protection within a pragmatic, responsive framework that addresses the country's structural constraints. At its core, this strategy must strengthen sovereignty, secure maritime domains, and safeguard vulnerable communities while carefully navigating the tensions between modernization and strategic autonomy. By doing so, the emphasis shifts from the accumulation of high-cost capabilities toward the development of layered, adaptive, and context-sensitive systems that can respond effectively to a wide range of threats.

To defend the homeland and its littoral spaces, priority must be given to building resilient, distributed security architectures. This involves deploying layered counter-UAS systems to protect border outposts, ports, critical infrastructure, and refugee settlements through a combination of electronic warfare, kinetic interception, camouflage, and decoy techniques. At the same time, enhancing ISR capabilities through domestically assembled drones and integrated coastal monitoring systems offers a cost-effective way to address persistent challenges such as illegal fishing, piracy, and smuggling. Strengthening maritime domain awareness requires integrating multiple data streams, including automatic identification systems, coastal radar networks, satellite data, and community-based reporting mechanisms. Such efforts can be further reinforced through selective participation in regional information-sharing platforms, provided that these engagements enhance

Bangladesh's independent operational capacity rather than deepen dependency. Equally important is protecting cyber-physical infrastructure, including ports, power grids, and telecommunications networks, through continuous vulnerability testing and closer coordination with private-sector operators.

Building an effective deterrent posture requires a shift away from expensive, platform-heavy models and toward scalable and adaptive capabilities that raise the cost of aggression without provoking escalation. In this context, the development of attritable mass through swarms of expendable systems integrated with existing coastal and artillery defenses offers a more sustainable and strategically appropriate pathway. Equally critical is the management of the electromagnetic spectrum, where disciplined emissions control, expanded training in electronic warfare, and the adoption of resilient communication systems can ensure operational continuity even in contested environments. Strengthening command-and-control networks through layered communication architectures, including satellite, radio, and mesh-based systems with fallback options, is essential to maintaining decision-making capacity under conditions of disruption. Within this framework, selective modernization under Forces Goal 2030 should prioritize multimission capabilities that enhance operational flexibility and sustainment, rather than symbolic acquisitions that impose long-term financial burdens without commensurate strategic returns.

At the heart of this strategy lies the imperative to protect people and communities, placing human-centered security at the center of national defense. This requires a significant expansion of anticipatory capacities, including improved early warning systems, prepositioned relief logistics, and

the integration of military transport assets into civilian evacuation and response frameworks during disasters. In the context of the Rohingya crisis, ensuring safety and dignity demands investments in resilient shelter infrastructure, fire prevention systems, and basic services, alongside longer-term initiatives in education and skills development to reduce vulnerability to exploitation and instability. Strengthening coastal and maritime livelihoods is equally critical, as these sectors underpin both economic security and social stability. Partnerships between universities, technology startups, and security agencies can play a transformative role in developing locally appropriate innovations, such as low-cost sensors, drones, and flood-resilient communication systems, thereby enhancing frontline response capacities.

At the same time, the ethical and governance dimensions of emerging technologies must not be overlooked. As Bangladesh adopts AI and human-machine systems within its security architecture, it must also establish clear regulatory frameworks to ensure accountability, transparency, and alignment with international norms. Active engagement in multilateral discussions on responsible autonomy can further reinforce Bangladesh's position as a norm-shaping actor rather than a passive recipient of external technological standards.

Ultimately, the sustainability of this strategy depends on how Bangladesh navigates its external partnerships. Strategic autonomy, in this context, is not achieved through isolation but through diversification and domestic capacity-building. Engagement with regional and global partners must therefore be guided by a clear principle: cooperation should enhance Bangladesh's independent operational capabilities rather than create new forms of dependency. This requires a calibrated approach to diplomacy,

leveraging the Indo-Pacific Outlook to attract capacity-building support across multiple domains, particularly maritime security, humanitarian assistance, disaster response, and the management of transnational threats, while avoiding alignment with any single power bloc.

In an increasingly complex security environment, Bangladesh's ability to defend its sovereignty, deter emerging threats, and protect its people will depend not on the scale of its military acquisitions, but on the coherence, adaptability, and human-centered orientation of its security strategy.

### **Lived Realities: Humanizing Strategy**

It is a storm-drenched night in Teknaf. Sheets of rain hammer the fragile coastline as the power goes out, plunging the settlement into darkness. In a cramped, makeshift cyclone shelter, a single volunteer radio operator steadies her trembling voice as she delivers weather updates to anxious families huddled together. Across the Naf River, muffled thuds of artillery fire from Myanmar echo faintly through the wet night air, a grim reminder that conflict refuses to respect borders.

Her cracked mobile phone, tethered to a small solar-powered, mesh-enabled communication node, becomes the lifeline of the shelter, connecting frightened residents to the Upazila control room far away. At the same moment, in Chattogram, a weary coast guard team hunches over a dimly lit tablet, tracking live video from a fixed-wing UAV. Village watch reports warn of two "dark skiff" boats without navigation lights, maneuvering erratically through contested waters. Smugglers, pirates, or something far more dangerous—no one knows.

In Ukhiya, inside one of the world's largest refugee camps, a schoolteacher hesitates, torn between ending classes early and keeping a semblance of normalcy. Rumors of unrest ripple quietly through the settlement. Nearby, a counter-UAS radar mounted on a steel post silently sweeps the skies, scanning for potential aerial threats while offering the camp a fragile sense of security.

These vignettes are not fragments of a distant dystopian future; they represent scenarios for which Bangladesh must increasingly prepare. They reveal a deeper truth: national security is no longer defined solely by platforms, weapons, or doctrines; it is lived every day by people at the periphery. When a volunteer's solar-powered radio holds a community together during a blackout, when UAVs extend coast guards' capabilities, and when digital sensors silently guard refugee camps, integrating these technologies with human security strategies becomes essential.

For Bangladesh, an effective security posture can no longer rely solely on traditional military power. It must combine high technologies with community resilience, local knowledge systems, and anticipatory action. By integrating technological innovations such as UAVs and digital sensors with community-based approaches, Bangladesh can better address climate change impacts, maritime disputes, and refugee flows, ensuring a more comprehensive, human-centered security framework.

Aligned with this approach, Bangladesh has adopted a policy of selective alignment, joining BRICS (Brazil, Russia, India, China, and South Africa) to diversify its economic alliances while supporting China's Global Development Initiative for infrastructure financing. Emphasizing regional

cooperation and technological independence can empower policymakers to build resilient security capabilities, fostering national confidence and stability.

## **Conclusion**

The grammar of warfare is undergoing a profound transformation, shaped by massed autonomy, data-intensive operations, cyber dominance, and contested electromagnetic environments. However, the enduring logic of warfare remains anchored in institutions, command structures, and ultimately public confidence. For Bangladesh, situated at the intersection of the Bay of Bengal and the wider Indo-Pacific strategic theater, the challenge is not to pursue maximalist armament or mirror the capabilities of larger powers. Rather, it is to cultivate a posture of strategic sufficiency—one built on layered defenses, flexible and adaptive forces, enhanced maritime domain awareness, resilient communications, and climate-responsive, human-centered security systems. Such an approach reconciles technological innovation with community-based resilience, ensuring that emerging capabilities serve society rather than overshadow it.

The dividends of this strategy extend well beyond conventional deterrence. They are reflected in more secure coastal spaces where piracy and illicit flows are contained, in safer and more reliable maritime trade routes that sustain Bangladesh's blue economy ambitions, and in communities better prepared to withstand and recover from climate-induced disruptions. Security, in this sense, becomes both protective and enabling, reducing risk while expanding opportunity.

Achieving this vision, however, requires more than institutional reform or technological investment; it demands an inclusive security governance

model that unites government agencies, civil society, local communities, private innovators, and regional partners. This approach can foster a shared sense of purpose and collective responsibility, strengthening social trust and diplomatic balance.

By doing so, Bangladesh has the opportunity to articulate a distinct security model that is adaptive, affordable, and inclusive. Highlighting this can evoke pride and motivation, positioning Bangladesh as a leader among small states navigating asymmetric pressures in the twenty-first century.

---

<sup>1</sup> Al Amin, "Sino-Indian Rivalry in Indo-Pacific and Bangladesh's Geo-strategic Hedging in Response to Its Security Threats," *Discover Global Society* 3, no. 15 (2025), <https://doi.org/10.1007/s44282-025-00144-1>.

<sup>2</sup> Xiao Liang et al., *Trends in World Military Expenditure, 2024* (Stockholm: Stockholm International Peace Research Institute, 2025).

<sup>3</sup> *Indo-Pacific Outlook of Bangladesh* (Dhaka: Ministry of Foreign Affairs, Government of the People's Republic of Bangladesh, 2023).

<sup>4</sup> Matthew Slusher, *Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience* (Washington, DC: Center for Strategic and International Studies, 2025).

<sup>5</sup> *The Military Balance 2025* (London: International Institute for Strategic Studies, 2025).

<sup>6</sup> "Ukraine Joins NATO Counter-drone Exercise for First Time," North Atlantic Treaty Organization, 19 September 2024.

<sup>7</sup> Andrew Radin et al., *Lessons from the War in Ukraine for Space: Challenges and Opportunities for Future Conflicts* (Santa Monica, CA: Rand, 2025), <https://doi.org/10.7249/RAA2950-1>.

<sup>8</sup> Joseph Clark, "DOD Innovation Official Discusses Progress on Replicator," DOD News, 12 December 2024; and "The Replicator Initiative (Iteration 2)," Defense Innovation Unit, 2024.

<sup>9</sup> Slusher, *Lessons from the Ukraine Conflict*.

<sup>10</sup> *The Military Balance 2025*; and "Ukraine Joins NATO Counter-drone Exercise for First Time."

<sup>11</sup> *The Military Balance 2025*.

<sup>12</sup> Amin, "Sino-Indian Rivalry in Indo-Pacific and Bangladesh's Geo-strategic Hedging in Response to Its Security Threats."

<sup>13</sup> Sohini Bose, *Continuity and Change in Bangladesh's Indo-Pacific Outlook: Deliberating Post-Election Scenarios* (Washington, DC: Observer Research Foundation, 2024); and Shadman Sharar, *An Assessment of Bangladesh's Indo-Pacific Outlook* (Dhaka: Center for Peace Studies, North South University, 2023).

<sup>14</sup> Iqram Hossain Mahboob, *Forces Goal 2030: Geopolitical Significance for Bangladesh and the Region* (Dhaka: Bangladesh Institute of Peace and Security Studies, May 2023); and Khandakar Tahmid Rejwan, "Revisiting 'Forces Goal 2030': Bangladesh's Military Modernization Plan under the New Government," *Diplomat*, 6 December 2024.

<sup>15</sup> "Piracy Incidents in Bangladesh Increased by Ninefold in First Five Months of 2024 Compared to Full Previous Year," Baird Maritime, 21 June 2024; and *Report on Roundtable*

---

*Discussion on Maritime Security in the Bay of Bengal: Emerging Threats and Strategies of Bangladesh* (Dhaka: Bangladesh Institute of International and Strategic Studies, 2024). The term *blue economy* describes the economic activities associated with the oceans and seas. See “What Is the Blue Economy?,” Grantham Research Institute on Climate Change and the Environment, 11 December 2024.

<sup>16</sup> “Bangladesh: Operational Data Portal,” United Nations High Commissioner for Refugees, 2025.

<sup>17</sup> Ruma Paul, “School Closures Push Rohingya Refugee Children into Marriage and Work,” Reuters, 22 August 2025.

<sup>18</sup> Mokammel Shuvo, “Myanmar Conflict: Fighting Flares up across the Teknaf Border,” *Daily Star*, 17 April 2024.

<sup>19</sup> “Piracy Incidents in Bangladesh Increased by Ninefold in First Five Months of 2024 Compared to Full Previous Year.”

<sup>20</sup> *Report on Roundtable Discussion on Maritime Security in the Bay of Bengal*.

<sup>21</sup> *UNICEF Bangladesh: Situation Report on Cyclone Remal and Floods in Bangladesh*, no. 3 (New York: United Nations Children’s Fund, 2024); “Bangladesh: Tropical Cyclone 2024/05/26,” Asian Disaster Reduction Center, 30 May 2024; and Gwyn Lewis, *Bangladesh Rapid Response: Tropical Cyclone Remal 2024* (New York: United Nations Central Emergency Response Fund, 2025).

<sup>22</sup> *National Adaptation Plan of Bangladesh (2023–2050)* (Dhaka: Ministry of Environment, Forest and Climate Change, Government of the People’s Republic of Bangladesh, 2022).

<sup>23</sup> “Neo-Jama’at Mujahideen Bangladesh,” Australian National Security, last updated 22 September 2024.

<sup>24</sup> Rahul Roy-Chaudhury and Viraj Solanki, “Bangladesh: Domestic Turmoil and Regional Insecurity,” International Institute for Strategic Studies, 20 August 2024.