Humanities and Social Sciences
2025, Vol. 13, No. 6, pp. 590–599
https://doi.org/10.11648/j.hss.20251306.19

Research Article

Constructing Cybersecurity: A Constructivist Analysis of Bangladesh's Response to Emerging Digital Threats

Sahely Ferdous*

International Studies, Macquarie University, Sydney, Australia

Abstract

Bangladesh's rapid digital transformation under the national vision of "Digital Bangladesh" has created both opportunities and vulnerabilities within cyberspace. As financial systems, e-governance, and communication networks expand, cyber incidents, such as the 2016 Bangladesh Bank heist and recurring data breaches, reveal that the nation's security challenges extend beyond technology. This article applies a constructivist theoretical framework to argue that cybersecurity in Bangladesh should be socially constructed through shared meanings, political narratives, and institutional identities rather than determined solely by material capacity. Drawing on the foundational insights of Onuf, Wendt, and Finnemore, it contends that the country's laws and policies, such as the Information and Communication Technology (ICT) Act (2006) and the Digital Security Act (2018), reflect the internalisation of state-centric norms that privilege control and reputation management over transparency and citizen trust. Through interpretive analysis of policy documents, legislative instruments, and media discourses, the study demonstrates that the prevailing cybersecurity narrative in Bangladesh equates resilience with regime stability and technological modernity. Constructivist reasoning reframes this narrative by highlighting how institutional legitimacy, social trust, and professional identity shape security behaviour. Further, research shows that international frameworks, such as the International Organisation for Standardisation/International Electrotechnical Commission (ISO/IEC) 27001 and the National Institute of Standards and Technology (NIST) Cybersecurity Framework, contribute to global norm diffusion but achieve a long-term impact only when locally internalised. Ultimately, the study concludes that Bangladesh's cybersecurity resilience depends not merely on technological and legislative reforms but on reconstructing the social meanings that underpin governance. By embedding openness, inclusivity, and accountability into institutional culture, Bangladesh can transform cybersecurity from a domain of control into a collective practice of trust and responsibility.

Keywords

Bangladesh, Cybersecurity, Constructivism, Digital Security Act, ICT Act, Governance, Norm Diffusion

1. Introduction

Bangladesh stands at a pivotal juncture between aspiration and accountability. Its digital transformation is irreversible; the challenge lies in whether its security culture can evolve accordingly. From a constructivist perspective, enduring progress depends on reconstructing security as a shared moral and professional enterprise rather than a domain of control. Building trust through openness, fairness, and inclusion will not only strengthen digital networks but also reinforce dem-

*Corresponding author: sahelyferdous@gmail.com (Sahely Ferdous)

Received: 9 November 2025; **Accepted:** 20 December 2025; **Published:** 27 December 2025

ocratic resilience. By embedding the reactive into law, policy, and everyday practice, Bangladesh can transform its cyber governance from a reactive defence to a proactive confidence. In doing so, it contributes not only to national stability but also to a global understanding of how ideas, norms, and identities shape the architecture of digital security.

Cybersecurity has shifted from a niche technical issue to a key aspect of national security and governance. In Bangladesh, goals for "Digital Bangladesh" and "Smart Bangladesh" have sped up the adoption of e-government systems, mobile financial services, and data-driven administration [1-3]. These changes have created new chances for inclusion and growth but have also increased exposure to transnational, low-cost, and quickly evolving cyber threats [4]. From a constructivist view, Bangladesh's interpretation, discourse, and response to cybersecurity threats fundamentally shape its security practices and results. Still, security is not just the sum of firewalls and patches; it results from socially shared ideas about what should be protected, by whom, and for whom. States can aim for security by turning the norm into one based on mutual trust and institutional cooperation through interaction and social learning processes [5].

Traditional approaches to studying security primarily emphasise material capabilities—such as military strength, technology, financial resources, and weaponry—and focus on whether states possess adversarial intent. While these elements matter, they do not explain why actors facing comparable technological risks adopt different policies, allocate resources differently, or communicate incidents with varying levels of transparency. Further, in the realm of cybercrime, offenders often exploit various internet protocols to conceal their identities, making it difficult to identify the actual perpetrator [6]. So, attributing guilt poses a major challenge. Since the internet allows a high degree of anonymity, international cooperation is critical to identifying the source of attacks while these originate outside the territory of the attacked state [7]. Consequently, cybersecurity differs fundamentally from traditional security analysis. Constructivism addresses this gap by foregrounding the social foundations of security [8, 5]. It invites inquiry into how political identities, institutional cultures, and public narratives shape the definition of cyber threat, the selection of countermeasures, and the willingness to learn after failure. In this sense, cybersecurity is co-produced through interactions among state agencies, regulated sectors, media, and citizens, as constructivists argue that security is socially defined and should ultimately protect people, not just states [9].

Despite significant improvements in its cybersecurity posture—reflected in Bangladesh's rise to 35th position in the e-Governance Academy Foundation's National Cyber Security Index (NCSI) by 2022—the country's cyber experience continues to be narrated mainly through a few emblematic incidents [3]. The 2016 Bangladesh Bank heist, in which attackers exploited authentication weaknesses to attempt nearly a billion-dollar transfer via the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network, remains a turning point. Subsequent server intrusions and hackings against civic portals reinforced a national narrative of external conspiracy and strengthened a belief that outsiders were mainly to blame [10]. From a constructivist perspective, this perception reflects a discourse centred on victimhood and external blame, often at the expense of introspective learning about how institutions could improve. This orientation is shaped by cultural factors that influence how actors construct and pursue their security interests [15]. When incidents are framed primarily as foreign aggression, the policy emphasis tends to shift toward secrecy and control rather than transparency, accountability, and fixing internal weaknesses [9].

At the societal level, technology-facilitated abuse—doxxing, non-consensual image sharing, sextortion—disproportionately affects women and youth. Yet these harms are often treated as peripheral to national security, such as state cyberattacks or military threats, revealing a hierarchy of concerns that privileges state systems over citizen safety. From a constructivist perspective, this hierarchy reflects how social norms and shared beliefs shape what counts as a real security issue and whose safety is valued. Constructivist theory helps interpret this hierarchy as a product of norms defining whose security matters and which harms count [9]. Normatively speaking, broadening the referent of security to include individuals and communities is essential for sustainable and inclusive digital development.

This analysis advances three arguments. First, Bangladesh's cybersecurity challenges are multidimensional, spanning finance, governance, and social life; they cannot be reduced to technical failure alone. Second, existing laws and policies embody particular constructions of security that influence prevention and response. Third, sustainable improvement requires cultural and normative transformation alongside technological enhancement. The discussion proceeds by elaborating the constructivist theoretical framework (Section 2), describing the methodology (Section 3), analysing Bangladesh's cybercrime environment (Section 4), examining cybersecurity challenges (Section 5), evaluating government policies and institutional effectiveness (Section 6), and concluding with reflections on identity, norms, and resilience (Section 7) to show how these three factors interact to shape Bangladesh's overall cybersecurity culture and responses.

2. Theoretical Framework: A Constructivist Approach

Constructivism occupies a distinct position within the broader landscape of international relations theory. It departs from materialist and rationalist traditions by positing that the international system is not merely governed by objective structures but is socially constructed through shared ideas, norms, and identities. This theoretical turn emerged as a re-

sponse to the perceived limitations of both realism and liberal institutionalism in explaining variation in state behaviour. Nicholas Onuf's seminal work in 1989, 'World of Our Making', established the central premise that rules make the world, arguing that social reality is continuously produced and reproduced through linguistic and institutional practices [8]. Alexander Wendt expanded this insight in his influential article 'Anarchy Is What States Make of It' in 1992 and his later monograph 'Social Theory of International Politics' in 1999, asserting that the key structures in the state system are intersubjective rather than material [5, 11]. So, international relations are not just physical power or material resources, such as military, wealth, laws, and norms, but rather the shared ideas, beliefs, and meanings that states hold about each other and maintain through social interaction. In this sense, power and interests are shaped by collectively held beliefs about appropriate behaviour.

Martha Finnemore advanced constructivism by demonstrating how international organisations and bureaucracies disseminate norms that redefine state interests [12]. According to her, states are surrounded by complex networks of transnational and international relationships that influence how they perceive the world and their place within it. Through continuous interaction with this broader international society, states become socialised into embracing particular norms, interests, and aspirations regarded as legitimate by the global community. However, domestic political dynamics often exert a pivotal, and occasionally determining, role in formulating a state's national objectives and strategic interests [12]. Peter Katzenstein similarly highlighted the influence of cultural context and national identity in shaping security policy, arguing that state interests are socially constructed through processes of interaction [13]. Collectively, these contributions demonstrate that political actors' behaviour is driven not only by instrumental rationality but also by socially constructed expectations of legitimacy, propriety, and normative obligation.

Applied to cybersecurity, constructivism provides an interpretive lens for understanding how states perceive threats, assign responsibility, and design responses. In particular, social constructivism argues that understanding political events, and hence security, requires less abstract theorising (focus on general theories that are detached from real-world contexts) and greater attention to the sociocultural contexts in which they occur [9]. From this perspective, cyber threats are not purely technical phenomena but also cultural narratives that construct identities such as victims, aggressors, and responsible stakeholders. This approach helps explain why countries with similar technological capacities and exposure to cyber risks exhibit divergent behaviours in disclosure, deterrence, and cooperation. It also elucidates why certain forms of harm—such as gender-based online abuse or disinformation—remain marginal in official security discourse. These differences arise because norms, identities, and collective meanings mediate the translation of technical vulnerabilities into political action.

For Bangladesh, a constructivist framework highlights the importance of historical experience and political culture in shaping cyber governance. The discourse surrounding "Digital Bangladesh" reflects a developmental identity that links technological progress with national pride and modernity [14]. Within this discourse, acknowledging vulnerabilities may be perceived as undermining that identity, leading to selective transparency in incident reporting. By contrast, shifting the narrative to portray cybersecurity as a shared civic responsibility—rather than a purely governmental domain—can transform public expectations and institutional behaviour. Normatively, constructivism thus opens analytical space to explore how prevailing ideas about legitimacy, trust, and accountability shape the effectiveness of technical and legal measures.

From this perspective, law and policy are not merely instruments of regulation but platforms where meanings are produced and legitimised. The ICT Act 2006 and the Digital Security Act 2018, for instance, do more than impose formal restrictions; they institutionalise a specific vision of order that elevates state security and reputation above public accountability [1, 2]. These legislative instruments embody what constructivists term norm internalisation—the process through which ideas of control and discipline become taken for granted within institutional practice [5, 13]. As administrative actors enforce these laws, they simultaneously reproduce the underlying belief that cyber resilience is maintained through surveillance and censorship rather than open dialogue. Constructivist analysis, therefore, reveals that effective reform must involve not only revising legal text but also reconstructing the cultural meaning of compliance and trust.

Finally, the theory underscores that identity and legitimacy are not merely strategic constructions but evolve through ongoing interaction with global norms and institutions. As Bangladesh deepens its integration into global digital and financial networks, international norms of transparency, data protection, and multi-stakeholder governance are exerting growing influence on its regulatory and institutional practices. The adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework and ISO/IEC 27001 standards demonstrates the gradual diffusion of external expectations into domestic practice [15, 16]. However, constructivists caution that transplanting foreign norms without cultivating local legitimacy yields only thin forms of compliance [17]. The long-term challenge, therefore, lies in fostering a professional ethos within public institutions that values transparency, continuous learning, and public trust as core indicators of competence and effectiveness. By situating cybersecurity within this constructivist framework, the subsequent analysis interprets Bangladesh's evolving digital security architecture not merely as a technical system but as an arena where existing narratives of sovereignty, modernity, and moral responsibility are reshaped.

3. Research Methodology

This study uses a qualitative interpretive document and discourse analysis informed by constructivist theory. Its primary objective is to examine how Bangladesh's national cybersecurity policies and institutional responses embody socially constructed meanings of security, trust, and legitimacy, rather than treating these as mere functional outcomes of material capacity. Within this framework, the study focuses on interpretive understanding rather than quantitative measurement, examining how discourse, identity, and norms shape state behaviour. Accordingly, the research design emphasises contextual insight rather than statistical inference. Finally, the study analyses the framing of cybersecurity in official texts and public discourse.

3.1. Research Design

The research is structured around a multi-source documentary analysis, triangulating data from legislative texts, government policy documents, media reports, and scholarly literature. This design enables a comprehensive understanding of how cyber threats and responses are framed across state, institutional, and societal levels. Constructivism encourages examining the language and narratives used by policymakers, journalists, and experts, as these discourses reveal social assumptions about authority, vulnerability, and accountability. By mapping these narratives, the analysis identifies recurring themes, such as the tension between transparency and control, that shape cybersecurity governance. The interpretive approach is supported by comparative references to regional and global norms, drawing insights from frameworks such as ISO/IEC 27001 and NIST Cybersecurity Framework. These international standards act as norm carriers, demonstrating how best practices transfer across contexts and are internalised or resisted by national institutions.

3.2. Data Sources and Analysis

Primary qualitative data consist of: (i) official publications from the Bangladesh e-Government Computer Incident Response Team (BGD e-Gov CIRT) and the Ministry of Posts, Telecommunications and Information Technology; (ii) national laws such as the ICT Act (2006) and Digital Security Act (2018); (iii) policy documents including the National ICT Policy (2009) and National Cybersecurity Strategy (2014); (iv) media text for Bangladesh heist coverage. International frameworks used for comparison are NIST and ISO/IEC 2700. Secondary materials include data from international organisation such as the World Bank.

To enhance interpretive credibility, the analysis triangulates legal texts, policy documents, institutional publications, and media reporting, and checks consistency of themes across sources. Media reports are used to capture societal-level harms that are often absent from state security discourse.

The analysis follows a deductive-inductive analysis process. Deductive analysis derived from constructivist concepts, such as constructivist ideas like identity, norm diffusion, legitimacy, and internalisation, and looks for evidence of these in the data. Inductive analysis emerged from textual features within the Bangladeshi context—phrases like "Digital Bangladesh," "cyber sovereignty," and "public confidence." These categories are then used to trace how certain narratives of security become dominant while others remain marginal. For instance, phrases invoking "national image" and "reputation" frequently appeared in legislative and media texts, indicating that the protection of symbolic legitimacy often outweighs user protection in policy discourse. Such findings reveal the cultural underpinnings of policy behaviour.

3.3. Methodological Limitations and Reflexivity

As an interpretive study, this research recognises that its findings are influenced by the researcher's analytical perspective and the availability of data. Since official reports and media coverage often underplay internal organisational dynamics or politically sensitive issues, the constructivist methodology addresses these limitations through reflexivity and triangulation. Reflexivity promotes transparency about the researcher's positionality and its impact on knowledge production, clarifying how interpretations are developed. Consequently, the study prioritises conceptual depth and narrative coherence over comprehensive event documentation.

In summary, the methodology applies constructivist principles by viewing cybersecurity not as an objective fact but as a socially constructed product of discourse, practice, and identity. Through systematic analysis of policy documents and public narratives, the study explores how competing norms, such as control versus transparency and sovereignty versus cooperation, are expressed and shaped within Bangladesh's evolving cyber governance framework.

4. Cybercrime Environment in Bangladesh

Bangladesh's cyber landscape has evolved rapidly in parallel with its broader digital transformation. The expansion of online banking, e-governance, e-commerce, and mobile financial services has generated vast opportunities and systemic vulnerabilities. While the digital economy now contributes significantly to national Gross Domestic Product (GDP), its underlying infrastructure remains susceptible to ransomware, phishing, data breaches, and misinformation campaigns. From a constructivist perspective, this environment is not merely technical but deeply social: how threats are perceived, framed, and narrated shape how institutions define priorities, assign responsibility, and construct accountability. To illustrate this gap, the case of the Bangladesh Bank heist provides a revealing example.

4.1. The Bangladesh Bank Heist and Institutional Preparedness

The Bangladesh Bank heist of February 2016 vividly illustrates this gap between technological advancement and institutional preparedness. The illicit transfer of funds from Bangladesh Bank's account at the Federal Reserve Bank of New York to accounts in the Philippines and Sri Lanka exposed deep institutional vulnerabilities. A Wall Street Journal investigation suggested the possible involvement of an insider within Bangladesh Bank, though the case remains under official investigation [18]. As Khan and Barua note, a further weakness lies in the persistent reluctance of local bank branches to implement the information threat management strategy prescribed by Bangladesh Bank [19]. This disconnect between formal directives and everyday practice illustrates a broader challenge of norm internalisation: cybersecurity continues to be treated as a technical task rather than as an institutional value embedded within organisational culture.

4.2. Transparency, Legitimacy, and the Politics of Disclosure

Beyond financial systems, digital government initiatives like online licensing, taxation, and identity verification have improved accessibility but also increased vulnerability to cyber intrusion. Repeated breaches of citizen data repositories and public portals show that state systems are attractive targets because of the sensitivity and symbolic importance of the information they contain [20]. From a constructivist perspective, such incidents threaten not only confidentiality but also institutional legitimacy. In several cases, officials delayed disclosure for fear that public acknowledgment might damage administrative credibility. For instance, the Bangladesh Bank governor was criticised for failing to inform the country's finance minister about the 2016 heist, which only came to light a month later through media reports in the Philippines [21]. Such hesitation reveals a deeper cultural tension between transparency and authority. However, international practice shows that transparent disclosure coupled with constructive remediation enhances legitimacy rather than diminishes it [16]. When the state sees security as invulnerability, silence becomes a default response; when it views security as accountability, disclosure serves as a sign of competence. As Wendt argues, the meanings that actors attach to their environment determine how they behave within it—self-help and power politics are not given features of anarchy but socially constructed institutions [5]. The ongoing debate about data sovereignty in Bangladesh thus demonstrates a continual negotiation between secrecy and trust within the framework of digital governance.

4.3. Gendered Dimensions of Cybercrime and the Hierarchy of Harm

The same dynamics of legitimacy and authority extend to online gendered harm. Technology-facilitated violence—such as cyberstalking, doxxing, and non-consensual image dissemination—has emerged as a critical yet under-addressed dimension of cybercrime. Reports from the National Human Rights Commission and women's organisations indicate a steady rise in such offences, particularly targeting young women and activists [22, 23]. These incidents are often suppressed due to social stigma and dismissed as personal or moral issues rather than recognised as matters of security, reflecting a patriarchal cultural logic that shapes institutional priorities. From a constructivist perspective, this neglect exposes a hierarchy of harm in which state attention gravitates toward institutional or financial breaches while gendered violence remains peripheral [8, 5]. A normative reframing of online abuse as a public-safety concern, supported by survivor-centred training for law enforcement, could help realign governance priorities, strengthen institutional legitimacy, and reinforce the social foundations of cybersecurity resilience.

4.4. Procurement Practices and the Construction of Cybersecurity Norms

Many vulnerabilities also arise from third-party service providers, subcontracted software developers, and imported hardware with limited traceability. Procurement processes have traditionally prioritised the lowest cost and speed of delivery over verifiable security assurance. From a constructivist perspective, this reflects an embedded culture of meaning-making in which procurement officials and contractors define success in terms of rapid implementation rather than resilient performance. This reflects Onuf's argument that social order is constructed through rules, practices and shared meanings [8]. Institutionalising mandatory security audits, software bills of materials, and independent verification would not only enhance technical compliance but also reconstruct professional norms around responsibility and quality [15, 16]. Embedding these expectations into contractual frameworks could help Bangladesh shift its bureaucratic narrative from reactive control to proactive stewardship—aligning governance practice with a deeper culture of accountability and resilience.

Overall, Bangladesh's evolving cybercrime environment illustrates that technological vulnerabilities are inseparable from institutional culture and social meaning. Incidents such as the Bangladesh Bank heist and recurring data breaches reveal that the most persistent risks emerge not from the absence of regulation, but from the limited internalisation of norms linking transparency, accountability, and trust. The prevailing tendency to frame cybersecurity as a technical or reputational issue, rather than as a shared moral and professional responsibility, continues to constrain systemic learning

and resilience. From a constructivist perspective, strengthening Bangladesh's cyber governance therefore requires a cultural transformation—one that redefines success through openness, ethical practice, and the protection of citizens as integral to national security.

Building on these insights, the next section explores how institutional mechanisms, policy frameworks, and governance practices have sought to respond to these challenges and shape the country's evolving cybersecurity architecture.

5. Cybersecurity Challenges in Bangladesh

Despite significant progress in building digital infrastructure, Bangladesh continues to confront a set of structural and cultural barriers that constrain effective cybersecurity. These challenges extend beyond technical vulnerabilities to include organisational behaviour, policy coordination, and the erosion of social trust. From a constructivist perspective, each of these obstacles represents a contest over meaning—what "security" entails, who bears responsibility for it, and how institutional competence is defined and recognised. Addressing these issues, therefore, requires more than technical reform; it calls for an understanding of the cultural and normative foundations that shape practice. Only by engaging these deeper layers of meaning can cybersecurity interventions achieve both sustainability and legitimacy. The following section examines how governance practices, policy initiatives, and organisational norms have responded to these evolving security demands.

5.1. Institutional Fragmentation and Contesting Mandates

In responding to these emerging security demands, Bangladesh's governance landscape has become increasingly complex, with multiple agencies operating under overlapping mandates. This institutional multiplicity has generated coordination frictions, duplicated reporting channels, and blurred lines of accountability. For example, policy implementation often involves nearly every ministry within the government, creating uncertainty over which entity is responsible for specific actions. Overlaps in programme agendas further contribute to stagnation. Awareness-building initiatives on IT-related business opportunities, for instance, are simultaneously mandated to the Ministry of Science and Information Technology, the Ministry of Agriculture, the Ministry of Fisheries and Livestock, the Bangladesh Association of Software and Information Services, and several non-governmental organisations [24]. From a constructivist perspective, such fragmentation reflects an ongoing contestation of institutional identity, as agencies compete for recognition as the principal guardian of national cyberspace [11]. Normatively, cultivating an inter-agency identity grounded in shared stewardship rather than bureaucratic rivalry would enhance collective resilience. Clear delineation of responsibilities, joint planning mechanisms, and periodic inter-ministerial reviews could therefore transform competition into cooperation, strengthening Bangladesh's institutional cohesion in cybersecurity governance.

5.2. Resource Allocation, Capacity Gaps, and Performance Norms

Budgetary constraints and uneven resource distribution across ministries have produced disparities in cybersecurity capacity. High-visibility projects—such as biometric systems or large-scale monitoring tools—often receive funding preference over capacity-building or maintenance. This pattern reveals an underlying narrative that equates progress with new procurement rather than sustained practice [8]. Furthermore, training initiatives often prioritise hardware maintenance and certification over the cultivation of professional ethics and continuous learning. Weaknesses in procedural law, the influence of vested interests, and the intrusion of political considerations collectively undermine the development of a coherent and accountable cybersecurity governance culture [25]. From a constructivist standpoint, such behaviour illustrates how institutional meanings of success are socially produced, privileging technological expansion over operational resilience. Reframing the budgetary discourse around measurable outcomes, such as detection speed, recovery time, and user trust, could redirect resources toward resilience rather than symbolism [15]. Transparent and outcome-oriented budgeting would also enhance public confidence by demonstrating that cybersecurity investment serves collective rather than partisan interests, reinforcing both legitimacy and trust in governance.

5.3. Public Awareness, Media Narratives, and the Social Construction of Risk

Cyber awareness among citizens and small enterprises remains limited, particularly in rural areas where most of the population resides. Media coverage of cyber incidents in Bangladesh often oscillates between alarmism and silence. Sensational headlines tend to generate moral panic, while institutional under-reporting or prolonged silence fosters public indifference and confusion about the actual scale of risk. Constructivist insight underscores that media discourse co-constructs public understandings of risk and that security behaviour is culturally transmitted rather than innate [13]. Balanced reporting that distinguishes between technical faults and systemic breaches, and collaboration among journalists, regulators, and technical experts, could promote public engagement. At the same time, awareness campaigns that communicate in plain Bengali, employ relatable examples, and frame protective practices as civic responsibilities can help reshape societal norms of digital responsibility. When individuals internalise safe online conduct as a collective

contribution to national wellbeing, resilience becomes not merely a technical goal but a socially embedded norm.

Overall, Bangladesh's cybersecurity challenges reveal that technological advancement alone cannot ensure resilience in the absence of institutional coherence and social trust. The persistence of fragmented authority, uneven resource distribution, and limited public awareness reflects deeper struggles over meaning—how security is defined, enacted, and valued within governance and society. From a constructivist perspective, effective cybersecurity depends not merely on technical defences but on the internalisation of norms that link responsibility with trust and progress with accountability. Cultivating such a normative foundation, through transparent coordination, inclusive policymaking, and civic engagement, would transform cybersecurity from an administrative concern into a shared national ethos, bridging the divide between digital innovation and institutional legitimacy.

Building on this foundation, the next section examines how government policies, legal frameworks, and institutional mechanisms have responded to these challenges, revealing how competing interpretations of security continue to shape Bangladesh's evolving cyber governance.

6. Government Policy and Institutional Effectiveness

Bangladesh's cybersecurity governance has evolved incrementally through successive policy reforms, institutional restructuring, and growing international engagement. Despite this expansion, coherence and accountability remain uneven across ministries and regulatory bodies. From a constructivist standpoint, these limitations stem not only from technical deficiencies but from the competing meanings attached to security, control, and legitimacy. The state's digital identity continues to oscillate between a developmental narrative of modernisation and an administrative logic of surveillance. Having examined the structural and cultural dimensions of Bangladesh's cybersecurity landscape, this section turns to the role of government policy and institutional mechanisms in shaping national cyber governance. It explores how laws, strategies, and organisational practices collectively define what security means in both normative and operational terms.

6.1. Legal and Policy Frameworks: Constructing Control and Legitimacy

The foundation of Bangladesh's cybersecurity governance rests on its evolving legal and policy instruments. Tracing their development reveals how the state's approach to digital security has been informed by shifting interpretations of control, legitimacy, and public accountability. While the ICT Act 2006, the Digital Security Act 2018 and related regulations are designed to address cybercrime, their broad and often ambiguous provisions have generated apprehension among journalists, researchers, and civil society actors. For example, Sections 31(a) and 31(c) of the ICT Act raise concerns about the accountability of the authority responsible for certifying digital signatures. According to these provisions, certifying authorities must ensure the use of hardware and software that are secured against intrusion and must adopt procedures to safeguard the secrecy of electronic signatures. However, the law does not specify what constitutes an acceptable standard of security or how such a procedure should be implemented. This omission creates a legal and procedural gap that undermines clarity and accountability within the digital certification framework. These tensions mirror Wendt's conception of anarchy: security and authority lack inherent meanings, which are constituted through social interaction and the identities that actors construct in relation to one another [5]. In Bangladesh's digital governance, these dynamics are evident in the competing understandings of security—where the state associates it with control and citizens link it to trust—revealing that authority and legitimacy are socially negotiated rather than fixed. Revising vague provisions and embedding clear due-process safeguards could therefore align Bangladesh's cyber laws with international rights norms and strengthen public confidence in digital governance.

Legislation, however, functions not only as an instrument of coercion but also as a signal of values. Laws that balance enforcement with procedural accountability enhance institutional legitimacy and voluntary compliance. Complementing the legal framework, national policy architecture has been shaped by a sequence of strategies—the National ICT Policy 2009, the Cybersecurity Strategy 2014, and the Digital Security Strategy 2021—each aspiring toward a "secure digital Bangladesh". Yet implementation remains fragmented. The policy does not consider 'business process re-engineering (BPR)', which is a system used to analyse and redesign workflows within and between enterprises to optimise the outcome of an organisation's policy [26]. The World Bank Development Report reveals that the attitude and unwillingness of Bangladeshi government officials are holding back the BPR system out of fear that it will erode their supervisory and decision-making supremacy [27]. Constructivist reasoning suggests that policy effectiveness depends on the internalisation of guiding norms by bureaucratic actors [11]. When cybersecurity is perceived as an external technical requirement, policies remain symbolic; when it becomes a professional responsibility, implementation acquires sustainability.

6.2. Policy Implementation and the Culture of Compliance

Policies succeed when implementing actors internalise their core values and turn them into consistent practice. In Bangladesh, however, uneven levels of norm internalisation across agencies have resulted in different performances in detection, reporting, and response. Organisational narratives

often favour compliance over resilience, as ministries under pressure to show visible progress prioritise completing projects or new procurement over long-term risk management and institutional maturity. Constructivist analysis sees this as the continued existence of a performance norm that links success to visibility rather than reliability [8]. Within this administrative culture, compliance often becomes a performative task aimed at satisfying auditors rather than enhancing systemic resilience [16].

These tendencies are compounded by a restrictive legal environment. Overly punitive provisions risk equating dissent with disorder, thereby limiting the civic space vital for participatory digital governance. The ICT Act (2006), especially its controversial Section 57, faced widespread criticism for criminalising online expression through vague definitions of "fake," "obscene," or "defamatory" content—contradicting constitutional protections of freedom of thought and expression while creating ambiguity around privacy rights [28]. Its successor, the Digital Security Act (2018), encountered similar criticism for even harsher penalties. Most of its provisions remain non-bailable, leading to prolonged detention and undermining public trust in digital rights protection. Collectively, these patterns show how the lack of normative coherence—reflected in performative compliance and punitive control—undermines both institutional legitimacy and societal trust. From a constructivist perspective, sustainable cybersecurity governance will depend not on additional regulation but on rebuilding the values and professional identities that underpin policy practice.

6.3. International Engagement and Norm Diffusion

Global and regional cooperation increasingly influences Bangladesh's cyber governance. Participation in the International Telecommunication Union (ITU), Association of Southeast Asian Nations (ASEAN), and Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) cybersecurity programmes introduces domestic actors to transnational norms of incident reporting, capacity development, and human-rights-based governance. Constructivist theory views this process as norm diffusion—the gradual internalisation of international expectations through social learning [12]. The adoption of ISO/IEC 27001 standards and the NIST Cybersecurity Framework shows a move towards global best practice. However, constructivist thought highlights that norms only persist when compliance is based on legitimacy rather than obligation [11]. Effective implementation thus requires local adaptation and professional communities that believe in the value of these standards, not mere procedural mimicry.

As Bangladesh deepens its engagement with global initiatives, translating international frameworks into locally resonant values becomes crucial. This requires not only regulatory harmonisation but also the cultivation of epistemic communities—professionals, policymakers, and technologists—who internalise cybersecurity as a shared responsibility rooted in trust and transparency. Such an approach would bridge the gap between external frameworks and domestic legitimacy, transforming Bangladesh from a rule-taker into a credible contributor to regional and global cyber stability.

Overall, Bangladesh's cybersecurity governance demonstrates that effectiveness arises not from the multiplication of laws or institutions but from the meanings actors attach to them. The persistent gap between policy design and implementation reflects a deeper struggle over what constitutes security, legitimacy, and professional responsibility. From a constructivist perspective, sustainable progress requires moving beyond procedural compliance toward the internalisation of shared norms that prioritise transparency, accountability, and trust. As international standards and regional collaborations continue to shape domestic practice, the challenge for Bangladesh is to translate these external frameworks into locally resonant values that guide everyday institutional practice. Only by reconstructing the moral and professional foundations of governance can the state transform cybersecurity from a reactive system of control into a proactive culture of cooperation.

7. Conclusion

This study demonstrates that cybersecurity in Bangladesh is not solely a technical or legal challenge, but a socially constructed process shaped by norms, institutional identity, and governance culture. Through a constructivist analysis of laws, policies, and public discourse, it shows that prevailing cybersecurity practices prioritise control, reputation management, and state-centric security over transparency, learning, and citizen trust. The central finding is that sustainable cybersecurity resilience depends on the internalisation of norms that value accountability, openness, and shared responsibility alongside technological capacity. Reframing cybersecurity as a collective governance practice, rather than a domain of surveillance and control, is therefore essential for strengthening institutional legitimacy and long-term digital security.

For future scholarships, the findings highlight the importance of interdisciplinary research that examines how social norms influence digital governance. Quantitative assessments of policy effectiveness should be complemented by ethnographic and discourse-based analyses that explore how officials, media, and citizens construct ideas of trust, authority, and accountability. For practitioners, the implications extend beyond technical capacity to the cultivation of institutional culture. Training that promotes transparency, inter-agency cooperation, and responsible communication can help translate cybersecurity from a system of control into a practice grounded in legitimacy and trust.

Abbreviations

ASEAN	Association of Southeast Asian Nations
BGD e-Gov	Bangladesh e-Government Computer
CIRT	Incident Response Team
BIMSTEC	Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation
BPR	Business Process Re-engineering
GDP	Gross Domestic Product
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
ITU	International Telecommunication Union
NCSI	National Cyber Security Index
NIST	National Institute of Standards and Technology
SWIFT	Society for Worldwide Interbank Financial Telecommunication

Acknowledgments

The author appreciates the insights of practitioners and scholars whose public reports and analyses informed this study. The author is also grateful to reviewers whose comments strengthened the clarity, balance, and practical relevance of this article.

Author Contributions

Sahely Ferdous is the sole author. The author read and approved the final manuscript.

Funding

This work is not supported by any external funding.

Conflicts of Interest

The author declares no conflicts of interest.

References

[1] Ministry of Science and Information and Communication Technology. The Information and Communication Technology (ICT) Act, Government of the People's Republic of Bangladesh, 2006. Available from: https://samsn.ifj.org/wp-content/uploads/2015/07/Bangladesh-ICT-Act-2006.pdf [Accessed 7 November 2025].

[2] Ministry of Law, Justice and Parliamentary Affairs. Digital Security Act, Government of the People's Republic of Bangladesh, 2018. Available from: https://basis.org.bd/public/files/policy/5e1653db166e8Digital-Security-Act-2018-English-version.pdf [Accessed 6 October 2025].

[3] National Cyber Security Index. Country profile: Bangladesh. e-Governance Academy, 2021. Available from: https://ncsi.ega.ee/country/bd_2022/ [Accessed 4 October 2025].

[4] Waxman, M. C. Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4), Yale Journal of International Law. 2011, 36, 421-459.

[5] Wendt, A. Anarchy is What States Make of it: The Social Construction of Power Politics, International Organization. 1992, 46(2), 391-425. https://doi.org/10.1017/S0020818300027764

[6] Wheeler, D. A., Larsen, G. N. Techniques for Cyber-Attack Attribution, Institute for Defense Analyses. 2003. Available from: https://archive.org/details/DTIC_ADA468859 [Accessed 8 August 2025].

[7] Lipson, H. F. Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues. Special Report, CMU/SEI-2002-SR-009, Carnegie Mellon University, 2002, 1-71. Available from: https://www.sei.cmu.edu/documents/1827/2002_003_001_13928.pdf [Accessed 3 August 2025].

[8] Onuf, N. World of Our Making: Rules and Rule in Social Theory and International Relations. Columbia, South Carolina: University of South Carolina Press, 1989, pp. 1-341.

[9] Hough, P. Understanding Global Security. 3rd ed. London: Routledge; 2013, pp. 1-490.

[10] The Daily Star, "2 Govt Websites Hacked", July 2013. Available from: http://www.thedailystar.net/news/2-govt-websites-hacked [Accessed 1 September 2025].

[11] Wendt, A. Social Theory of International Politics. Cambridge: Cambridge University Press; 1999, pp. 1-429.

[12] Finnemore, M. National Interests in International Society. Ithaca, NY: Cornell University Press; 1996, pp. 1-180.

[13] Katzenstein, P. J. The Culture of National Security: Norms and Identity in World Politics. New York: Columbia University Press; 1996, pp. 1-562.

[14] Kabir, S. Global ICT Indicators' Status in Bangladesh, Bangladesh Bureau of Statistics. 2014, 1-15.

[15] National Institute of Standards and Technology. Cybersecurity Framework 2.0. Gaithersburg, MD: NIST; 2024, pp. 1-27. Available from: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf [Accessed 4 September 2025].

[16] ISO/IEC 27001: 2022. Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. 2022, Edition 3, 1-19. Available from: https://www.iso.org/standard/27001 [Accessed 2 November 2025].

[17] Finnemore, M., Sikkink, K. International Norm Dynamics and Political Change. International Organization. 1998, 52(4), 887-917. https://doi.org/10.1162/002081898550789

[18] Ejinsight, "Hackers Lurked in Bangladesh Central Bank's Servers for Weeks", March 2016. Available from: http://www.ejinsight.com/20160322-hackers-lurked-in-bangladesh-central-banks-servers-for-weeks/ [Accessed 5 August 2025].

[19] Khan, M. S., Barua, S. The State and Threats of Information Security in the Banking Sector of Bangladesh: Policy Required, Bangladesh Journal of MIS. 2009, 1(2), 1-27.

[20] Rahman, S. ATM Frauds Rattle Banks, Customers, The Daily Star, February 2016. Available from: http://www.thedailystar.net/business/atm-frauds-rattle-banks-customers-510868 [Accessed 3 August 2025].

[21] Bergman, D. Bangladesh Bank Governor Resigns after $81m Hack, Aljazeera, March 2016. Available from: https://www.aljazeera.com/news/2016/3/15/bangladesh-bank-governor-resigns-after-81m-hack?utm_source=chatgpt.com [Accessed 5 October 2025].

[22] Hossain, M. Violence against women rises 74%, News Network, April 2016. Available from: http://newsnetwork-bd.org/newsletter/2016/04/28/violence-against-women-rises-74/ [Accessed 3 August 2025].

[23] Sarker, P., Hasan, M., Akhter, R., Sakir, S. Women's Rights, Gender and ICTs in Bangladesh, Global Information Society Watch. 2013, 70-72. Available from: https://giswatch.org/sites/default/files/gisw13_chapters.pdf [Accessed 5 October 2025].

[24] Ministry of Science and Information and Communication Technology. National ICT Policy 2009, Government of the People's Republic of Bangladesh, 2009. Available from: https://www.scribd.com/document/220439314/ICT-Policy-Bangladesh-2009 [Accessed 3 August 2025].

[25] United Nations Development Programme. Access to Information (A2I) Programme 'Strategic Priorities of Digital Bangladesh', 2011, 1-265. Available from: https://www.amtob.org.bd/assets/resource/research_center/Strategic_Priorities_of_Digital_Bangladesh_Jan_2011.pdf [Accessed 9 September 2025].

[26] Hammer, M., Champy, J. Reengineering the Corporation: A Manifesto for Business Revolution. New York: HarperCollins Publishers, 1993, pp. 1-223.

[27] The World Bank. Making Services Work for Poor People, World Development Report, pp. 1-271. Available from: https://documents1.worldbank.org/curated/en/832891468338681960/pdf/268950WDR00PUB0ces0work0poor0people.pdf [Accessed 20 October 2025].

[28] Badruzzaman, M. Controversial issues of section-57 of the ICT Act, 2006: A Critical Analysis and Evaluation, Journal of Humanities and Social Science. 2016, 21(1), 62-71. https://doi.org/10.9790/0837-21126271