BIISS JOURNAL, VOL. 44, NO. 2, APRIL 2023: 117–141
DOI: https://www.doi.org/10.56888/BIISSj2023v44n2a1
ISSN: 1010-9536 (Print)

Nahian Reza Sabriet

CYBERSECURITY AND PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURES (CI/CII): A FRAMEWORK FOR BANGLADESH

Abstract

Following the fourth industrial revolution, the cyber world and cyber security have become inseparable parts of human lives. At the same time, the growing number of cyber threats compels a state to identify and protect its critical information infrastructure from possible cyber-attacks. This article aims at drafting a framework for Bangladesh's Critical Infrastructure (CI) protection using a four-tiered model. The model incorporates technical level, institutional level, architectural or community level and state level actions to protect the CI institution and prepare for cyber threats based on qualitative research. While explaining the model, it also attempts to build a correlation between cyberspace and national security and the role of CIs in this evolving relationship.

Keywords: Cyberspace, Cyber Security, National Security, Critical Infrastructure, Cyber Insurance, Cyber Protection Framework

1. Introduction

In the digital age, cyber security has become an integral part of a state's security strategy. Bangladesh is now looking at the fourth industrial revolution, where digitalisation, automation, artificial intelligence, and e-governance are some of the routine-mechanisms the country has to adapt to. *The Perspective Plan* (2021–2041) of the Government of Bangladesh (GoB) has given particular emphasis on digital infrastructure, innovation, and strategic transformation in the cyber realm.[1] With the faster pace of development in this field, threats and risks have also arisen. Therefore, it is important to have more detailed and focused studies on specialised cyber-security issues. In this regard, the idea of Critical Information Infrastructure

Nahian Reza Sabriet is Research Officer at Bangladesh Institute of International and Strategic Studies (BIISS). His e-mail address is: nahiansabriet@biiss.org

[1] Government of the People's Republic of Bangladesh, Ministry of Planning, General Economics Division (GED), *Making Vision 2041 a Reality: Perspective Plan of Bangladesh 2021–2041* (Dhaka: Ministry of Planning, 2020)

(CII) or Critical Infrastructure (CI) and its protection from cyber threats are necessary areas to consider.

The United Nations Security Council (UNSC) defines Cyber Security as "proposed solutions (including laws, guidelines, technological safeguards, etc.) to the threats posed by hacking and compromising computer systems".[2] However, in practice, the concept of cyber security has become more inclusive than the definition provided by the UNSC. The International Telecommunication Union (ITU) defines it as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organisation and user's assets".[3] This definition is more applicable here since it looks at the cyberspace as an environment in which multiple organisations and individuals operate.

On the other hand, the GoB's e-Government Computer Incident Response Team (BGD e-GOV CIRT) or the National CIRT (N-CIRT) has addressed CI as "infrastructure that would affect the economic and national security of a country if it were negatively impacted or eliminated."[4] It also refers to the definition provided by the United States (US) Homeland Security which includes both physical and electronic networks, structures and resources. This definition suggests that loss or failure of these infrastructures will impair national security, public health, and economic security, respectively or in a combined manner.[5]

It is important to look at the ranking of Bangladesh in global index of cyber security. Bangladesh has recently climbed up 27 positions in the Estonia based e-Governance Academy's *2021 Cyber Security Index* holding the first position in South Asia.[6] The country also has a comprehensive cyber security strategy adopted for 2021-2025. However, identification and conceptualisation of CI in Bangladesh is

[2] United Nations Security Council (UNSC), Background Guide, *Cybersecurity and International Cybersecurity Legislation* (New York: UNSC), 1.
[3] International Telecommunication Union, "Definition of Cybersecurity," accessed August 16, 2021, https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx
[4] Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT), "Critical Infrastructures and Control Systems: How to Protect?" https://www.cirt.gov.bd/critical-infrastructure-and-control-systems-how-to-protect/
[5] BGD e-GOV CIRT, "Critical Infrastructures and Control Systems."
[6] e-Governance Academy Foundation, "National Cyber Security Index," https://ncsi.ega.ee/ncsi-index/; also see, "Bangladesh Ranks First in South Asia in the National Cyber Security Index," *The Daily Star*, August 23, 2021.

still at "infancy", as pointed out by the Cyber Security Capacity Review of N-CIRT in 2018.[7] Although the Review refers to Bangladesh Power Development Board (BPDB), Bangladesh Bank (Central Bank) and Titas Gas as CI owners, it also mentions the existence of "no official procedures" to identify them. The Information and Communication Technology Division, Ministry of Posts, Telecommunications and Information Technology, Government of Bangladesh has recently enlisted 29 organisations as CIs (for the detailed list, see Annex-1). The 2016 Bangladesh Bank heist is an example of how CIs can be exposed to vulnerabilities that have impacts on state, institutions as well as people.

Against this backdrop, this article addresses a pertinent question: How can Bangladesh protect its CIs from cyber threat? While answering the question, it attempts to identify the strategies to protect CIs through developing consolidated framework. The research will help relevant policymakers in formulating National Information and Communications Technology (ICT) Strategy and other related laws/acts. It will also be useful for the CI owners to frame strategies for protecting their own institutions and make structural arrangements. However, most importantly, it will initiate a dialogue on identification and protection of CIs in Bangladesh. Academically, it upholds a sustainable and needs-based Bangladeshi approach towards cyber-security and CI protection that establishes a balance between traditional and non-traditional security realm vis-á-vis the cyberspace.

The research is qualitative in nature. Both primary and secondary data have been used for the purpose of the research. For primary data, 15 KIIs with relevant stakeholders have been conducted. The list of respondents includes officials from CI institutes,[8] Professors/Directors of the ICT Cell of Dhaka University and Institute of Information and Communication Technology (IICT) of Bangladesh University of Engineering and Technology (BUET), and officials from the ICT Division, Ministry of Posts, Telecommunications and Information Technology. Journal articles, books, legal and policy documents as well as information available in the reports of different organisations and think-tanks have been used as secondary data sources. Collected data were analysed for around six months. The reliability of the research was ensured by respondent validation.

[7] BGD e-GOV CIRT, *Global Cyber Security Capacity Review—Bangladesh, August 2018* (Dhaka: BGD e-GOV CIRT, Global Cyber Security Capacity Centre and Oxford Martin School, 2019), 26.
[8] As mentioned in the N-CIRT Review. The institutions are listed in Annex-1.

It cannot be ignored that analytical and policy making tasks related to cyber security require a clear distinction between technical and non-technical expertise. This article consciously focuses on the issue of CI protection from a security and policy (not technical) perspective. Hence, almost all of the secondary materials have been chosen from journals or books that deal with Security Studies or Public Policy.

The article is divided into five sections. After the introduction, the next chapter outlines and evaluates important pieces of literature in this field. The third chapter outlines the proposed framework. The fourth chapter analyses the framework and explains each unit in detail. The article ends with concluding remarks.

2. Literature Review

Broadly two types of literature can be found on cyber security and critical infrastructure protection. The first type of literature shows how critical infrastructure becomes a bridge between national security and cyber security. The second type of literature focuses on different frameworks for CI protection and challenges related to the implementation of those frameworks or strategies.

Studies on cyber security from defence policy analysis or conflict analysis take a state-centric approach. Vedder looks at "security" as an "unimpaired integrity of an entity itself".[9] This "entity" can range from a mobile device to society and state.[10] Kovacs brings an interesting debate—if rapid modernisation is curtailing state authority, then cyber security concerns are becoming "non-state".[11] However, he refers to state as a "coordinator" and "the highest-level player" in guaranteeing and implementing cyber defence policy. Limba et al. have argued that the entire idea of "critical infrastructure" is to protect elements of "vital national interest" and therefore, state-involvement is a prerequisite here.[12] Moreover, risks may derive from issues beyond technical areas (i.e., corruption, disclosure of information),

[9] Anton Vedder, "Safety, Security and Ethics," in *Security and Law: Legal and Ethical Aspects of Public Security, Cyber Security and Critical Infrastructure Security*, eds. Anton Vedder, Jessica Schroers, Charlotte Ducuing and Peggy Valcke (Cambridge: Cambridge University Press, 2019).
[10] Vedder, "Safety, Security and Ethics."
[11] László Kovács, "National Cyber Security as the Cornerstone of National Security," *Land Forces Academy Review* 23, no. 2 (2018): 114.
[12] Tadas Limba, Tomas Plėta, Konstantin Agafonov and Martynas Damkus, "Cyber Security Management Model for Critical Infrastructure," *International Journal of Entrepreneurship and Sustainability* 4, no. 4 (2019).

which require not only institutional support but also legal intervention.[13] Only state has this kind of resource and penetrative ability.

Cavelty[14] distinguishes between three sets of institutions, which are vulnerable to cyber-attack: (i) computer networks, (ii) business and government networks, (iii) military and different networks. In her discussion, although business and government networks are viewed as primary referent object for intelligence and classified information, CI has been seen as part of defence establishments. However, the ambiguity here is not only related to the referent object; oftentimes, the different sources of the attack and the motives are hardly distinguishable from one another, which Cavelty refers to as the "attribution" problem. Buchanan[15], in his attempt to find out the "national security research agenda" for cyber security, brings in two more variables apart from attribution, namely, "detection" and "interdiction." While detection of a malleable attack is probably one of the key areas of cyber-security protective infrastructure, interdiction is more critical. It demands a holistic understanding which signifies that, in a more critical and complex structure, the same machine learning mechanism used for detecting and defending can eventually learn to delay detection and defence. Over the period of time, the offensive points are getting more and more intricate. Nowadays, cyber threats incorporate combination of generative adversarial networks (GANs) and traditional integrity attacks, data poisoning and data pipeline manipulation which not only attack a particular network, rather can modify input data or reverse training mechanism of the AI.[16]

An actor-centric analysis on the theories of cyber security by Balzacq and Cavelty critiques the format of "speech act" used for agenda-setting at national level.[17] According to them, securitisation of the cyberspace is missing from traditional policy-agenda and policy dialogues. At the same time, the authors have noted that in the cyber-security reports, threats are generally counted based on aggregated infection rate per country.[18] Furthermore, states are also responsible for

[13] Limba et al., "Cyber Security Management Model for Critical Infrastructure."
[14] Myriam Dunn Cavelty, "Cyber-security," in *Routledge Handbook of New Security Studies*, eds. Myriam Dunn Cavelty and Thierry Balzacq (London: Routledge, 2010), 154–162.
[15] Ben Buchanan, "A National Security Research Agenda for Cybersecurity and Artificial Intelligence," *Georgetown University Centre for Security and Emerging Technology (CSET) Issue Brief* (Washington, DC: CSET, May 2020).
[16] Limba et al., "Cyber Security Management Model for Critical Infrastructure."
[17] Thierry Balzacq and Myriam Dunn Cavelty, "A Theory of Actor-Network for Cyber-Security," *European Journal of International Security* 1, no. 2 (2016): 176–198.
[18] Balzacq and Cavelty, "A Theory of Actor-Network for Cyber-Security," 189.

putting restrictions on "cyber-behaviour" and maintaining cyber-hygiene of the population in a given state.[19]

It is evident from existing works that states' interactions with the cyberspace is also evolving. Governing cyber infrastructure compels the state to think about governing a "socio-technical" space.[20] Misinformation and cyber threat campaigns also threaten democratic stability of a country and the digital public sphere. Schünemann[21] divided the impacts in three different levels—micro (individual), meso (mass media) and macro (political discourse). At the macro level, cyber threats can have serious impact on public policy, public psyche and the overall public discourse, thus posing threat to national security as well. Hence, Schünemann gives example of the Russian attempt to misconstrue Western discourse. Nonetheless, this kind of threat can come from any particular state to another state or any particular community to another community, making the spectrum of analysis more complicated than traditional security domains.

Existing studies on protection frameworks are more theoretical and needs-based. Lewis has seen cyber threat on CIs as "weapons of mass annoyance" which can jeopardise both critical state (civil) functions and critical military functions.[22] He has shown how both the US Power Grid and the US Military faced cyber-attacks from terrorists and hackers. A different approach comes from Xu et al. who are in favour of looking at CIs as a domain of network that hosts "multiple interactions" among policies, people, business, culture, and environment where each of them represents a "critical" entity.[23]

Scholarly writings dedicated to the CI frameworks can help a researcher understand why cyber security needs a state-centric approach, why it is being seen as a part of national security and why states' roles are still vital when it comes to cyber security protection, management and governance. Contemporary researchers

[19] Balzacq and Cavelty, "A Theory of Actor-Network for Cyber-Security," 190.
[20] Marie Baezner and Sean Cordey, "Influence Operations and Other Conflict Trends," in *Cyber Security Politics: Socio-Technological Transformations and Political Fragmentation*, eds. Myriam Dunn Cavelty and Andreas Wenger (New York: Taylor & Francis, 2022.
[21] Wolf J. Schünemann, "A Threat to Democracies?" in *Cyber Security Politics*, eds. Cavelty and Wenger, 35-39.
[22] James Andrew Lewis, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats* (Washington, DC: Center for Strategic & International Studies), 2002.
[23] Tie Xu and Anthony J. Masys, "Critical Infrastructure Vulnerabilities: Embracing a Network Mindset," in *Exploring the Security Landscape: Non-Traditional Security Challenges*, ed. Anthony J. Masys (Cham: Springer, 2016), 177–193.

identify critical cyber infrastructure as part of a broader critical infrastructure framework, where national infrastructure is intertwined with cyber capabilities. Mohebbi et al[24] have made content analysis and quantitative study based on 601 published papers and identified organisational or infrastructural interdependency as a key element. Their research highlights two critical infrastructure – transport and water, and their resolute dependency on cyber infrastructure. For example, water and wastewater systems require cyber endeavours for automating supply facilities, monitoring and conveyance; while transport infrastructure require cyber frameworks for transport control systems and detection of vehicle movements. Miron and Muita have opined that attacks impinged upon critical infrastructures can have three types of cascading impacts: direct, indirect and exploitative.[25] Here, direct impacts mostly affect a critical node or network system, but indirect impacts disrupt the functionality of government, the national economy as well as the society.[26] Therefore, "matured" capability models require government interventions along with other stakeholders.

The "market" represents another important issue. Maintaining CI is a costly project. Chung pointed out that, although CI protection framework come from a public administrative body, the infrastructures are owned by many private or business authorities.[27] However, the cost associated to the maintenance of the cyber infrastructure is complex since overspending on low-risk threats and underspending on high-risk threats can ultimately jeopardise the business.[28] A significant economic barrier that the scholars identify is "misalignment". This problem occurs when one system replicates or takes help from the (cyber) security infrastructure of another institution. Moore[29] captures two relevant areas of "misalignment": medical systems where records are procured by insurance companies, and electricity companies where the authorities use the same Internet Protocol (IP) infrastructure as their Information Technology (IT) networks to reduce subsidies. Over the time, these types of interchanges are getting common. As scholars have noted, most technical or techno-

[24] Shima Mohebbi, Qiong Zhang, E. Christian Wells, Tingting Zhao, Hung Nguyen, Mingyang Li and Noha Abdel-Mottaleb, "Cyber-physical-social Interdependencies and Organisational Resilience: A Review of Water, Transportation and Cyber Infrastructure Systems and Processes," *Sustainable Cities and Society* 62 (2020): 102327.
[25] Walter Miron and Kevin Muita, "Cybersecurity Capability Maturity Models for Providers of Critical Infrastructure," *Technology Innovation Management Review* 4, no. 10 (2014).
[26] Miron and Muita, "Cybersecurity Capability Maturity Models," 35.
[27] John J Chung, "Critical Infrastructure, Cybersecurity and Market Failure," *Oregon Law Review* 96, no. 2 (2017): 441.
[28] Chung, "Critical Infrastructure, Cybersecurity and Market Failure," 474–76.
[29] Tyler Moore, "The Economics of Cybersecurity: Principles and Policy Options," *International Journal of Critical Infrastructure Protection* 3, no. 3–4 (2010): 103–117.

commercial part of public critical infrastructure are either owned by or leased to private owners. Black-market botnets are at more advanced stage to infiltrate into any junction of that big communication network and exploit the leeway of data breach or information asymmetry. This can happen to both civil and military infrastructures. Cyber-attacks can also lead to hardware destruction and electromagnetic interference.[30] Using this Denial of Service (DoS) technic, adversaries have claimed minor victories over the North Atlantic Treaty Organization (NATO) during the Kosovo War in 1999.

In summary, existing research on cyber security and CI considers the growing changes in the strategic and operational world of infrastructure governance. Although the number of actors and their interoperability are changing over time, these pieces of literature more or less agree to the fact that "state" as an entity still holds a prominent position in terms of administrative power and responsibility to provide all-inclusive protection to its critical cyber infrastructure.

2.1 *Research Gap*

The most striking research gap here is the dearth of literature from South Asian scholars. Here, the term "South Asian" (and not non-Western) has been mentioned consciously; because, even in the non-Western world, countries in Latin America, East Asia and Southeast Asia have ample literature on CI strategies. Among the available literature, however, there is a tendency to strictly identify the CIs based on either adversaries or the referent object. As a result, for some countries, it completely becomes a traditional security concern ignoring the threats from non-state actors and vice-versa. Therefore, for Bangladesh, it is important to develop a framework that can address threats based on its own empirical research and address attacks coming from multiple levels and both state and non-state adversaries.

3. Proposed Framework for Bangladesh

The study takes state as the referent object. It proposes a four-tier framework inspired by the respective studies of Tabansky and Boudeau et al. However, both frameworks need to be modified for the purpose of this research (Figure-1). The proposed framework is a combination of ideas from these two studies, but not a replication of either of them.

[30] Kenneth Geers, "The Cyber Threat to National Critical Infrastructures: Beyond Theory," *Information Security Journal: A Global Perspective* 18, no. 1 (2009): 1–7.

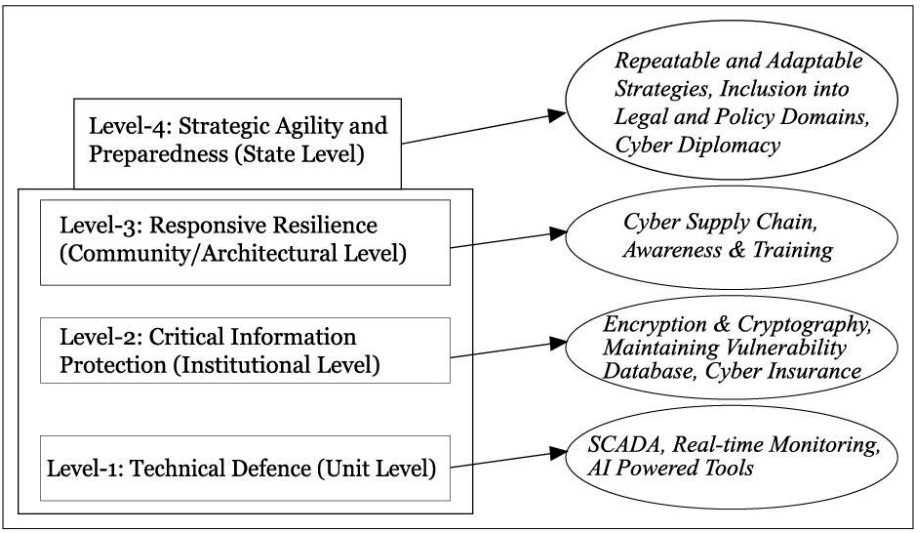
Tabansky aims at understanding the vulnerabilities associated to CIs.[31] He particularly emphasises the "novelty" of threat, which may result in common-cause failure (affecting facilities only in geographic proximity), cascading failure (affecting one particular infrastructure) and escalating failure (attacking an entire network, i.e., the communication network). From his study, he suggests a dual-level framework that involves technical and strategic approaches.[32] Deb Bodeau, Richard Graubart and Jennifer Fabius Greene[33], in their research, have identified five different levels of threats: Cyber Vandalism, Cyber Theft, Cyber Incursion/Surveillance, Cyber Sabotage/Espionage and Cyber Conflict/Warfare. They have also suggested five levels of targeted preparedness for each of them: Foundational Defense, Critical Information Protection, Responsive Awareness, Architectural Resilience and Pervasive Agility.[34]

Figure 1 illustrates the proposed framework. It is divided into four initial stages and a few substages. The first stage represents the unit level. This stage includes application of Supervisory Control and Data Acquisition (SCADA), real-time monitoring and AI powered tools. This stage is useful for fundamental defence mechanism at the technical or operational level. The second stage, "critical information protection", represents the institutional level. Protection measures at this stage incorporate encryption and cryptography, maintaining a vulnerability database and cyber insurance. While the first and second stages primarily illustrate short-time and immediate measures, the third stage illustrates a long-term resilience mechanism through interventions at community-based or architectural level. This stage suggests that people have to be well-informed of the cyber security architecture to complement the strategies formulated by the state. At the same time, since there is a political economy dimension relevant to the cyber architecture, the cyber supply chain needs to be incorporated in this framework. The topmost stage ensures strategic agility and preparedness, and state is the primary actor here. Measures at the strategic level ensures repeatability and adaptability as well as developments at legal, policy and diplomatic levels.

[31] Lio Tabansky, "Critical Infrastructure Protection against Cyber Threats," *Military and Strategic Affairs* 3, no. 2 (2011).
[32] Tabansky, "Critical Infrastructure Protection against Cyber Threats."
[33] Deborah J. Bodeau, Richard Graubart and Jennifer Fabius-Greene, "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels," Paper Presented in *IEEE Second International Conference on Social Computing*, Minneapolis, Minnesota, USA, 2010.
[34] Graubart and Fabius-Greene, "Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels."

The first and the fourth stages in the proposed framework resemble both Tabnsky and Boudeau et al.'s ideas. Only the second stage of the framework has directly been taken from Bodeau's model as it specifically addresses the protection of critical information.

Figure 1: Proposed Framework for Bangladesh's CI Protection against Cyber Threats[35]



The framework shows that, for Bangladesh, a top-down approach is more suitable. There are mainly three reasons behind it. First, in most western frameworks, infrastructural, institutional, or architectural levels operate individually. In those countries, institutions (i.e., Apple, Microsoft, Google) are more proactive in providing responsive awareness and building architectural strength. In Bangladesh, institutional base (Stage 2) of private tech organisations has not developed substantially. These institutions do not have the scope or capacity to take over such responsibilities. On the other hand, the protection framework is dedicated to securing the national interest of the state, and therefore, state is the most relevant stakeholder for coordinating it. Finally, state has the legislative and executive authorities to draft, formulate and implement policy doctrines. Hence, to maintain the coherence among technical, institutional and community level measures, the topmost level has to be independent.

[35] Prepared by author.

4. Analysis of the Framework

This section analyses the proposed Cyber Security and CI Protection Framework for Bangladesh. It discusses the existing conditions of the elements, comparing them with international standards and chalking out future policy options. Its scope is highly focused. It does not venture into mapping all the stakeholders and all policy options. Instead, it offers a primary draft layout which can be used as a basis for future research and policy-mapping.

4.1 *Technical Defence*

4.1.1 *Supervisory Control and Data Acquisition (SCADA)*

Perhaps the most common technical defence mechanism used for critical cyber infrastructure is SCADA. Although it is a supervisory mechanism at the industrial level, it is a useful tool for expanded connectivity that incorporates hundreds to thousands of plants. Among the cyber engineers, SCADA is well-known for its reliability. With its suitable functionality, requirement of activities at the end-user level is very limited.[36]

SCADA is most popularly used in the power generation system. In fact, it was the failure of the US power grid in 2003 that invoked mainstream use of SCADA for controlling the power system.[37] In Bangladesh, SCADA has been adopted for power transmission since the 1990s, yet its application is limited. Bangladesh's journey towards the "smart grid" will help it utilise the SCADA facilities to reduce the cost of electricity transmission in a more secure way. According to the PDB, total 71 incidents of power disruptions took place in Bangladesh between 2017 and 2021.[38] In Bangladesh, SCADA functions within Chattogram, Mymensingh, Cumilla and Sylhet zone, covering 79 sub-stations.[39] PDB is now adopting SCADA Master Control System (SMCS) using optical fibres which will reduce cost by around BDT 227.50 crore every year.[40] The Asian Development Bank (ADB) is involved in

[36] David Bailey and Edwin Wright, *Practical SCADA for Industry* (Boston: Newnes, 2003).
[37] Rajib Baran Roy, "Application of SCADA for Controlling Electrical Power System Network," *University of Information Technology Journal* 1, no. 2 (2003): 85–97.
[38] Bangladesh Power Development Board (BPDB), *Annual Report 2019–20* (Dhaka: BPDB, 2021).
[39] Details can be found in BPDB Annual Reports 2017–18, 2018–19 and 2019–2020, http://bd.bpdb.gov.bd/bpdb/new_annual_reports
[40] "Equitable, Uninterrupted Fuel Supply to Ensure Sustainable Energy System: Nasrul," *The Business Standard*, December 14, 2022.

installation of the SCADA facilities in the Dhaka Electric Supply Company Limited (DESCO) areas and looks forward to complementing the power extension framework taken by the GoB by 2041.[41]

SCADA is also applicable for other public infrastructures that use cyber networks including water reservoirs, traffic signal management, heating and cooling system etc. Dhaka Water Supply and Sewerage Authority (DWASA) has also launched SCADA for online monitoring, control and zone-wise data collection[42] since 2013.[43] In the FY 2020–2021, BDT 147,203,332 was allotted for water supply related (cyber) security management through the Integrated Water Operative Centre (IWOC).[44] However, there was no allotment for sewerage management and monitoring.

From the reports of the relevant CIs and the interviews of the officials, it was evident that SCADA is still being used as a tool for mainly data acquisition, system and enterprise resource planning. However, the usage of SCADA needs to be expanded and properly utilised. It also requires a combination of knowledge and training that can help the authorities transform these aggregated data into security planning. This is discussed later in section 4.3.2.

4.1.2 *Real Time Monitoring*

The discipline of cyber security is heavily dominated by non-traditional security lenses. Due to the lack of a generic referent object, it is often hard to find the scope and focus for these kinds of studies. For cyber security, this becomes more crucial due to the "attribution" problem. As mentioned before, the threat can come from an international hacker group, from another state or even from an engineering fault in the machine learning process. Therefore, real-time monitoring and maintenance is very crucial for ensuring comprehensive cyber security of the critical infrastructure.

---

[41] Based on interviews of Senior Officials from Dhaka Electric Supply Company Limited (DESCO) and BPDB, September 21, 2022. The details related to requirement and restrictions are available at Asian Development Bank (ADB) Social Monitoring Report, *Bangladesh Power System Enhancement and Efficiency Improvement Project: Installation of Supervisory Control and Data Acquisition (SCADA) System in DESCO Areas* (Dhaka: ADB, December 2019).

[42] These zones are called Maintenance, Operation, Distribution and Service (MODS) zones.

[43] Information collected from telephone interviews with Executive Engineers of WASA MODS Zones 1 (Bashabo, Zatrabari, Syedabad, Maniknagar) and MODS Zone 5 (Tejgaon, Banani, Gulshan, Kawran Bazar), March–May 2022.

[44] Water Supply and Sewerage Authority (WASA), *Annual Report 2020–2*1 (Dhaka: WASA, 2022).

A real-time monitoring scheme is primarily developed with an objective of the detection of anomalies, analysis of the cyber threat impacts and formulating mitigation strategies.[45] This mitigation strategy needs to be both preventive and remedial. Ten and Mainmaran have developed a security framework which takes into account both cyber and physical aspects of an infrastructure to gather information while formulating a framework for real-time monitoring.[46] Elements of real-time monitoring models include: security logs, system event logs, file integrity logs, critical alerts and system health notifications.[47] Based on these data, output-anomalies and impacts assessments, mitigation strategies are formulated.

It has been empirically proven how critical real-time monitoring can be for CI protection. Nation-wide power failure and blackout can be caused by poor real-time monitoring and control, dependence on non-synchronised data, quick analysis of the status and being forced to make decisions without any rigorous study.[48] A similar situation was also found during Bangladesh's national power grid failure in November 2022 as a steel mill started to draw electricity from the Ghorashal substation which remained unnoticed and unreported at National Load Dispatch Centre (NLDC).[49] Due to the time-lapse, it was not also possible to cut down power supply from the distribution bases like Dhaka Power Distribution Company (DPDC), DESCO or PDB. If real time monitoring and the consecutive procedures are maintained properly, these issues can be resolved by initiating prompt changes in user privilege and suspending suspicious users.[50]

[45] Chee-Wooi Ten, Govindarasu Manimaran and Chen-Ching Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans* 40, no. 4 (2010): 853–865.
[46] Ten, Mainmaran and Liu, "Cybersecurity for Critical Infrastructures," 855.
[47] Ten, Mainmaran and Liu, "Cybersecurity for Critical Infrastructures," 853–857; Xavier Clotet, José Moyano, and Gladys León, "A Real-Time Anomaly-Based IDS for Cyber-Attack Detection at the Industrial Process Level of Critical Infrastructures," *International Journal of Critical Infrastructure Protection* 23, Issue C (2018): 11–20.
[48] Leandros A. Maglaras, Ki-Hyung Kim, Helge Janicke, Mohamed Amine Ferrag, Stylianos Rallis, Pavlina Fragkou, Athanasios Maglaras and Tiago J. Cruz, "Cyber Security of Critical Infrastructures," *ICT Express* 4, no. 1 (2018): 42–45; Ram Mohan Reddi and Anurag K. Srivastava, "Real Time Test Bed Development for Power System Operation, Control and Cyber Security," Paper presented at *North American Power Symposium*, Arlington, Texas, 2010.
[49] Asifur Rahman, "Not Following Procedure Caused Grid Failure: PGCB Probe Report," *The Daily Star*, October 18, 2022.
[50] Ten, Manimaran and Liu, "Cybersecurity for Critical Infrastructures," 853–855.

4.1.3 *Utilisation of AI-powered Tools*

Utilisation of artificial intelligence (AI) is one of the most contested concepts regarding security and technology. However, AI can be extremely helpful for securing critical cyber infrastructures through proper risk-modelling techniques.[51] First, with automated detection and secure authentication, AI can help in reducing human error. Second, AI is also useful for ensuring faster response, proper management of dynamic load[52] and robust performance. For smooth adaptability and efficiency, AI uses two forms of regularisation programme (implicit and explicit) through which it learns network architecture and algorithm.[53] Finally, AI is also useful for simulation process which can be used for advanced preparedness.

Use of AI powered tools in CIs is not very common. Globally, banks are also using AI tools for Contract Intelligence (COiN) for reviewing documents and legal contracts with the help of image recognition software.[54] In Bangladesh, only one multinational banking institution (Standard Chartered Bank) has been using AI for telecommunication and user-data management.[55] None of the banks mentioned in the CI list (Annex-1) have started full-fledged AI-based activities. It can be understood since using AI in an experimental basis can lead to further unintended consequences. A common problem is the unmanageable velocity of information produced by the banks and the capacity of AI to record and analyse those.[56] For example, in Australia, the AI of a bank failed to report around US$ 19.5 million worth fund transfers that took place within five years.[57]

---

[51] Abdellah Chehri, Issouf Fofana and Xiaomin Yang, "Security Risk Modeling in Smart Grid Critical Infrastructures in the Era of Big Data and Artificial Intelligence," *Sustainability* 13, no. 6 (2021): 3196.

[52] Dynamic loading refers to a mechanism through which a computer program simultaneously loads information, retrieves the addresses and variables, execute functions and unload data from memory.

[53] Jacob Sakhnini, Hadis Karimipour, Ali Dehghantanha and Reza M. Parizi, "AI and Security of Critical Infrastructure," in *Handbook of Big Data Privacy*, eds. Kim-Kwang Raymond Choo, Ali Dehghantanha (Cham: Springer, 2020), 17–26.

[54] George A. Selgin and Lawrence H. White, "The Evolution of a Free Banking System," *Economic Inquiry* 25, no. 3 (1987): 439–457.

[55] ASM Ahsan Habib and Rafiqul Islam, "Artificial Intelligence in Banking: Global and Bangladesh Perspectives," *The Daily Star*, January 06, 2022.

[56] Arvind Ashta and Heinz Herrmann, "Artificial Intelligence and Fintech: An Overview of Opportunities and Risks for Banking, Investments, and Microfinance," *Strategic Change* 30, no. 3 (2021): 211–222.

[57] GRC World Forum, "Australian Banking Giant Westpac Agrees to Pay Record A$1.3bn Fine for AML Failures," accessed August 26, 2022, https://www.grcworldforums.com/main-navigation/australian-banking-giant-westpac-agrees-to-pay-record-a13bn-fine-for-aml-failures/276.article

Application of AI technology through simulation is mostly evident in the military infrastructure. Although no military institution is enlisted as CI till now, the same technology and skill can be used to prepare for probable cyber-attacks. As per Bangladesh Institute of Bank Management (BIBM), in Bangladesh, 72 per cent of online fraudulence take place through the Society for Worldwide Interbank Financial Telecommunications (SWIFT) system.[58] With the increasing pace of banking and fin-tech market, the heightened risk has to be countered with robust preparedness. This preparedness also has to overcome technology-related "overfitting patterns"[59] stemming from bigger "noise to signal ratios" and technical latch as a result of it.

4.2 *Critical Information Protection*

4.2.1 *Encryption and Cryptography*

Encryption and cryptography are required for securing data both at the user and the institutional ends. The encryption mechanism is provided by an institution through a public key and a private key. A significant type of encryption for critical infrastructures is format preserving encryption (FPE). FPE uses a specific "non-standard format" which restricts the process of modification and thus provides security to legacy CI systems which had not been created with advanced security frameworks in the first place.[60] For critical infrastructures, encryption system has to be layered and hierarchical due to their large parameters and countrywide network.[61] These network models also depend on physical infrastructures of a particular area as well as technological developments. Cyber infrastructures, which are countrywide distributed and more widely used, can be accessed and permeated from the hundreds to thousands entry points. Layered infrastructures, through hash-chain functions, follow a principle that only allows the attacker to access data of the compromised devices and not the data of the higher security zones.[62]

[58] Research findings presented at the first ever Cyber Summit organised by the Association of Bankers, Bangladesh (ABB), "Building Cyber Resilience for Banks," Hotel Pan Pacific, Dhaka, June 12, 2022. Lead Researcher: Md Mahbubur Rahman Alam, Associate Professor, BIBM.
[59] Ashta and Herrmann, "Artificial Intelligence and Fintech," 12.
[60] Richard Agbeyibor, Jonathan Butts, Michael Grimaila and Robert Mills, "Evaluation of Format-preserving Encryption Algorithms for Critical Infrastructure Protection," paper presented at *International Conference on Critical Infrastructure Protection*, Heidelberg, Germany, 2014.
[61] Huayang Cao, Peidong Zhu, Xicheng Lu and Andrei Gurtov, "A Layered Encryption Mechanism for Networked Critical Infrastructures," *IEEE Network* 27, no. 1 (2013): 12–18.
[62] Cao, Lu et al., "A Layered Encryption Mechanism for Networked Critical Infrastructures,"14.

Bangladeshi experts are now also focusing on public-key encryption format through Bangla scripts. This idea follows Difffie and Hellman's concept[63] where the public key will be available for everyone, but the encrypted data will only be opened if someone has the private key. This Unicode based character set will provide more secure and specific control over encryption.[64] However, at the institutional end, Bangladesh Standard Code for Information Interchange (BSCII) and Bangladesh Standards and Testing Institution (BSTI) have to make sure that these data follow the ligatures of global Unicode standards.

4.2.2 *Maintaining Vulnerability Database*

The overall scarcity of data is a major issue for the analysts and practitioners working on cyber security. There is no comprehensive dataset or indexing developed for global cyber security concerns. The most cited organisations that develops concrete research and quantitative indexing on cyber security are the International Telecommunication Union (ITU)[65] and an Estonia based think-tank e-Governance Academy Foundation (eGAF).[66] However, ITU takes into account critical infrastructure protection only under the legal pillar of the indexing, ignoring all other components. On the other hand, eGAF's National Cyber Security Index (NSCI) only focuses on confidentiality breach, data integrity breach and denial of e-service. No particular emphasis has been given on critical infrastructures of the nations.

Nonetheless, it has to be considered that a holistic database on CI has to be developed nationally rather than internationally. The concerns related to the protection of CIs is purely a national security issue and, on the other hand, different countries will define and protect their CIs in different ways. An observatory with the combination of different think tanks working on security can be developed for this purpose. Bangladesh Institute of International and Strategic Studies (BIISS) and Bangladesh Institute of Peace and Security Studies (BIPSS) are currently the two think tanks that solely focus on national security issues. Among other relevant think-tanks, there are Centre for Genocide Studies (CGS) at the University of Dhaka,

---

[63] Whitfield Diffie and Martin E. Hellman, "New Directions in Cryptography," in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, ed. Rebecca Slayton (California: Morgan & Claypool, 2022), 365–390.

[64] Sabbir Mahmud, Subrata Kumar Dey and M. Lutfar Rahman, "Implementation of Public Key Encryption Using RSA Algorithm for Bangla," *National Council for Public-Private Partnerships (NCPPP)*, Independent University, Bangladesh.

[65] For details, see International Telecommunication Union, "Global Cyber Security Index," https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

[66] For details, see e-Governance Academy Foundation, "National Cyber Security Index—NCSI," https://ncsi.ega.ee/ncsi-index/

Centre for Governance Studies and Bangladesh Enterprise Institute (BEI). However, most of the CI institutes have their own research wings which can also be pertinent data sources for the development of the index.

4.2.3 *Cyber Insurance*

Following the growing dependency on external networks, and dependency on markets, cyber insurance has become an integral part of CI protection. Building insurance for cyber infrastructures require both market oriented and security-oriented perspectives. At the same time, cyber-risk correlations have to be studied with a view to recovering both hardware and software related losses. For cyber insurance, mostly two types of issues are covered under the umbrellas of "first-party" and "third party" insurance policies (Table-1).

However, the diversity in critical infrastructures and the attribution problem make it hard to adopt an insurance policy that stands in the middle ground between the insurer and the insured. On the one hand, cyber-attacks are continuously adaptive and the nature is ever evolving. When it comes to CIs, insured data and equipment are also too huge to handle. Most insured policies do not have coverage up-to that indemnity limits. Mehr and Cammack has taken up the issue of "insurability" of cyber-risks seriously and identified seven criteria: incidental loss, calculable loss, large number of homogenous units, definite loss, large loss, affordable premium and limited risk.[67] It is very hard to ensure that the risk related to the CIs will follow this particular pattern. A solution in this regard can be achieved if the CIs seek for separate insurance from different providers based on their necessity.

[67] R. Mehr and E. Cammack, *Principles of Insurance* (Homewood: Richard D. Irwin, inc,1961).

Table 1: Cyber Security Insurance Coverage[68]

Type of Insurance	Coverage
First Party	• Loss or damage to digital assets • Business interruption • Cyber extortion • Theft of money and digital assets
Third Party	• Security and privacy breaches • Computer forensics investigation • Customer notification/Public Relations (PR) expenses • Multi-media liability • Loss of third-party data • Third-party contractual indemnification

Since Bangladesh's internal cyber insurance system is at a nascent stage, it is obvious that at least during the early days, the primary providers will be private companies or international organisations. In this case, there is a considerable "information sharing barrier"[69] from the user's (herein, the government) end since a large portion of information regarding the CIs will be highly classified and crucial to the nation's security. In this regard, a national coordination committee or board can categorise the CIs into different sections and formulate integrated insurance policies based on the requirement of each category. For example, for critical infrastructures which rely on distant public outlets (i.e., power grid, water supply networks), have an advantage since their distributive units are separated from each other. As a result, system failure in one unit will not have catastrophic impact on the entire system.[70] On the other hand, institutes that rely on archival data and information (i.e. Prime Minister's office, National Board of Revenue) will require robust focus as single units.

[68] Angelica Marotta, Fabio Martinelli, Stefano Nanni, Albina Orlando and Artsiom Yautsiukhin, "Cyber-Insurance Survey," *Computer Science Review* 24 (2017): 35–61.
[69] Philip Auerswald, Lewis M. Branscomb, Todd M. La Porte, Erwann Michel-Kerjan and Michel Kerjan, "The Challenge of Protecting Critical Infrastructure," *Issues in Science and Technology* 22, no. 1 (2005): 77–83.
[70] Yunfan Zhang, Lingfeng Wang, Zhaoxi Liu, and Wei Wei, "A Cyber-Insurance Scheme for Water Distribution Systems Considering Malicious Cyberattacks," *IEEE Transactions on Information Forensics and Security* 16 (2020): 1855–1867; Elisabeth Paté-Cornell, Marshall Kuypers, Matthew Smith and Philip Keller, "Cyber Risk Management for Critical Infrastructure: A Risk Analysis Model and Three Case Studies," *Risk Analysis* 38, no. 2 (2018): 226–241; Pikkin Lau, Lingfeng Wang, Zhaoxi Liu, Wei Wei and Chee-Wooi Ten, "A Coalitional Cyber-Insurance Design Considering Power System Reliability and Cyber Vulnerability," *IEEE Transactions on Power Systems* 36, no. 6 (2021): 5512–5524.

4.3 *Responsive Resilience*

4.3.1 *Maintaining Cyber Supply Chain*

For the smooth functionality of technical and institutional level protection, maintaining an uninterrupted supply chain is extremely crucial. This part connects the national critical infrastructure network to the global network through market. According to policy makers, cyber supply chains have to be capable of utilising flexibility and redundancy.[71] In other words, relevant institutions have to be able to deploy and redeploy similar strategies to recover from a supply chain disruption during critical moments. "Packet switching" is one of the known options through which data are grouped into small packets and transmitted through digital units.[72] Making the best use of package units at district and local levels can be helpful for taking immediate actions during cyber-attacks. On the other hand, BSTI in collaboration with the Digital Security Agency can provide "electronic certification" based on quality and performance of elements used for CIs to ensure the best outcome of the supply-chain management. Albania has already taken this step meticulously.[73] Nonetheless, proper application of this method requires overall composition of an auditory body and sound cyber professionalism in the business sector.

The cyber supply chain includes human, physical as well as cyber elements. When the supply chain is comprehended, these elements, their roles, risk induced by probable damage and risk measurement units have to be properly identified. For instance, public telecommunication includes communication centres, communication towers, the optical fibres used for running the wireless towers and people who are engaged in operational activities.[74] In the case of Bangladesh, Bangladesh Telecommunication Company Ltd has been proposed as one of the CI institutions. While ensuring smooth functionality of this kind of cyber supply chain,

[71] Paolo Trucco, Boris Petrenj and Seyoum Eshetu Birkie, "Assessing Supply Chain Resilience upon Critical Infrastructure Disruptions: A Multilevel Simulation Modelling Approach," in *Supply Chain Risk Management*, ed. Yacob Khojasteh (Singapore City: Springer, 2018), 311–334.
[72] James A. Lewis, "Cybersecurity and Critical Infrastructure Protection," *Center for Strategic and International Studies* 1 (January 2006): 12.
[73] Ogerta Elezaj, Dhimiter Tole and Nevila Baci, "Big Data in E-Government Environments: Albania as a Case Study," *Academic Journal of Interdisciplinary Studies* 7, no. 2 (2018): 117.
[74] Akhilesh Ojha, Suzanna Long, Tom Shoberg and Steven Corns, "Bottom-Up Resource and Cost Estimation for Restoration of Supply Chain Interdependent Critical Infrastructure," *Engineering Management Journal* 33, no. 4 (2021): 272–282.

insulated human alternatives should also be prepared for working on tasks assigned for automated capabilities.

4.3.2 *Awareness and Training*

Building awareness about cyber security and CIs in general has to be in the core strategic plan. Bangladesh has shown some good progress in this field. The 2020 Cyber Security index of ITU, "capacity development" has been mentioned as the area of relative strength with a score of 17.04 out of 20.[75] Bangladesh Association of Software and Information Services (BASIS) and BD-CERT arrange training and awareness workshop that include participants from the CI institutes.[76] These trainings incorporate representatives of intelligence organisations and community representatives. CI institutes also organise training programme for their own staff. WASA provides training on Operations and Maintenance (O&M), SCADA Reporting Analysis, Data logging, Certificate Course on Core Python, Senior Security Course/2021 and Capability Enhancement on Innovation.[77] Following the creation of Cyber Security Unit (CSU) in 2019, Bangladesh Bank has reportedly planned to open outlets for training and capacity building on cyber security and Banks as critical infrastructure.[78]

However, further emphasis is required on training at university levels. In order to make the youth adept at technical and policy level understanding about cyber infrastructure, particularly the CIs, Cybersecurity can be offered as credit courses. At present, no university in Bangladesh has a department of Security Studies or Cyber Security Studies. At the University of Dhaka, cyber threats and cyber security issues are taught under the "violent extremism and cyber-crime" label as a part of "Non-Traditional Security Studies" course of the "International Security" stream. The Department of Criminology, University of Dhaka also takes a similar approach. The Military Institute of Science and Technology (MIST) has recently launched certificate course on cyber security operation and threat hunting. However, the need to address cyber security concerns from specifically security (not technical) and national (not international) perspective is pivotal. In fact, the entire debate evolving around CIs opens up an opportunity to create a separate discourse on critical national

[75] International Telecommunication Union, *Global Cyber Security Index* (Geneva: ITU, 2022), 81.
[76] Interview with Senior Officials, Bangladesh Association of Software and Information Services (BASIS) Board of Council (2022–23), July 2022.
[77] *WASA Annual Report 2021*, 74.
[78] Interview with Joint Director, Bangladesh Bank, August 12, 2022.

infrastructures and critical cyber infrastructures. Bangladesh's National Cyber Security Strategy (2021-25) also aims at massive investment in the academic sector for producing 250+ graduates, 100+ postgraduates 25+ PhD in cyber security.[79] This project has to be fully implemented in coordination with the Ministry of Education and the University Grants Commission (UGC).

4.4 *Strategic Agility*

4.4.1 *Formulation of Repeatable and Adaptable Strategies*

For building the core strength, strategies related to key infrastructures have to be repeatable and adaptable. In this regard, the relevant policies need to be well aligned. The *National Cyber Security Strategy (2021–25)* addresses the protection of critical information and critical infrastructures through nationwide implementation of Secure Software Development Life cycle (S-SDLC).[80] It also notes down the importance of human resource development, citizen involvement, and IT industry promotions as integral part of the strategy. To chalk out of the coordination plan, in January 2022, a meeting on responsibility matrix was organised by the Digital Security Agency (DSA) of Department of Information and Communication Technology (ICT).[81] More significantly, the strategy calls for a Data Protection Act along with the Digital Security Act, appropriate rules under the acts, guidelines to implement the rules and review of existing rules and regulations for seamless coordination.

The next big challenge in formulating this strategy is to have it well coordinated with regional and global strategic guidelines. Unfortunately, there is no common regulatory platform at the regional level for such guidelines. Europe has shown some significant examples in this respect. The European Union Agency for Cybersecurity (ENISA) is dedicated to the development of a common cyber policy for Europe and enhance capacity building and trustworthiness among the states. It also provides National Cybersecurity Strategy guidelines, research and innovation (R&I) observatory, market analysis framework and standardisation framework.[82]

[79] N-CERT, Bangladesh National Cyber Security Strategy (2021–25) (Dhaka: ICT, N-CERT and DSA, 2022).
[80] N-CERT, Bangladesh National Cyber Security Strategy (2021–25), 12.
[81] BGD C-IRT, "Meeting on Bangladesh Cybersecurity Strategy 2021-2025 Responsibility Matrix," accessed January 23, 2022, https://www.cirt.gov.bd/meeting-on-bangladesh-cybersecurity-strategy-2021-2025-responsibility-matrix/
[82] European Union Agency for Cybersecurity (ENISA), "Cyber Crisis Management," https://www.enisa.europa.eu/topics/cyber-crisis-management

The development in the Indo-pacific region on the other hand is significantly low. The Asia Pacific Group on Money Laundering (APC) under Financial Action Task Force (FATF) partially addresses misuse through "virtual assets", yet it is not well-representative of the entire issue.[83] Although Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) has an expert group on cyber security, the progress is negligible. There is a plan to set up a BIMSTEC CERT by 2025.[84] BIMSTEC can take into account this development as its revamped journey towards securing digital connectivity in the region and formulate a deft cyber security and CI protection guideline for the member states.

Globally, ITU has developed a National Cyber Security Strategy Guide. It necessarily suggests setting up National Cyber Security Agency for the coordination of CI protection.[85] However, it was developed in 2011 and now there is a need for revision. Bangladesh does have a Digital Security Agency and the Digital Security Act designates the Director General of the Agency as the authority in decision making regarding the CIs. The Agency, therefore, also has the authority to come up with a policy document dedicated specifically to the protection of the critical infrastructures.

4.4.2 *Inclusion into Legal and Policy Domains*

CI protection needs a clearly defined legal and policy basis. The DSA dedicates its Chapter V for the protection of the CIs.[86] Article 16 of the DSA illustrates the importance of monitoring and inspection of the CIs. Under Chapter VI, Article 17 outlines "illegal access to any CI" and "by means of illegal access, harm or damage to it" as punishable offense:

> "…punished with imprisonment for a term not exceeding 7 (seven) years, or with fine not exceeding Taka 25 (twenty five) lac, or with both [for the first type of offense]

[83] Financial Action Task Force (FATF), "Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers," accessed January 23, 2022, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets2021.html
[84] BIMSTEC Events, "First Meeting of the BIMSTEC Expert Group on Cyber Security Cooperation met in New Delhi on 14-15 July 202," accessed August 11, 2022, https://bimstec.org/event/first-meeting-of-the-bimstec-expert-group-on-cyber-security-cooperation-met-in-new-delhi-on-14-15-july-2022/
[85] International Telecommunication Union, *National Cybersecurity Strategy Guide* (Geneva: ITU, 2011).
[86] Government of the People's Republic of Bangladesh, Legislative and Parliamentary Affairs Division Ministry of Law, Justice and Parliamentary Affairs, *Digital Security Act* (Dhaka, GOB, 2019), 23327–23329.

> …punished with imprisonment for a term not exceeding 14 (fourteen) years, or with fine not exceeding Taka 1 (one) crore, or with both. [for the second type]"[87]

Bangladesh can make progress through three types of development in this sphere: First, coordination of relevant policies. For instance, Bangladesh also has a National Blockchain Policy formulated in 2017 which is relevant to the CI Banks. It can be streamlined with the cyber security strategy and vice-versa. Second, the Digital Security Agency has to conduct a comprehensive stakeholder mapping and formalise the distribution of tasks, including public-private partnership. Third, with the consecutive developments in the legal domain, the first step towards a cyber- insurance policy or legal guideline can be issued.

4.4.3 *Cyber Diplomacy*

Cyber diplomacy is a comparatively new concept in both cyber and diplomatic world. The term has two connotations—use of cyber tools as means of communications and negotiations among diplomats and executives; or, the use of cyber platform for conducting diplomacy.[88] Although it encompasses the broader arena of cyber security rather than the CI, cyber diplomacy can be utilised for crafting well-coordinated strategies for the countries in the cyber-setting.[89] Under United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)'s platform, Bangladesh, Samoa and Lao-PDR connected to discuss about digital and transport connectivity on 03 November 2019.[90] The programme did not directly address the issue of cyber security; however, it took into account automation, digital connectivity, risk reduction, sustainability and using ICT for social changes. Each of these elements are relevant to different CI institutions. On the other hand, this event addressed the issue of digital connectivity between South and Southeast Asia. The first ever meeting of the BIMSTEC cyber experts also took place in July 2022. In future, through further interactions, an Indo-Pacific platform can be built for protecting the CI infrastructures in the member states and aiming at transnational collective cyber security.

---

[87] *Digital Security Act*, 23328.
[88] André Barrinha and Thomas Renard, "Cyber-diplomacy: The Making of an International Society in the Digital Age," *Global Affairs* 3, no. 4–5 (2017): 353–364.
[89] Ronald Peter Barston, "Cyber Diplomacy," in *Modern Diplomacy* (New York: Routledge, 2019), 112.
[90] United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), Events, *Inception Meeting*, November 3, 2022, accessed December 15, 2022, https://www.unescap.org/events/2022/inception-meeting-digital-and-transport-connectivity-socioeconomic-resilience-rural#

5. Concluding Remarks

This article attempted to propose a broad framework for the protection of critical infrastructures in Bangladesh. Throughout the process, it incorporated ground-level, policy level and normative approaches to provide a broad-brush mapping. However, each of the areas discussed can be further analysed through field based and scientific research. The base research has been dependent on qualitative and subjective interpretation from different concerned authorities. Although "criticality" cannot be quantified, a nation-wide quantitative study could complement it.

The framework has tried to include legal, institutional, community-based, market-oriented and time-sensitive policy options. Since the concept of CI protection is still at a nascent stage, it is time to take into consideration all these multifaceted areas. However, the article keeps its base-framework intact by proving that state has to stay on top of the heap and coordinate technical, institutional and architectural frameworks through strategic planning.

At the national level, the state has to identify and meddle with the large group of stakeholders. The *big-tech vs state regulation* is already a heated debate among the cybersecurity experts. Hence, transcending the market-demands and focussing on national demands have to be properly coordinated. At the individual level, human rights and privacy concerns may boom up. Since critical infrastructures are public infrastructures, processing of data and information sharing have to be properly justified with encryption capabilities. Finally, cost-management has to be ensured through utilisation of optimum energy and technical resources.

Bangladesh's journey from digital to smart Bangladesh involves essential and critical developments in the areas of technology and innovation. However, the entire concept of digital connectivity and cyber security has ushered a new perspective towards security beyond "gates, guns and guards." To capture the demands and values of critical information infrastructure of the nation, one has to understand the intersections between territorial space and cyber space as well as national security and cyber security. By implementing a comprehensive CI protection framework, Bangladesh can indeed become an archetype in this new era of technological revolution where cyber security is being considered as a key global security concern.

Annex 1: List of 29 CI Institutes issued by the ICT Division, (Until October 03, 2022)

1. President's office
2. Prime Minister's Office
3. National Board of Revenue
4. Bangladesh Data Center Company Ltd
5. Bridges Division
6. Department of Immigration and Passports
7. National Data Center of Bangladesh Computer Council
8. Bangladesh Telecommunication Regulatory Commission
9. National Identity Registration Wing of Election Commission Secretariat
10. Central Procurement Technical Unit
11. Rooppur Nuclear Power Plant Establishment Project
12. Biman Bangladesh Airlines
13. Immigration Police
14. Bangladesh Telecommunication Company Ltd
15. Bangladesh Water Development Board
16. Power Grid Company of Bangladesh
17. Titas Gas Transmission and Distribution Company Ltd
18. Bangabandhu Satellite Company Ltd
19. Civil Aviation Authority Bangladesh
20. Birth and Death Registration unit of the Office of the Registrar General
21. Bangladesh Bank
22. Sonali Bank
23. Agrani Bank
24. Janata Bank
25. Rupali Bank
26. Central Depository Bangladesh Ltd
27. Bangladesh Securities and Exchange Commission
28. Dhaka Stock Exchange
29. Chittagong Stock Exchange