THE NATIONAL CYBERSECURITY STRATEGY OF BANGLADESH: A CRITICAL ANALYSIS

Md. Riaz Uddin*****

Abstract

How do we explain and assess Bangladesh's level of preparedness in its cybersecurity measures? This research paper investigates the question by analysing 'The National Cybersecurity Strategy of Bangladesh' - the official document outlining the cybersecurity measures of the country for the upcoming days. The domain of cybersecurity consists of complex interactions among different stakeholders – both public and private. In order to assess the proper interaction among relevant actors and to monitor and implement effective governing policies so that up-to-date cybersecurity systems can be ensured, Government of Bangladesh has aligned its strategy with the five key pillars of Global Cybersecurity Agenda, which were prepared by International Telecommunication Union. Based on these pillars, this research critically evaluates Bangladesh's strategy and finds that this scheme is lagging behind to a large extent from the contemporary practices in worldwide cybersecurity preparedness. Policy recommendations are suggested before the concluding remarks in order to fix the pressing issues and modernise the cybersecurity preparedness of Bangladesh in a timely manner.

INTRODUCTION

Bangladesh has embraced digital services across all sectors at an unprecedented rate. Very few countries in the world have witnessed massive digital orientation of its populace in a short time span like this country. But vulnerability is often an unwanted by-product of rapid transformation. Mitigation of such vulnerability via effective policies is usually considered to be a durable solution. As per the introduction of digital services in Bangladesh, the concepts of security and privacy had to be shed light upon sufficiently. Unfortunately, the Government of Bangladesh (GoB) adopted digitalisation in many sectors without emphasising on important issues like information security and infrastructure development. As a result, this country has faced several massive cyberattacks on its critical infrastructures in the past few years. The recent Bangladesh Bank heist in February 2016 and the latest large scale data theft from the server of Teletalk, a state-owned mobile operator, in November 2017 are just two glaring examples of the unwanted digital incidents that Bangladesh had to witness.

***** **Md. Riaz Uddin**, M.S.S. Student, Department of International Relations, University of Dhaka.

It is important to note that whenever a country appears to be vulnerable to large scale cyberattacks, then it becomes an alluring target for digital delinquents from all over the world. On the one hand, just after a massive cyberattack, there is great possibility that the state's security system is still highly vulnerable. On the other hand, the Government might still be occupied with investigating the earlier attack leaving other critical structures unprotected. For these reasons, Bangladesh is now in a very susceptible position in terms of securing its digital arena.

In order to secure the national cyberspace from internal and external threats, the GoB published The National Cybersecurity Strategy of Bangladesh back in March 2014. Almost four years have passed ever since. A critical evaluation of this strategy is essential now to understand Bangladesh's preparedness in preventing cybercrimes and protecting its cyberspace. In this regard, the central question this paper aims to answer is *how do we explain and assess Bangladesh's level of preparedness in its cybersecurity measures?*

In order to answer the research question, qualitative research method is applied in this study, which involves both primary and secondary data analysis. Interpretative documented analysis combined with content analysis is used in this paper. Moreover, four cybersecurity experts were selected as key informants for in-depth interviews. These interviews portrayed a better understanding of the way which cybersecurity strategy operates, intervenes, and intertwines with national security agendas. Interviews were taken in a semi structured procedure to give the interviewees an opportunity to elaborate on the subject.

Areas covered in the key informant interviews were: (1) how we can explain Bangladesh's cybersecurity strategy from a bird's eye view; (2) how different states have addressed cybersecurity and cybercrime within their policies; (3) Bangladesh's prospect in following contemporary trends in her cybersecurity preparedness; and (4) scopes for Bangladesh to amend and improve its existing cybersecurity policies.

This study is broadly divided into four major segments. A brief discussion regarding contemporary international standards in cybersecurity preparedness unfolds the trend setting advancements in the industry. Another analysis focusing on the legal understanding and cybersecurity in the context of Bangladesh helps to understand what the established policy instruments in the country to counter cybercrimes are. Later on, a critical analysis of Bangladesh's cybersecurity strategy is presented which aims towards finding out the spectrum of policy details and evaluating the document thoroughly. Finally, appropriate policy recommendations are presented which require effective implementation in a timely manner. In short, this study points out to the crucial factors that had to be addressed long before any major cyber incident had the chance to occur in Bangladesh.

CONCEPTUAL UNDERSTANDING

International Telecommunication Union (ITU) published ITU National cybersecurity Strategy Guide in 2011 to define a reference model for countries elaborating new or improving existing national strategies on cybersecurity.[1] The pillars of Global Cybersecurity Agenda (GCA), as shown in Figure 1, were at the heart of that model.[2] The model will be used as a conceptual framework for this study. It sets the stage for collaboration between cybersecurity strategists and a diverse group of stakeholders responsible for national cybersecurity policies.

The pillars depicted in the GCA focus on five major areas. 'Legal Measures' focus on legal institutions and frameworks dealing with cybercrime. 'Technical & Procedural Measures' cover technical institutions and frameworks dealing with cybersecurity. 'Organisational Structures' centre around policy coordination institutions and strategies for cybersecurity development. 'Capacity Building' emphasises Research and Development (R&D), education and training programmes, and certified professionals and public sector agencies. And finally, 'International Cooperation' entails partnerships, cooperative frameworks, and information sharing networks.

According to the reference model, legal, technical and procedural, and organisational measures are required to be undertaken at the national and regional levels. But they are also to be harmonised at the international level. The two remaining pillars, capacity building and international cooperation, cross-cut in all areas.

---

1 F. Wamala, "ITU National Cybersecurity Strategy Guide," available at: <http://www.itu .int/ITU-D/cyb/cybersecurity/docs/ITU National CybersecurityStrategy Guide.pdf> (accessed on 23 October 2017).

2 "ITU Global Cybersecurity Agenda (GCA)," available at: <https://www.intgovforum.org/ Substantive_2nd_IGF/ITU_GCA_E.pdf> (accessed on 23 October 2017).