doi: https://doi.org/10.3329/dulj.v32i1.57190

Cybersecurity and Cyber Diplomacy at the Crossroad: An Appraisal of Evolving International Legal Developments in Bangladesh Context

Md. Ershadul Karim
Senior Lecturer, Department of Law, University of Malaya, Malaysia

I. INTRODUCTION

A clearly defined territory, sovereignty, and the security of the state including its subject are very fundamental and less disputed issues recognised by the principles of classical international law.[1] Though it could not be anticipated that the main hallmark of the Third Industrial Revolution i.e. the information and communication technologies (ICTs) would create any genuine challenge in this regard, things started to change dramatically when the Internet was made open for general use in the mid-1990s with the introduction of the World Wide Web. The ICTs, the most important scientific innovation having a similar impact like electricity, and an enabling, disruptive, and general-purpose technology,[2] have the prospects to assist in achieving every single goal listed in the United Nations Sustainable Development Goals (UN SDGs).[3] However,

---

1 *Corfu Channel* case, Judgment of April 9th, 1949: I.C. J. Reports 1949, 4; *Nicaragua Case, 1986 I.C.J. Rep 14 (1986)*; *Nicar. v. Costa Rica), Judgment, 2015 I.C.J. Rep. 665 (2015)*; Schmitt M and Vihul L, 'Respect for sovereignty in cyberspace' (2017) 95 Texas Law Review 1639.
The concept 'national security', started with the creation of the Westphalian or modern state, focuses on protection of state values or the prerogatives such as "territory, sovereignty, foreign policy interest and national economy" from e.g., outside arms attacks which amount to the commission of internationally wrongful act having legal consequences. Mijalković S and Blagojević D, 'The basis of national security in international law' (2014) NBP Nauka, bezbednost, policija 49-68.

2 Generally speaking, enabling technologies promise to offer radical changes in performance ability of anything, including existing technologies. Disruptive technologies promise to change the operation behavour of anything including human being, business and industries significantly. General purpose technologies virtually can be used everywhere and can affect everything in an economy.

3 According to the United Nations Development Program and UN ICT Task Force, "ICTs are basically information-handling tools – a varied set of goods, applications and services that are used to produce, store, process, distribute and exchange information. They include the "old" ICTs of radio, television and telephone, and the "new" ICTs of computers, satellite and wireless technology and the Internet. These different tools are now able to work together, and combine to form our "networked world"– a massive infrastructure of interconnected telephone services, standardized computing hardware, the Internet, radio and television, which reaches into every corner of the globe." See, 'Tools for Development Using Information and Communications Technology to Achieve the Millennium Development Goals' (2003) United Nations ICT Task Force Working Paper, December 2003 <http://www.itu.int/net/wsis/stocktaking/docs/activities/1103056110/ICTMDGFinal.pdf> accessed 1 March 2021.
The Internet, interconnection of computer networks, was initially invented for military use and subsequently expanded for academic purpose. In the mid-1990s, it was made open for general, public and commercial use. For an authoritative history of the Internet, please see, Leiner BM and others, 'A brief history of the Internet' (2009) 39 ACM SIGCOMM Computer Communication Review 22.

the ICTs are dual-use products i.e. can be used for both good and evil purposes, and a conventional product that can be weaponised, very easily available and accessible, and are not expensive like other dual-use products/items such as nuclear technology, arms, and chemicals, etc. While the combination of ICTs and the Internet has shaped the lives of millions in every corner of the earth diminishing the apparent inequalities through the 'digital revolution' which is often showcased as the laurel of success by the policymakers of all levels, this combination, on the flip side empowers anyone interested to enter the cyberspace of another country using various devices and applications and cause economic and socio-political damages through unauthorized access to the ICT systems, sometimes having catastrophic impacts.[4] Thus, the ICTs are additionally projected as double-edged sword.

Though some forms of cybercrime can be committed individually or by a small group of technerds having limited ideas or incomplete understandings about the consequences, various forms of cybercrimes are white-collar organized crimes and a multi-trillion-dollar industry.[5] Due to the complex nature of the cyberspace and diversified use of ICTs in our daily life, it is hard to quantify the overall misfortunes caused due to cybercrimes. While by and large, if not in most cases, the affected parties tend to hide the incident on the fear of trust or reputation issues, some reliable international bodies have shared some figures of consequential financial loss.[6] In the United States of America (USA), the official statement from the Whitehouse revealed that the malicious cyber activity such as denial of service attacks, data and property destruction, business disruption, theft of sensitive financial and strategic information, and intellectual property, etc. cost the private and public entities of the country between USD 57-109 billion only in 2016.[7] The United Kingdom's National Cyber Security Centre estimated that in 2019, the country received on an average weekly ten cyber-attacks, most of which were targeted by the state-sponsored cybercriminals, popularly known as hackers.[8] Bangladesh, with its economy size of USD 3,02,571 million,[9]

---

4 For a list of major international cyberattack and cybercrime incidents till 2013, please see, Marco Roscini, *Cyber operations and the use of force in international law* (Oxford University Press, USA 2014).

5 See, United Nations Office on Drugs and Crime, 'The Globalization of Crime- A Transnational Organized Crime Threat Assessment', (2010) <https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf> accessed 1 March 2021.

6 In a Working paper published in 2018, the International Monetary Fund (IMF) calculated the losses caused to financial institution due to cyberattacks was USD 100 billion. See, Antoine Bouveret, 'Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment', IMF Working Paper, WP/18/143. Renowned Cybercrime Magazine estimates that the financial damage of cybercrime will be USD 6 trillion by 2021. See, Cybercrime 'Damages $6 Trillion By 2021' (*Cybercrime Magazine Report*, 2016) <https://cybersecurityventures.com/annual-cybercrime-report-2017/> accessed 27 November 2021.

7 The Council of Economic Advisers, 'The Cost of Malicious Cyber Activity to the U.S. Economy' (2018) <https://www.hsdl.org/?view&did=808776> accessed 1 March 2021.

8 'National Cyber Security Centre, Weekly threat reports' (2020) <https://www.ncsc.gov.uk/section/keep-up-to-date/threat-reports?q=&defaultTypes=report&sort=date%2Bdesc> accessed 1 March 2021.

9 The World Bank Group, GDP (current US$)-Bangladesh (2019) <https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?locations=BD> accessed 1 March 2021.

experienced one of the worst cyberattacks in global history when USD 81 million was heisted from the Central Bank, Bangladesh Bank in February, 2016. As the classical international law principle of sovereignty applies to cyberspace also,[10] such an attack on the Central Bank, being one of the most important institutions of any government and the ultimate custodian of citizens' fund, should be considered as a clear case of an attack on Bangladesh's sovereignty.

After several cyberattacks and threats in different parts of the world led by both state-sponsored and non-state actors, different countries have started to perceive cyberspace as the *'fifth domain of warfare'* after land, sea, air, and space since 2010, as such an attack is viewed as a threat on state sovereignty.[11] While some scholars are reluctant to acknowledge this new domain of war since in a justly-waged war as happened between states, force is used to cause extreme savagery, destruction, and casualties, etc., these are apparently missing in cyberspace attacks.[12] Besides, due to the technical complexities and technological impediments around cyberspace, the elements of attribution to make any state responsible are technically difficult to establish, if not impossible. Albeit, the reality is that due to various types of cyber threats, countries around the world, irrespective of size and economy, have been suffering badly. Such a context compelled various countries to set up a dedicated workforce sometimes referred to as *cyber-army*, a group of highly skilled computer professionals employed with necessary arrangements and infrastructures to protect and maintain the national cyberspace secured.[13]

Technically speaking, because of its ever-dynamic nature, it is realistically difficult to

---

[10] United Nations General Assembly, Note by the Secretary-General, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/68/98, 24 June 2013; United Nations General Assembly, Note by the Secretary-General, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, A/70/174, 22 July 2015.

[11] In 2010, in the briefing of Jul 1st, 2020 edition, The Economist depicted computer mouse and keyboard as the new weapons of conflict in the fifth domain of warfare i.e. cyberspace. See, 'Cyberwar: War in the fifth domain' *the Economist* (London, 1 July 2010) <https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain> accessed 27 November 2021. Since 2011, the Department of Defence of the United States of America has been officially incorporating the new domain into its planning, and the North Atlantic Treaty Organization (NATO) started to acknowledge cyberspace as an operational domain since 2014.

[12] *See*, for example, McGuffin C and Mitchell P, 'On domains: Cyber and the practice of warfare' (2014) 69 International Journal 394

[13] Some of the cyberwar superpowers are United States, China, Russia, Israel, the United Kingdom, North Korea and Iran who developed the cyber capabilities and have been investing more realising the importance of protection of devices and critical information infrastructures such as transport sector, information communication and telephone sector, utilities, energy, healthcare, finance and insurance sectors. *See*, Aschmann M, van Vuuren JJ and Leenen L, 'Towards the establishment of an African Cyber-Army' (2015) 14 Journal of Information Warfare 15; Keith Breene, 'Who are the cyberwar superpowers?' (*World Economic Forum*, 4 May 2016) <https://www.weforum.org/agenda/2016/05/who-are-the-cyberwar-superpowers/> accessed 1 March 2021; Lesley Seebeck, 'Why the fifth domain is different' (*Australian Strategic Policy Institute*, 2019) <https://www.aspistrategist.org.au/why-the-fifth-domain-is-different/> accessed 1 March 2021.

calculate the depth and size of the cyberspace or infosphere alongside the ICTs devices introduced and globally used precisely. So is the variety of legal and regulatory issues and the actors involved in this sector. Yet, some relevant issues in this regard can be identified from the indexes published by different authoritative global organisations. Accordingly, different countries have been taking various measures, reviewing and updating their cyber or information security landscape within their financial and technical capabilities to garner the best of ICTs in attaining UN SDGs and to shield their cyberspace from outside attacks, though there is, unfortunately, no perfect and completely secured system/solution.

Bangladesh, being an active member of the United Nations (UN), is entitled to enjoy sovereignty within the territorial limits and to remain secured from outside attacks including a cyberattack. Simultaneously, articles 27 and 31 of the Constitution of Bangladesh, 1972 dealing with the equal protection of the law, and article 32 dealing with the protection of the right to life and personal liberty impose a duty and obligation on the State to protect and safeguard a citizen of the Republic and to ensure his security.[14] Thus, following others, the governments of Bangladesh have been taking various initiatives since the 1990s to make the best use of ICTs products and services. The present government has been taking various technological and legal measures in line with its political motto epitomised in the election manifesto i.e., 'Digital Bangladesh by 2021',[15] to make cyberspace secured to harness the optimum benefits of the ICTs.

In the first Global Cybersecurity Index, launched by the International Telecommunication Union (ITU) in 2014, Bangladesh positioned 53, which should be applauded considering the socio-economic foundation of the nation. The situation, tragically, started to deteriorate subsequently and the country slipped to 78, 74, and 147 in the Global Cybersecurity Index, National Cyber Security Index, and ICT Development Index released by the ITU respectively, and 112 in the World Economic Forum's Network Readiness Index. However, the government took some initiatives and the recent rank of the country improved significantly to 42, 53, 147 and 105 respectively.[16] The rankings in these indexes indicate that even with some improvements, there are some gaps, limitations, and challenges in Bangladesh's existing cybersecurity legal regime which demand an investigation.

As Bangladesh has been approaching to be more digitalized steadily, the country has been experiencing cyber threats frequently. In many such occurrences, even after the availability of legal and technical solutions, Bangladesh seems to be helpless due to non-cooperation from other countries. For example, in the 2016 Bangladesh Bank incident, though it is strongly believed that the North Korean cybercriminals alongside

[14] *Tayazuddin and another v The State* 21 BLD (HCD) 503.

[15] Even though the present government deserves the credit to effectively utilise the 'Digital Bangladesh' slogan starting before the national election in 2009, all the previous governments since 1990 have contributions in popularising ICTs in the country. For a history of ICTs and the Internet in Bangladesh, see, generally, Karim ME, *Cyber Law in Bangladesh* (Wolters Kluwer 2020).

[16] See generally, National Cyber Security Index (2020) <https://ncsi.ega.ee/country/bd/> accessed 27 November 2021.

their Filipino allies committed the heist, Bangladesh could not recover the full amount but only USD 15 million,[17] due to the concept of 'attribution' needed to be established to make any state responsible under the public international law and non-cooperation from other countries. The existing tools available that could be utilized in a comparable circumstance e.g., the extradition treaty, mutual legal assistance or cooperation, etc. were found to be genuinely ineffective since such threats can be sourced from more than one jurisdiction. Hence, Bangladesh can consider the new idea which is brewing in other parts of the world i.e., 'cyber diplomacy', which also requires an examination and evaluation in the context of the initiatives taken by the government to make cyberspace more secured for the inhabitants.

In this backdrop, this paper aims to present relevant issues, challenges, and concerns around cybersecurity, and the legal tools available and utilized by different countries, including Bangladesh, in addressing those, and their efficacy in the context of cyberspace or infosphere. To accomplish these, the paper is partitioned into five sections, including an introduction and conclusion. Before delving deep into the existing challenges in the regulation and governance of cyberspace, Part two sets the scene and discusses distinctive technical issues, while Part three deals with the legal and regulatory issues, and challenges within the cyberspace landscape. Part four covers cybersecurity issues and an assessment of the initiatives taken in the Bangladesh context while sharing some policy directions.

This paper, in short, endeavours to project that though there are shreds of evidence of some advancement in cybersecurity at the domestic level, much more should be done to attain the political commitments of the government i.e., making the country completely digitalised. This paper features that while many governments started the process of securing cyberspace long ago in a systematic and coordinated manner, the Bangladesh government has only taken some systematic legal and technical steps recently, which promise to protect the country in reducing some of the inbound security threats. However, to reduce cross-border cybersecurity threats, there is no alternative than to promote cybersecurity culture among the citizens, enhance cooperation between countries by joining the relevant organization and initiatives, express this issue in the bilateral or multilateral treaties, including bilateral investment treaties (BITs); and to consider introducing cyber diplomacy immediately.

II. UNPACKING CYBERSECURITY: TERMINOLOGIES AND TECHNICAL ASPECTS

A discussion on the relevant terminologies and the technical aspects regarding cyberspace is unavoidable as there are some apparent misconceptions among the stakeholders in this regard. Some words e.g., data and information, electronic (or, very shortly 'e' or 'E'), cyber and digital, etc. are used synonymously and/or interchangeably in the common parlance.[18] Such misconceptions may create some

[17] Nurul Amin & Shafayat Hossain, 'Not much progress in recovering Bangladesh Bank's stolen money' *the Business Standard* (New Delhi, 4 February 2020) <https://tbsnews.net/economy/banking/ not-much-progress-recovering-bangladesh-banks-stolen-money-41711> accessed 1 March 2021.

[18] For example, sections 22 & 23 of the Digital Security Act, 2018 deal with digital or electronic fraud

inevitable circumstances, even for the security professionals which may tax huge leaving the information system vulnerable in the long run.

While the word 'data' is used in many different contexts to denote different things, in the ICTs literature, it is generally used to mean processed information such as word, number, picture, knowledge, facts, concepts or instructions etc.[19] However, when these 'data' are refined and can be interpreted in a given context to enable someone to derive some meaning, these data can be considered as 'information'.[20] 'Information' can be both digital/automated and analogue/manual. Apparently, the data is used in digital or electronic systems, though information can be manual.

The word 'digital' is theoretically used more in an ethical context e.g. digital divide, whereas the word 'electronic' is used to mean the commercial or business aspects, and 'cyber' is used to mean the security aspects of the ICTs, when these are connected to the Internet.[21] Therefore, from the understandings above, one can reasonably envisage differences between 'data security', 'cybersecurity', 'digital security', and 'information security' etc. This is because one may observe that e.g., in the case of bank management, the regulators impose obligations to adopt separate cybersecurity and information security policies.

From a security context, the concept 'information security' means the security of the contextualized data, and focuses on confidentiality, integrity, and availability of the information (popularly known as the CIA Triangle). Whereas the concept 'cybersecurity' includes the protection of digital information and also digital assets which are considered non-information, but vulnerable through ICTs e.g., computer system and network, etc. An exact definition of 'cybersecurity' is difficult to craft and even the international organisations are unable to succinctly define it, though some features or characteristics can be shared.

The ITU's recommended definition considers 'cybersecurity' 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 organization and user's assets" such as

---

and cheating.

19 In the context of computer, data means any information, knowledge, facts, concepts, or instructions processed or capable to be processed that can be converted through binary coding system. Section 2 (10) of the Information and Communication Technology Act, 2006 (Act no. 39 of 2006) defines "data" as "a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed, or has been processed in a computer system or computer network, and may be in any form including computer printouts, magnetic or optical storage media, punch cards, punched tapes or stored internally in the memory of the computer."

20 The words 'data' and 'information' are popularly used interchangeably in the context of personal data or information protection literature to mean some of the relevant data or information of the natural individual human being in general and a very specific human being respectively.

21 In the context of Bangladesh, it seems that as the government has been using 'digital Bangladesh' as the political slogan and has been promoting the 'digital Bangladesh' brand, the government prefers to use the word 'digital' instead of 'cyber' in all the legal and policy documents bypassing the global trend.

"connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment". With the objectives to make assets and properties available while maintaining their integrity and confidentiality, the purpose of cybersecurity is to ensure the "attainment and maintenance of the security properties ...against relevant security risks in the cyber environment.[22] Thus, the concept 'cybersecurity' covers all aspects of information, data, technology, server, device, software, hardware, hard disc, cloud, network, the internet, etc. which are digitally connected and can be exploited to ensure data integrity and authenticity. In most of the information landscape, initiatives are taken to ensure the protection of CIA Triangle and these three, along with two additional elements i.e. authentication with uniquely identified personal information, and the inclusion of logbook through which the presence of anyone in the cyberspace can be identified are the main elements of cybersecurity. Finally, the phrase 'digital security' means the security of digital devices or digital systems.[23] Thus, it is evident that these are different things even though they are used interchangeably.

After terminologies, a technical discussion in an easy language is desired to understand the complexities in the effective regulation or governance of cyberspace. The precise origin of the word 'cyber', which generally denotes anything relating to the Internet, is unknown; so is the vastness of the web cyberspace, a domain consisting of interdependent networks of IT infrastructure i.e. the Internet, telecommunication networks, computer systems and embedded processors and controllers, etc. through the Internet.[24] Five components (i.e. geographical, physical network, logical network, cyber persona, and persona) in three layers (physical, logical, and social) generally define cyberspace.[25] While the non-technical people may consider website security as cybersecurity, these are different things as the websites are a very small component of the whole cyberspace ecosystem.

The websites we surf are placed in the logical layer. In terms of content accessibility, the web has again three layers i.e. surface web, deep web, and dark web. It is the surface

[22] International Telecommunication Union, 'X.1205: Overview of cybersecurity' (2008) <https://www.itu.int/rec/T-REC-X.1205-200804-I> accessed 27 November 2021.

[23] Section 2 (k), the Digital Security Act, 2018. The law further defines 'digital' as the 'working procedure based on binary system (0 or 1) or digit based system, and . . . electrical, digital, magnetic, optical, biometric, electrochemical, electromechanical, wireless or electro-magnetic technology will be the part of it' [section 2(i)].

[24] It is believed that the word was derived from the word 'cybernetics', first used by the American mathematician, Nobert Wiener in 1948, having Greek origin, meaning the theory of control and communication in living beings and machines. For a historical background on the origin on how Wirner used the word 'cybernetics' in the context of World War II, see, Bynum TW, 'Computer ethics: Its birth and its future' (2001) 3 Ethics and Information Technology 109-12.

[25] In the *physical layer*, telecommunication structures, hardware, and infrastructure ensure the interoperability of the network and different other devices e.g., server, router, ICTs, etc. The *logical layer* ensures the logical connections of every device i.e., various ICT devices, network appliances, and websites having an IP address. The *social layer* is comprised of a persona and cyber persona. While 'persona' means the people, who use a common network collectively, and 'cyber persona' indicates an individual with his identification e.g., email address, computer IP address, mobile number, etc. Thus, with the possibility of more than 'cyber persona', the number of 'cyber persona' can be more that the number of natural human beings.

web, which is only 4% of the whole web, where general people have access and there are more than 2 billion websites, which increase at the rate of around 400 new websites every minute.[26] The web cyberspace is dynamic and ever-evolving with the introduction of different devices. Using the super powerful and sophisticated tools, techniques, applications, and devices, etc. crimes can be committed in cyberspace from anywhere in the world, having devastating effects on the targeted objects, including implications on national security and sovereignty. Such innovative security challenges dubbed as cybersecurity is an extension of cybercrimes.

An ideal Cybersecurity Framework, promoted by the ITU Global Cybersecurity Agenda (GCA), should have five interrelated and coordinated arms.[27] These are- (a) *legal*, where a country should enact a legislation on cybercrime and cybersecurity containing provisions on spam regulation, (b) *technical and procedural measures*, where a country should establish CERT/CIRT/CSIRT, develop standards implementation framework, appoint a standardized body, adopt technical mechanisms and capabilities to address spam, use cloud for cybersecurity purposes, and employ child online protection mechanisms, (c) *organizational measures/structures* where a country should have a national cybersecurity strategy, along with an established responsible agency, and cybersecurity metrics, (d) *capacity building measures*, where a country needs to take public awareness campaign, framework for the certification and accreditation of cybersecurity professionals, professional training course, educational program or academic curricular, research and development programs and incentive mechanisms in cybersecurity, and (e) *cooperation measures* where the country should enter into bilateral and multilateral agreements, participate in international fora or associations, foster public-private partnerships, Interagency or intra-agency partnership, and adopt best practices.

In short, a cybersecurity framework must have clear objectives, action plans, reference of measures (legal, procedural, technological, and institutional), and responsibilities of the institutions designed to safeguard systems, networks, services, and data, etc. While cybercrime legislation deals with rule of law, human rights, crime prevention, and criminal justice, etc., the purpose of cybersecurity legislation is more about national interest and security, trust, resilience, and reliability of ICT. The way different forces have been working in promoting security within the national territory of a state, cybersecurity mechanisms need to be employed similarly to make different stages of cyberspace such as network, server, application, and database, etc. secured.

III. REGULATION TOWARDS SECURED CYBERSPACE AND INTERNATIONAL LEGAL DEVELOPMENT: AN OVERVIEW

[26] One of the most reliable and widely consulted live interactive database, which assist in monitoring different aspects such as the number of Internet users, users of various social media platforms, different ICTs devices computer, smartphone, tablet, etc., total number of websites, hacked websites, blog posts, electricity used, and CO2 emissions etc. See generally, Internet Live Stats <https://www.internetlivestats.com/watch/websites/> accessed 21 November 2021.

[27] International Telecommunication Union, Global Cybersecurity Agenda, <https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx> accessed 1 March 2021.

It is impractical for the discussion to accommodate all the relevant legal and regulatory issues regarding cyberspace as they are too uniquely diversified to cover in this article. Therefore, this paper will provide an overview of some of the selective and relevant events/issues. At the international level, even though the ITU, one of the oldest international organisations in operation, has been playing a significant role in shaping the regulations of the technological aspects of the telecommunication infrastructure which is a backbone of cyberspace, the vertical regulation of international law covering other areas in this regard is absent. After the Internet was made available for general use in the mid-1990s, the global community started a concerted move almost immediately. In 2003, in the framework of the World Summit on Information Society, it was pledged to achieve a "people-centred, inclusive and development-oriented Information Society [...] premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights". Nevertheless, even after almost two decades, the Internet is a largely legal vacuum and every country has been struggling to find out the effective form of regulation and the regulatory tools in this regard.

With the vastness of the web in cyberspace, the issue of regulatory tools and measures are also progressing at various levels focusing mainly on the five integrated areas proposed by the ITU GCA shared above. From the ITU's GCA, it is evident that law is only an enabling tool in the effective regulation and governance of the cyberspace ecosystem and therefore, it will be relevant to understand the regulatory and legal issues involved, and the challenges faced by governments in implementing these. While the words 'governance' and 'regulation' are used interchangeably, the word 'regulation' is part of the term 'governance', which deals with the role of the state, the authority of its institutions, and its use of legal rules. Legitimacy, accountability, and authority are important normative attributes of governance.

Due to the magnitude of the Web cyberspace and the actors involved along with the rapid developments in the sector, the effective or suitable way of 'regulation' of the cyberspace is a very complex, perplexing, and contentious issue. There are three main theories of cyberspace regulation- liberal institutionalists, cyberlibertarians, and statists. *Liberal institutionalists* advocate for an international institution and rule-based multilateralism in managing cyberspace, *libertarians* propose to make cyberspace free from oppressive regulation that may restrict the liberty of people in the infosphere, and *statists* feel that the state, being the most important subject of international law, should take the responsibility to govern cyberspace.[28] However, a close look at the relevant regulatory framework of any country in the world will reveal that a better regulatory framework shares some features of all these three theories and there are combinations of strict state regulations in selected sectors, institutional and industrial self-regulation in some sectors, and there are free spaces where the netizens can share ideas freely.

As cyberspace regulation has been a very complicated issue, only selected issues are regulated at the international level while most of the issues are left in the hands of the individual states. After the historic terrorist attack on September 11, 2001, the global

[28] Reardon R and Choucri N, *The role of cyberspace in international relations: A view of the literature* (2012).

community started to consider the state control of online information.[29] From the Global Cyber Strategies Index, developed by the USA based Think Tank, Center for Strategic & International Studies, it can be revealed that at least 78 countries have national strategies, 31 countries have military strategies, 35 countries have content related strategies, 113 countries have privacy-related strategies, 63 countries have strategies on critical infrastructure, 114 countries have strategies on commerce and 91 countries have strategies on crime.[30] Yet, almost every country has been suffering to control various forms of crimes committed in cyberspace.

There is a close relationship between globalization,[31] economic development, and crimes.[32] The cybercriminals take the chances of weak legal and regulatory systems, and technological weaknesses, as can be seen in developing economies.[33] Besides, the easy and cheap access and the dual-use nature of the ICT products e.g. software, hardware, and devices pose serious challenges for the regulators and law enforcement agencies making the ICT products a double-edged sword.

With the ever-increasing number of internet and smartphone users, the risks of cybercrimes are also increasing. From various live interactive cyber threat maps available, it can be seen that different types of cyber threats, both successful and attempted, are a common phenomenon nowadays.[34] The situation gets worse when such cyber threats are committed in an organized manner from multiple jurisdictions. In such circumstances, despite the affected countries having the necessary technical and technological capabilities and good faith, it is somehow impossible to investigate and prosecute the criminals.

Technologically speaking, anyone can access any live website hosted anywhere in the world using the correct web address. These websites can be accessed only through a

---

[29] Watney M, 'The evolution of Internet legal regulation in addressing crime and terrorism' (2007) 2 Journal of Digital Forensics, Security and Law 3.

[30] 'Global Cyber Strategies Index' <https://csis-website-prod.s3.amazonaws.com/s3fs-public/Cyber%20Regulation%20Index%20V2%20%28002%29.pdf> accessed 1 March 2021.

[31] Friman HR, *Crime and the global political economy* (Lynne Rienner Publishers Boulder 2009).

[32] Soares RR, 'Development, crime and punishment: accounting for the international differences in crime rates' (2004) 73 Journal of development Economics 155-184.

[33] Kshetri N, 'Diffusion and effects of cyber-crime in developing economies' (2010) 31 Third World Quarterly 1057-1079.

[34] Though there are some limitations of these maps, the cybersecurity professional can use these important tools to strengthen the security systems after evaluating the available information. Some of these maps are- *Kaspersky*, for cyber malware and DDoS, see generally, 'Cyberthreat Real-time Map' *Kaspersky* <https://cybermap.kaspersky.com/>; *Norse Corporation* <https://norse-corp.com/map/>; for infections, attacks and spams, see generally, Bitdefender <https://threatmap.bitdefender.com> accessed 4 December 2020; Fortinet <https://threatmap.fortiguard.com/> accessed 1 March 2021; for malicious and Phishing URL data feed, see generally, *looking glass* <https://map.lookingglasscyber.com/> accessed 1 March 2021.
For a list of significant cyber incidents developed by Center for Strategic & International Studies, see generally, CSIS (*Center for strategic & International Studies*, 2020) <https://csis-website-prod.s3.amazonaws.com/s3fs-public/200901_Significant_Cyber_Events_List.pdf> accessed 1 March 2021.

national gateway, which may be considered as the territorial limit of the country where the website is hosted. Therefore, theoretically, any state should be able to bar the entry of anyone to access any such website and vice versa.[35] However, with an unfathomable number of websites registered and live in every second along with the use of sophisticated technologies and the absence of the proper level of technical understandings and capabilities; many countries, especially from the global south, are unable to protect their national virtual territory confidently. Moreover, due to the theory and philosophy of 'limited government' in modern state functioning, the government cannot interfere in all the private and economic activities of the citizens.

For a government with supporting available reliable technologies, the issue of governance of cyberspace is less troublesome when any cyber threat is committed within one single jurisdiction. The main challenges start when cyber threats are initiated from outside the territorial limit of any country. In such a context, the classical public international law principles and issues of state sovereignty, territory, responsibility and jurisdiction, etc. will arise and need to be settled. Before taking any initiatives/actions, an affected country needs to establish state-sponsorship behind such threats, grounds for use of force as self-defense, etc. Apparently, even after rampant cyberattacks, even the most developed countries have been facing challenges to establish attribution and state-sponsorship, although all countries pledge not to allow their land for e.g. cyberattacks or cyberterrorism. For an affected country, this is thus difficult, if not impossible, to establish the attack unless there is co-operation from the source countries.[36]

Moreover, this is somehow unfortunate that the classical international law principle of state responsibility, though very relevant in the case of cyber-attacks, is not well developed. In the case of cyber threats and cyberattacks, attribution is one of the most important challenges in the making of any state directly responsible and any state cannot be held responsible for the activities of non-state actors such as criminal gangs. Fortunately, the International Law Commission adopted the Draft Articles on the Responsibility of States for Internationally Wrongful Acts in 2001, which has also been referred by the International Court of Justice, etc. Though these are soft law, these cannot be treated as an authoritative document yet as these are still in Draft form. The Tallinn Manual on the International Law Applicable to Cyber Operations provide some insights and is considered to be the most comprehensive guidelines for the stakeholders in this regard; however, this manual is not legally binding on the states.[37]

What is more unfortunate is that there is no internationally binding legal instrument

[35] For example, some countries block some of the websites or web-based services in different occasions or reasons.

[36] UN member states, under article 2(1) of the United Nations Charter, are under an obligation to fulfil in 'good faith' their obligations derived from the Charter.

[37] The very influential 'Tallinn Manual on the International Law Applicable to Cyber Warfare' was developed by a group of nineteen international law experts in 2013. According to NATO Cooperation Cyber Defence Centre of Excellence, the Manual which was subsequently revised and released with the title 'Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations' in 2017 is the most comprehensive analysis on how international law applies to cyberspace.

addressing this issue so far. The United Nations Office on Drug and Crime (UNODC), though recognises multi-jurisdictional cybercrime as organized crime, has not included any definition of 'organised crime' in the Convention on Transnational Organized Crime, 2020. Within the UN, the First Committee of the UN General Assembly (UNGA) has been functioning as an important forum to discuss various issues on state behavior in cyberspace. Russia introduced a resolution in 1998 on "Developments in the field of information and telecommunications in the context of international security" and similar resolutions are adopted almost every year by the First Committee. Besides, the Committee periodically form a Group of Governmental Experts (GGE), the first one being formed in 2004 as the successor of the Group of Governmental Experts on Information Security.[38] Additionally, the ITU established the International Multilateral Partnership Against Cyber Threats (IMPACT) in 2008. An important development in this regard is that the GGE proposed some norms of responsible state behaviour in cyberspace in their reports of 2010, 2013, and 2015.[39] Even though these are the only norms proposed by high impact bodies, these do not have any binding effects. Unlike the GGE, which is a relatively exclusive forum of 25 members, in December 2018, the UNGA established an Open-ended Working Group (OEWG), which is open for all UN member states to participate and discuss ICT related issues in cyberspace which may help in developing an International Cyber Law Convention to help shape the international move on setting the international law norms and rules on e.g. attribution and effective control. This is a wonderful opportunity for all countries in the world, including Bangladesh, to raise their voice towards making a more secured cyberspace. Besides, there are at least twenty regional agreements and initiatives on cybersecurity. [40] The European Convention on Cyber Crime (also known as "Budapest Convention"), the most famous but non-binding instrument, is also open for non-European countries to sign and ratify and the African Union Convention on Cybersecurity and Personal Data Protection (also known as "Malabo Convention") is open for signature for the African countries.

Apart from these selected moves at the international and regional level, a recent trend that some of the industrialized countries and global cyber superpower have been considering the issue of inclusion of cybersecurity issues in their BITs, can be noticed.[41] Moreover, some jurisdictions e.g. Europe has been considering to impose economic sanction due to cybersecurity issues.[42] Thus, these are some of the attempts

[38] The formation of such a committee begins with an expression of interest, after that it has to receive recommendation of the High Representative to the Secretary-General (UNSG), and finally, the UNSG nominates the Committee.

[39] For an overview of different moves taken in this regard, see, Paul Meyer, "Norms of Responsible State Behaviour in Cyberspace." In Markus Christen, Bert Gordijn and Michele Loi (eds.), *The Ethics of Cybersecurity*, (Springer 2020).

[40] For the list of these agreements and initiatives, please see, Internet Governance Forum, 'IGF 2019 Best Practice Forum on Cybersecurity: Cybersecurity Agreements' (2019) 16-17 <https://www.dfat.gov.au/sites/default/files/cyber-submission-best-practices-forum-on-cybersecurity-igf-2-of-2.pdf> accessed 27 November 2021.

[41] Shackelford S and others, 'Using BITs to Protect Bytes: Promoting Cyber Peace by Safeguarding Trade Secrets through Bilateral Investment Treaties' (2015) American Business Law Journal 1.

[42] See for instance, 'Guardian of the galaxy: EU cyber sanctions and norms in cyberspace' (2019)

different jurisdictions have been trying to consider in the absence of any binding international instrument that the UN member states can adhere to ensure cyberspace more secured.

IV. REGULATION TOWARDS SECURED CYBERSPACE IN BANGLADESH CONTEXT

It has already been shared that ITU's GCA considers five interrelated and coordinated arms- legal, technical, and procedural measures, organization measures, capacity building measures, and cooperation measures important for an ideal cybersecurity framework. This segment will provide an overview of these initiatives taken in the Bangladesh context and share some policy directions after evaluating these.

A. Cybersecurity in Bangladesh Context: An Overview

When Bangladesh was born as an independent country, Sweden had already enacted the first national cybersecurity-related law in the year 1973 in the form of a data protection law. In the first two decades after independence, Bangladesh had to face various political turmoil and natural disasters while concentrating on her economic development. These factors, alongside the poor foresight of the then governments in power, had an impact on Bangladesh's late joining in the ICT revolution compared to some of her neighbours.[43]

The Information and Communication Technology Act, 2006 (Act no. 39 of 2006) ("ICT Act, 2006"), the first standalone piece of legislation, was enacted containing important provisions on various aspects of ICTs securities e.g. legal recognition of digital signature and electronic records,[44] attribution, acknowledgment, and dispatch of electronic records,[45] secure electronic records & digital signatures.[46] The Law also listed a good number of substantive criminal offences with punishments e.g. damage to computer system, computer system (sec. 54), temperament of computer source code (s. 55), computer system hacking (s. 56), unauthorized access to protected system (s. 61), disclosure of confidentiality (s. 63), use of computer for crime commission (s. 66), etc. Besides, the Bangladesh Computer Emergency Response Team (bdCERT) was established in 2007 to assist the stakeholders in dealing with computer threats, vulnerabilities, incidents and incident responses, etc.

There are several limitations and challenges due to which the provisions of the law are not implemented effectively. As a result, the news about various cybercrimes are reported almost regularly. The incidents of malware attacks or website hacking are quite common. In the Holey Artisan Bakery incident, the terrorists successfully completed the bloodshed while using electronic devices, and this raised concerns over

---

Chaillot Paper 155 <https://www.iss.europa.eu/sites/default/files/EUISSFiles/cp155.pdf> accessed 27 November 2021; Erica Moret and Patryk Pawlak, 'The EU Cyber Diplomacy Toolbox: towards a cyber sanctions regime?' <https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2024%20Cyber%20sanctions.pdf> accessed 27 November 2021.

43 For a history of ICTs and the Internet in Bangladesh, see, generally, Karim ME (n 15).

44 Information and Communication Technology Act, 2006 (Act no. 39 of 2006) ch II, secs 5-12.

45 *Ibid*, ch III, secs 13-15.

46 *Ibid*, ch IV, secs 16-17.

the awareness and preparedness capabilities of the local security professionals. Besides, the security of Bangladesh National Defence College's website was breached through state-sponsored cyberattacks several times.[47] Moreover, there were frequent allegations that the provisions of the law, especially section 57 dealing with defamation in electronic form, were used for political purposes and to limit the voice of the opposition or critics of the government. Due to some technical and technological limitations of the law enforcement agencies, lack of dedicated forensic labs, etc. offences under this law committed could not be investigated, tried, and prosecuted. As a result, not a single case under this law was unfortunately brought to the higher court, and reported in the law reports in the last fifteen years. The ICT Act, 2006 was subsequently amended extensively through the provisions of the Digital Security Act, 2018 (Act 46 of 2018) ("the DSA, 2018"), leaving the ICT Act, 2006 merely a digital signature law as available in other jurisdictions. Furthermore, dedicated wings with necessary cyber forensic expertise were established in the police administration and cyber tribunals are established in all divisional districts.

Bangladesh has adopted the National Cybersecurity Strategy, 2014 following the Pillars of the ITU's GCA though unfortunately, no specific body was assigned with the responsibility for the 'design, implementation, monitoring, and revision of the strategy'. Some sectors such as communications, emergency services, energy, finance, food, government, health, transport, and water were indicated as Critical Information Infrastructure (CII) though no such specific CIIs have been formally declared yet. It was reiterated through the DSA, 2018 and the Digital Security Rules, 2020 ("the DSR, 2020") that the government may declare any computer system, network, or information infrastructure as CII.[48] In 2014, the government also issued the Information Security Policy Guidelines which provided all the government agencies to develop and implement their respective information security policy within six months of the commencement of the Guidelines.[49]

In 2016, the ICT Division, under the Ministry of Posts, Telecommunications and Information Technology, established the Bangladesh e-Government Computer

---

47 Mohammad Nurus Salam, 'Evolving Cyber Security Threat and Preparedness of Bangladesh Army' (2018) 64 Bangladesh Army Journal 83-95.

48 See generally, Digital Security Act, 2018 (Act No. 46 of 2018), sec 15. Examples of critical infrastructures include transport/traffic (aviation, navy, railway, road traffic), government (administration, parliament, judiciary), IT & T (telecommunication and information technology), media and culture (electronic and print media and national monuments), utilities such as water (water supply and sewerage), energy (electricity, gas, oil), health (medical care, drugs, laboratories), finance and insurance (banks, stock exchange, insurance and other financial services). These are treated as critical as the control, process, circulation, or preservation of any information after damaging or compromising may adversely affect: (i) public safety or financial security or public health, and (ii) national security or national integrity or sovereignty. The example of BB cyber heist can be shared here when in February 2016, by exploiting in a SWIFT global payment network, the hackers stole USD 81 million of the national reserve.

49 The Guidelines define 'information security policy' as "a documented list of management instructions that describe in detail the proper use and management of computer and network resources with the objective to protect these resources as well as the information stored or processed by Information Systems from any unauthorized disclosure, modifications or destruction."

Incident Response Team (BGD e-GOV CIRT) under Bangladesh Computer Council to support the government efforts to develop and amplify ICT programs by establishing and maintaining cybersecurity incident management capabilities within the environment of the government.[50] One of the important contributions of BGD e-GOV CIRT is the introduction of an Information Security Manual, mainly to ensure the security of unclassified government information and systems, entitled Government of Bangladesh Information Security Manual (GoBISM), based on International Standards such as ISO/IEC 27001:2013, ISO/IEC 27002:2013 following New Zealand Information Security Manual.[51] With its mandates to support the government mainly, the BGD e-GOV CIRT has been taking various initiatives. There are some limitations and scopes for further improvements in the rapidly changing circumstances. For example, the GoBISM, which suggests two sets of controls- mandatory and recommended, is only a manual having no legally binding force and the government departments are not bound to follow this for the time being.

With all these fragmented initiatives, it is evident that there was no standalone cybersecurity law in Bangladesh, and the overall domestic cybersecurity ecosystem was not found to be satisfactory as it was reflected in the Indexes shared already.[52] Subsequently, the government enacted the DSA, 2018 apparently in a rush just before the General Election of 2018 to ensure national digital security, and the identification, prevention, suppression, trial, and other related matters regarding digital crime. Some of the most important immediate contributions of the Law was the provision for the

---

[50] The BGD e-GOV CIRT is now serving as National CIRT of Bangladesh (N-CERT) under the administrative control of the DSA. See, Digital Security Rules, 2020, rule 8.

[51] Some of the provisions included in the GoBISM are on information security governance, system certification and accreditation, information security documentation, information security monitoring, information security incidents, physical security, personnel security, infrastructure (cable management), communication systems and devices (fax machines, multifunction devices and network printers), product security, decommissioning and disposal (media usage, media sanitization, media destruction), software security, email security, access control, cryptography, network security (Network Management, Wireless LANs, Video and Telephony Conferencing and IP Telephony, Intrusion Detection and Prevention, Gateways, Firewalls, etc.), working off-site, and enterprise system security.

In the case of *M. Habibur Rahman & Ors vs. Govt. of Bangladesh & Ors.* 7 BLT (HCD) 327, it was held that- the word 'government' denotes the person or body of persons administering the laws and governing the state. 'government' is the body of persons changed with the duty of governing and exercising certain powers and performing of certain duties by public authorities or officers together with certain corporations exercising public function.

[52] In the high profile report titled 'Cybersecurity Capacity Review: Bangladesh', released by BGD e-GOV CIRT, Global Cybersecurity Capacity Center (GCCC), and Oxford Martin School, Oxford University resulting from the invitation of the BCC to understand the cybersecurity capacity of Bangladesh to strategically prioritize investment in the sector have identified serious gaps and limitations in the existing system. The five sectors evaluated were- (a) cybersecurity policy and strategy, (b) cyberculture and society, (c) cybersecurity education, training and skills, (d) legal and regulatory framework, and (e) standards, organizations and technologies. The GCCC evaluates the cybersecurity capacity of any country into five stages- (i) startup, (ii) formative (iii) established, (iv) strategic, and (v) dynamic. It was found that almost all the sectors are in the 'startup' stage. See, Cybersecurity Capacity Review Bangladesh 2018 <https://www.cirt.gov.bd/wp-content/uploads/2020/01/CMM_Bangladesh_Report_FINAL.pdf> accessed 27 November 2021.

creation of a Digital Security Agency (DSA) and National Digital Security Council (NDSC),[53] emergency response team (s. 9), digital forensic lab (s. 10), etc. The law provides for the punishment of some relevant offences e.g. illegal access to- CII (s. 17), computer, digital device, computer system (s. 18), damage to computer and computer system (s. 19), change of computer source code (s. 20), electronic forgery (s. 22), electronic fraud (s. 23), identity theft (s. 24), sending of phishing or spam message (s. 25), collection and processing of personal information without any legal authority (s. 26), cyberterrorism (s. 27), illegal electronic money transaction (s. 28), hacking (s. 34), aiding in commission of offence (s. 35), etc. The Law also provides for mutual legal assistance as per the provisions of the Mutual Legal Assistance Act, 2012 (Act no. 4 of 2012) in case of necessity.

Besides, many relevant issues on cybersecurity are included in the National ICT Policy, 2018 where some plans of action are set, and responsibilities are assigned to different bodies.[54] The government has also issued or drafted some relevant policy documents.[55] While these are all very encouraging moves and promise towards more secured cyberspace, from the experiences of the developed economies it can be anticipated that the implementation of these will be challenging. Moreover, the Policies have no binging effects in the eye of law in Bangladesh.[56] Yet, these initiatives should be applauded for at least the authorities have realized the importance of this and considered adopting relevant necessary measures in a systematic and coordinated approach. Nevertheless, there is still room for improvement.

B. Cybersecurity in Bangladesh Context: An Evaluation and Policy Directions

Cybersecurity issues are a common concern for all countries and require collective, coordinated, and holistic attention and efforts from the relevant stakeholders within a clear policy framework to reduce the menace. It has already been discussed that there is no perfect model for cybersecurity due to the magnitudes of the web cyberspace and complexities. Apparently, the initiatives taken by the government, following the ITU's GCA five pillars should be appreciated keeping in mind that other countries that have started all these processes almost three decades ago are still struggling to make their cyberspace better secured to harness the potentials of ICTs. Therefore, they have been taking innovative initiatives after reviewing the existing ones regularly as routine work.

The present national cybersecurity framework seems to be optimistically progressing, especially after the enactment of the DSA, 2018 and the DSR, 2020. While the present

---

[53] The Digital Security Act, 2018 (n 41) ch II, secs 5-7, and ch IV, secs 12-14. The government established the DSA on January 16, 2019 under the ICT Division and the NDSC, headed by the Prime Minister.

[54] It will be relevant to share here that the previous National ICT Policies of 2009 and 2015 also contained some isolated provisions in this regard.

[55] For example, National Strategy for Internet of Things, Blockchain, Artificial Intelligence. The Examination and Certification of Standards of Software and Hardware, 2020 (Draft), etc.

[56] *National Board of Revenue v. Abu Saeed Khan and others*, 2012, 41 CLC (AD) [8674] = 18 BLC (AD) (2013) 116.

framework promises to protect digital crimes originated and committed from inside the country, it will be challenging to implement the available legal provisions if the threats originate from outside the country. When using malware and phishing emails, personal information is stolen to get illegal access to a computer system, Bangladesh does not effectively implement the phishing or spam related legal provisions available in the ICT Act, 2006 or the DSA, 2018. Though an Information Privacy and Protection Rule has recently been drafted, it is not finalised yet. The DSA, 2018 has a provision on the extraterritorial application; however, it is evident from various incidents of threats and attacks that unless there are proper co-operation mechanisms available between countries, this is difficult to implement such provisions in real-world criminal cases, let alone the cybersecurity incidents.

The absence of a competent national body is an important concern. Enacting the DSA, 2018 or recent formation of the DSA is not enough for a government that included 'digital dreams' in their election manifesto almost a decade ago. These are only the beginning and a lot more should be done. Bangladesh still does not have any dedicated cybersecurity policy unit responsible to develop, monitor, or implement cybersecurity policies continuously considering the developments and international best practices.[57] Until 2019, there was no dedicated national body to deal with overall cybersecurity issues, though the government established the DSA recently. While it is yet not the right time to evaluate the activities of the DSA, one serious concern is that the Defence forces are not directly included in the DSA like other countries e.g. Australia, though the Director-General of the Defence Intelligence is made as an *ex officio* member of the NDSC. It indicates that the government has been trying to address this as a technical issue only ignoring the national security aspect of it. It may be argued that since the Prime Minister heads the Ministry of Defence and is the Chair of the DSA, the defence personnel will automatically be included; however, it may not happen and therefore, we need to wait till then. Moreover, Bangladesh lacks a National Security Council; instead, the government has recently formed a National Committee on Security Affairs. The government has recently updated the previous 2-pages defence policy of 1974 in 2018. Though the National Defence Policy, 2018 could not be accessed, perhaps for some security reasons, it can be seen from the newspaper reports that the Policy provides the citizens to be ready always to play their role as they did during the time of liberation war in 1971.[58] To expect similar cooperation from the general people on cybersecurity-related threats and attacks, there is no alternative to make them aware of cybersecurity basics.

The government should realise practically that making cyberspace safe for the citizens is fundamental to avoid catastrophic incidents in the future. In making cyberspace more secure, the need for awareness of citizens is paramount. Therefore, cybersecurity culture should be promoted in the country. This does not require a huge investment, it rather requires conveying a message effectively, which is that cybersecurity starts with

---

57 See, National Cybersecurity Index (n 16).

58 Shakhawat Liton and Partha Pratim Bhattacharjee, 'Draft National Defence Policy: PM to head nat'l security body' *the Daily Star* (Dhaka, 21 March 2018) <https://www.thedailystar.net/frontpage/draft-national-defence-policy-pm-head-natl-security-body-1551244> accessed 27 November 2021.

awareness and personal carefulness. Citizens need to be made aware that the cybersecurity issues are for their benefit. Many universities have been offering computer science and engineering courses in Bangladesh. The students and students of other courses of these universities can be engaged as volunteers as part of their community service/contribution to make people aware of different cybersecurity issues. There is already enough literature proposed by internationally recognised bodies available in the common domain on how to develop the cybersecurity culture within an organization. It is encouraging to share that some regulators have issued instructions to initiate some awareness programs. For example, Bangladesh Bank instructs all banks to run information security awareness programmes. Besides, the DSA and other government bodies have been organising some isolated cyber hygiene programmes and taking initiatives on or before some international dates or events, but these are not enough again. There are also incidents that some over-enthusiast Bangladeshi hacktivists target the websites of different countries in the aftermath of some sensitive incidents. The government should also disseminate the information that for such activities the country may face economic sanctions.

It has been reported frequently that the provisions of the laws i.e. the ICT Act, 2006 and the DSA, 2018 are regularly abused for political purposes and to control the voice of the political opponents and criticisms of the government or ruling political party. That's why even if the enacted laws contain some favourable provisions which are common in other jurisdictions, the general mass has an apprehension about the effectiveness of the law. Though the police administration has issued some guidelines on the use and application of the provisions of these laws, it is still perceived to be misused.

The cybercrime trial and prosecution success rate in Bangladesh is very few if not nil. It is believed that the officers involved in different stages are not adequately prepared and trained. This situation can be improved. Already there are international best practices available in the public domain. The book titled "Combating Cybercrime: Tools and Capacity Building for Emerging Economies" released by the ITU is an important contribution designed targeting the capacity building of the stakeholders involved in the cyberspace landscape e.g. law and policymakers, judges, law officers, investigators, and civil society members towards making a safe, secure and equitable Internet. Besides, different countries have already come up with Cybercrime Prosecution Guidance.[59] The policymakers can consider to adopt these in the Bangladesh context keeping in mind the economic and socio-cultural issues.[60]

It is apparent from the DSR, 2020 that the government has realised that 'security by design' should be the primary aim behind all government digital moves. While we need to wait to evaluate the effectiveness of the government's such move, the N-CERT

[59] See generally, 'Cybercrime - prosecution guidance' (26 September 2019) <https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance> accessed 1 March 2021.

[60] In updating the cybersecurity policies in future, Bangladesh should consider international best practices available at the website of United Nations Institute for Disarmament Research Cyber Policy Portal. See generally, 'UNIDIR Cyber Policy Portal' <https://unidir.org/cpp/en/> accessed 27 November 2021.

should actively consider taking part in the cyber drills run by ITU to evaluate its preparedness in cyberattacks scenarios. This is because except for the Bangladesh Army, Bangladesh reportedly imports most software from abroad. Though this is not sure how the procurement process of such software is conducted, this is obvious that not the software code rather only .exe file is normally shared which causes some additional problems in the maintenance of e.g. the router, firewall, software maintenance, password, backdoor hook, or maintenance hook, etc. This is even unfortunate as Bangladeshi technopreneurs are well capable to develop the required software to meet the national needs. Good thing is that Bangladesh Bank authorities have decided to use local software developed by the local developers in the banking sector, which is a very welcoming move.[61] Therefore, the involvement of the legal professionals having expertise in cybersecurity and international law should be considered in the future procurement process. Moreover, like the move of banking regulators, initiatives can be taken to organize hackathons and introduction of 'regulatory sandbox' on different aspects of cybersecurity through which the winners can be engaged to develop customised tailormade but more secured applications and systems.

Unfortunately, there is no dedicated civil society think tank to deal with cybersecurity issues exclusively. Though the most renowned think tank i.e. Bangladesh Institute of International and Strategic Studies does not also have any noticeable program on cybersecurity, the Bangladesh Institute of Peace & Security Studies has been playing some role in this regard and has been researching on this issue besides their other activities.

In the socio-economic context of the country where the education, awareness, and understanding of the people are still not satisfactory, and the government and other stakeholders are unable to invest a significant amount in the protection of national cyberspace, the government should consider promoting the notion of cyber diplomacy. Within the UN system, the co-operation between the member states is very fundamental,[62] and the act of diplomatic relations plays an instrumental role to this end. Diplomacy, a means to implement the foreign policy of any country, "uses certain set of skills, tools, procedures, methods, norms and rules . . . to orchestrate and moderate the dialogues between states . . . to optimize the content and quality of international relation . . ."[63] The issue of 'electronic diplomacy' is not a new concept as different countries have been following this for years.[64] However, cyber diplomacy, relatively a new idea emerging in Europe about cyber defence and cybersecurity, aims to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in

---

61 Special Correspondent, 'State-owned banks asked to bank on local software' *the Business Post* (Dhaka, 17 August 2020) <https://businesspostbd.com/post/5293> accessed 27 November 2021.

62 For example, the Preamble, Article 1(3), the Charter of the United Nations, 1945.

63 Bolewski W, *Diplomacy and international law in globalized relations* (Springer Science & Business Media 2007).

64 The concept 'electronic diplomacy' or 'digital diplomacy' is used in a different context. Adesina OS, 'Foreign policy in an era of digital diplomacy' (2017) 3 Cogent Social Sciences 1297175. If the definition of the term 'electronic' includes the communication of diplomatic affairs through electronic means, then Bangladesh has also been practicing this since her birth.

cyberspace, and effective global digital governance through the joint efforts of like-minded countries and relevant stakeholders. This initiative is getting traction as cyber threats are seen as an attack on the sovereignty of the state. The European Union has already developed the Cyber Diplomacy Toolbox and some regional treaty arrangements towards making safer and more principled cyberspace.

There is no binding international instrument on cybersecurity and Bangladesh is not part of any important global alliances that work to make the cyberspace secured though the country is an active member in the various international forum, including its membership in the UN Security Council between 1979-1980 and 2000-2001, and has bilateral and multilateral agreements/treaties with several countries. Hence, Bangladesh, based on the Constitutional mandate and the initial Foreign Policy i.e. 'friendship with all and malice towards none', prefers the settlement of any kind of extra-territorial dispute, including the disputes in cyberspace, peacefully. [65] Yet, Bangladesh should consider including the issue of cybersecurity in their diplomatic agenda.

This is a good sign that the government has realised the importance of cyberwar and cybersecurity and has started to raise these at the international forum. In 2017, in her speech at the 72nd UNGA, Prime Minister Sheikh Hasina expressed her concerns on cyber threats to prevent money laundering, terrorist financing, and other transnational organized crimes.[66] In 2018, at the High-Level Side-Event on Cyber Security and International Cooperation, the Prime Minister has eloquently articulated the risks and challenges in cyberspace.[67] Thus, it is high time that the government reconsiders establishing both a cyber army wing and cyber diplomacy. This is also needed as the changing world demands the proper representation of the country at the international forum effectively and efficiently. In various databases maintained by international communities, e.g. UNODC Database on cybercrime, the position of Bangladesh is not properly updated.[68] The very poor level of entry in the database may prevent another country to co-operate with Bangladesh. If not, it will surely kill a very important time in case of an emergency. Besides, in most of the previous massive successful cyberattacks having security consequences targeted in various countries, where Bangladesh has diplomatic missions, it is not apparent if the diplomatic missions

---

65 Article 25 of the Bangladesh Constitution 1972, which forms the foundation in dealing with international affairs, provides to maintain the international relation of the country based on the "principles of respect for national sovereignty and equality, non-interference in the internal affairs of other countries, peaceful settlement of international disputes, and respect for international law and the principles enunciated in the United Nations, and on the basis of those principles shall – (a) strive for the renunciation of the use of force in international relations and for general and complete disarmament; . . ."

66 External Publicity Wing, Ministry of Foreign Affairs, Government of Bangladesh, 'Selected Speeches of Prime Minister Sheikh Hasina During Official Visits (2009-2018)' 153 < https://mofa.gov.bd/site/publications/4c50b8a7-f408-4070-8504-848987691768/Selected-speeches-of-Prime-Minister-Sheikh-Hasina-during-official-visits-2009-2018> accessed 1 March 2021.

67 *Ibid*, 202-203.

68 See, for reference, the Chapter on Bangladesh maintained by the UNODC's database on Sharing Electronic Resources and Laws on Crime (SHERLOC) <https://sherloc.unodc.org/cld/v3/sherloc/legdb/> accessed 1 March 2021.

realised the importance of these and update the government back home about the necessary needful. If that could be done, the experience could be utilised in recovering the heisted Bangladesh Bank fund.

Through cyber diplomacy, Bangladesh needs to take initiatives to include the issue of cybersecurity in the existing treaties and future ones. The country should delve into cyber diplomacy and should foster bilateral and multilateral efforts to settle the issue peacefully. This is because it has been reported that in the recovery of the Bangladesh Bank Cyber heist, due to non-co-operation of countries such as the Philippines, China, Malaysia, and Sri Lanka, the Criminal Investigation Department (CID) is incapacitated to submit the charge-sheet though the investigation was completed.[69] As a result, Bangladesh could only recover USD 15 million out of heisted USD 81 million. The Foreign Services Academy, responsible to train the Bangladeshi diplomats, can include the issues of cybersecurity and cyber diplomacy in their training module. Finally, Bangladesh should consider playing an active role by joining the UN OEWG and can further consider joining the Budapest Convention as a party.

Interestingly, the initial foreign policy has been changing over the years and the country has been emphasizing economic diplomacy. As Bangladesh is emphasizing economic diplomacy in recent years, the country should review the existing BITs and all future BITs to include the provisions of cybersecurity. Fortunately, Bangladesh has BITs with some cybersecurity giants and therefore, can exchange experiences if this issue is included in the meeting agenda.[70]

V. CONCLUSION

The relationship of crime with economic development and globalization is well recognised, so is the case of cybercrimes, which are committed to breaching the computer security system of a cyber persona. Cybercrime and cybersecurity are concerns of all and every country in the world, everyone has been facing this in some shape or form at a varied level making it to be common concern of mankind. The recent economic progress of Bangladesh has been recognized by various authoritative bodies. With Bangladesh's vision to transform an agrarian country into a manufacturing one and with the political slogan of the present government i.e. 'Digital Bangladesh' and to fully digitalise the country to improve the socio-economic conditions of the people, the number of cyber threats has increased too since the issues of digitalization come with inherent security challenges. Therefore, the government should also consider the

---

69 Nurul Amin & Shafayat Hossain (n 17).

70 From the database of the UNCTAD, it is apparent that Bangladesh has existing bilateral investment treaties with Denmark, India, Singapore, Thailand, Iran, Austria, Switzerland, Uzbekistan, Japan, Indonesia, Philippines, Poland, China, Netherlands, Malaysia, Turkey (1987), Romania, Korea, USA, France, Belgium-Luxemburg Economic Union, Germany, and the United Kingdom. There are also some countries with whom Bangladesh has already signed the investment treaties though these are yet to come into force. The list of such countries includes- Cambodia, Turkey (2012), United Arab Emirates, Vietnam, North Korea, and Pakistan. See, for reference, UNCTAD, 'Investment Policy Hub' <https://investmentpolicy.unctad.org/international-investment-agreements/countries/16/bangladesh> accessed 1 March 2021.

issue of safe and secured cyberspace seriously.

Technically speaking, there is no exclusively secured system, and none can guarantee the most effective cybersecurity infrastructure which will remove the possibilities of all the prospective future cyber threats though the taking of effective measures can promise to reduce the number of threats. With various super-powerful technologies in the market and some are in the pipeline such as 5G technology, AI and quantum computing, etc. when data will be processed within nanoseconds, and due to the immortal nature of computer data, this issue of cybersecurity should be considered very seriously. Like natural calamities, the policymakers and everyone should realize that cyberattacks will surely happen; but initiatives should be taken to reduce the chances, respond immediately and prevent the prospective intruders/criminals. There is, unfortunately, no 'one size fits all' solution to the various types of cybercrime and cyber threats. That's why different countries have been framing a tailor-made customised cybersecurity framework based on their own need. But one thing is obvious that along with the legal and technological solutions, and the formation of a dedicated body with the core mandate of cybersecurity responsibilities, the awareness of cyberspace user citizens following the adage 'prevention is better than cure' can reduce the number of cyber threats significantly.

Bangladesh has been facing various development challenges common to other developing economies such as natural calamities, lack of good governance, corruption, etc. These were reconfirmed during the novel COVID-19 time when the policymakers initially were confident about the readiness of the national healthcare system, which was reported to be scrambling or found ineffective with full of inconsistencies and mismanagements subsequently. While manmade disasters may be settled with the passage of time and proper management of allocated resources, unfortunately, the effects of the digital disaster as a consequence of the cybersecurity crisis cannot be healed easily as it takes time even to realize that the computer system has been compromised.

Bangladesh has been leading the UN Peacekeeping mission in different countries in the world to ensure the security of that area and the country has been progressing even after facing devastating natural calamities. These indicate that the people of the country are smart and can handle prospective cybersecurity threats smartly if they are properly guided. Successive governments have taken some initiatives to introduce ICTs and make cyberspace secured; however, these are not properly implemented. Even though some of the law enforcement agencies such as CID, DB have dedicated forensic labs with the necessary expertise, the vulnerability of cyberinfrastructures can be seen through the news of ATM booths hacking reported in national media. The members of the law enforcement agencies seem to be helpless when these cyber threats are committed from outside the country. With all the technology-related initiatives, a massive, realistic, and effective campaign to make the citizens aware of their conduct in cyberspace, training of the government officials, programs adopted to produce more efficient human resources, and continuous technological updates are the key to success. Thus, the country needs to give focus on developing a culture of cybersecurity domestically and cyber diplomacy beyond the jurisdiction of the country.