BIISS JOURNAL, VOL. 43, NO. 4, OCTOBER 2022: 339-358
DOI: https://www.doi.org/10.56888/BIISSj2022v43n4a2
ISSN 1010-9536 (Print)

Mohammad Sohrab Hossain

SECURITISATION OF CYBERSPACE IN BIMSTEC: NORMS SETTING AND CAPACITY BUILDING

Abstract

Rapid changes happening in cyberspace are influencing geoeconomic and geopolitical orders around the globe. The BIMSTEC countries are also looking forward to establishing a data-driven economy. E-commerce has already become a buzzword in the industrial dictionary and an increasing trend of e-commerce can be seen in the BIMSTEC countries. Cyberspace has become a significant means for wealth creation, employment generation, and leveraging technological capacity. The paper argues that the securitisation of cyberspace in the BIMSTEC region would bring a political commitment to act collectively to transform the cyberspace of the BIMSTEC region into a common good and face emerging cyber threats collectively. This paper is an endeavour to understand the expansion of cyberspace in the BIMSTEC countries, assess the security threats for cyberspace in the countries of the organisation, and develop a regional framework for BIMSTEC countries for the securitisation of cyberspace in the region.

Keywords: Cyberspace, BIMSTEC, Cybersecurity, Securitisation

1. Introduction

In the modern world, cybersecurity has emerged as a common challenge for almost all the countries of the world. The unscrupulous expansion of Information and Communication Technology (ICT) has facilitated people to be benefitted from communication and connections. Modern technologies, i.e., Internet of Things (IoTs), 5G internet, and artificial intelligence, changed the lives of people all over the world. But such technologies are facing threats due to cybercrimes all over the world. Therefore, the issue of cybersecurity is gaining global importance to protect a body of technologies, processes, networks, devices, and data from any attacks. Since cyberspace is borderless, therefore, it is difficult for countries to protect cyberspace separately. Without international cooperation, it is almost impossible for any country to prevent cyber-attack without help from other countries. Because cybercriminals can attack anywhere in the world where the victim country cannot take any help without the help of the attacker's country. Therefore, there is a global urge for international cooperation to ensure cybersecurity. Under the auspices of the United Nations Group of Governmental Experts in information (UNGGE), the United Nations (UN) is helping to develop cybersecurity mechanisms for many countries and regions. Moreover, a number of regional arrangements have already been developed to face the emerging challenges of cybersecurity.

Mohammad Sohrab Hossain, **PhD** is Professor, Department of Political Science, University of Dhaka. His e-mail address is: sohrab1974@du.ac.bd

The Bay of Bengal Initiative for Multi-sectoral and Technological Cooperation (BIMSTEC) countries are focusing on securitising cyberspace within this regional framework. In the last several decades, there has been a boom of cyber technology in the countries of BIMSTEC. Therefore, the political and security leadership of the BIMSTEC countries are focusing on the securitisation of cyberspace in the region. The securitisation process includes awareness building and adoption of new measures to tackle the threats of the cyber world. In 2017, during the security advisors meeting, member countries focused on the necessity of regional cooperation in cybersecurity issues and agreed to adopt necessary measures to tackle the threats.[1]

Although there are a good number of scholarly articles on cybersecurity in the region, they mostly see the security problem from the technical, industrial, or institutional point of view. On the other hand, most of these literature come from a specific state's perspective and do not address the BIMSTEC region as a whole. Therefore, the existing literature fails to address how taking up the region as a referent object may help policymakers and analysts see through the threats and opportunities from a broader horizon.

Although cybercrime is generally seen from the perspective of transnational crime, it requires specific attention. Since 2008, after the BIMSTEC Convention on Combating International Terrorism, Transnational Organised Crime, and Illicit Drug Trafficking; transnational crime has earned a significant status at the BIMSTEC table of discussion. However, the development regarding the cyber realm is relatively slow. The first-ever meeting of the BIMSTEC cybersecurity expert group took place in 2022, after 14 years. In the 2021 global cybersecurity index prepared by the globally renowned Estonian National Cybersecurity Index (NCSI) Project team, none of the BIMSTEC states ranks among the top 30 states.[2] On the other hand, several international organisations like the United Nations Office on Drugs and Crime (UNODC), The International Criminal Police Organisation (INTERPOL), and Kaspersky have flagged the rising trend of cyber crime in the South Asian and Southeast Asian states; the BIMSTEC member states are part of either of these two regions.[3] These issues underscored the necessity for securitising cyberspace, for the region, and the globe.

In this backdrop, this article is an initiative to understand the expansion of cyberspace in the BIMSTEC countries, assess the security threats for cyberspace of BIMSTEC countries and develop a regional framework to securitise the issue. It also aims at bridging the gap between industry-driven and security-driven literature on cybersecurity. Hence, the research questions of this article are as follows: Why does the BIMSTEC cyberspace need to be securitised? What are the

[1] "First Meeting of the BIMSTEC National Security Chiefs," Ministry of External Affairs, Government of India, accessed March 21, 2017, https://mea.gov.in/press releases.htm?dtl/28193/First_meeting_of_the_BIMSTEC_National_Security_Chiefs_March_21_2017.
[2] "National Cyber Security Index," Estonian e-Governance Academy Foundation, accessed September 21, 2022, https://ncsi.ega.ee/ncsi-index/?order=rank.
[3] "The Rise of Cybercrime in Asia Pacific and Considerations for Organisations Operating in the Region," UNODC, accessed September 20, 2022, https://www.unodc.org/documents/southeastasiaandpacific/darknet/index.html.

opportunities and challenges associated with cybersecurity-related developments?, and What measures can be taken to securitise the BIMSTEC cyberspace?

Including introduction and conclusion, the paper is divided into six sections. Section two focuses on the cyberspace of BIMSTEC countries to understand the expansion and complexities of the cyber issues. Section three concentrates on the concept and trends related to BIMSTEC cyberspace. Section four explores the new opportunities these countries can exploit due to the expansion of the cyber world and emerging threats. By examining the regional cybersecurity mechanism of the European Union (EU), The Association of Southeast Asian Nations (ASEAN) and African Union (AU), section five emphasises on two-pronged securitisation measures for BIMSTEC countries when dealing with cybersecurity issues. Section six concludes the paper.

2. Understanding Securitisation of Cyberspace

Security of cyberspace is one of the emerging concerns for almost all countries of the world. Traditionally, the concept of security was solely the border security of nation-states. The introduction of securitisation theory by Copenhagen School helped to understand security from a different perspective. The school is prominent for its securitisation concept where threats and insecurities are pronounced as "existential threats to a referent object by a securitising actor who generates endorsement of emergency measures."[4] The school articulates that security deals with survival threats, when a particular issue poses an existential threat to a defined referent object. The "speech act" by the security actors legitimise the use of force by the securitising actors. The issue of legitimacy comes from the consent of the audience.[5]

The important part of securitisation is the securitising process. Lene Hansen elaborates the difference between politicising and securitising.[6] The politicising refers to taking an issue with particular importance and implications to society and the topic needs open discussion and contestation in the political arena. It is a public decision-making process with negotiation, bargaining and deliberations. On the other hand, securitisation demands emergency handling of issues, because the whole existence of national security of the referent object depends on the prompt and successful resolution of the situation. According to Alber and Buzan, every issue can be located on the spectrum ranging from non-politicised—politicised—securitised and the position of a particular issue differs from state to state.[7] Therefore, the authors suggest a textual analysis would provide answers to concerns where the securitisation spectrum is the particular issue. As the authors

[4] Rit Floyd, "Human Security and the Copenhagen School's Securitization Approach," *Human Security Journal* 5, no. 37 (2007): 38-39.
[5] Michael C Williams, "Modernity, Identity and Security: A Comment on the 'Copenhagen controversy'," *Review of International Studies* 24, no. 3 (1998): 435-439; Paul D Williams, *Security Studies: An Introduction* (London: Routledge, 2012).
[6] Lene Hansen and Helen Nissenbaum, "Digital disaster, cyber security, and the Copenhagen School," *International Studies Quarterly* 53, no. 4 (2009): 1155-1175.
[7] Mathias Albert and Barry Buzan, "Securitization, Sectors and Functional Differentiation," *Security Dialogue* 42, no. 4-5 (2011): 413-425.

point out, "successful securitisation components: existential threat, emergency action and effects on inter-unit relations by breaking free to rules."[8]

However, the Westphalian state system dominated the security understanding till the end of the World War II. But, the decentralised and unregulated nature of cyberspace meant that it was a medium quasi-separated from the traditional scope of state security. The Copenhagen School "widened and deepened" the idea of security. Therefore, securitisation of cyberspace encompasses a wide range of issues. Firstly, the Copenhagen School identified an issue as a security problem when it has "cascading effects on other security issues."[9] In the last few decades, technological developments exponentially increased human dependence on critical networks. Just like environmental and economic affairs, cybersecurity has global implications and it also tore down national borders. Therefore, the security actors, like the state, technology experts, and business groups, need to focus on security networks. They feel a compulsion to securitise cyberspace.

Secondly, cyber threats can be categorised in three ways: cybercrime, cybersecurity and cyberwarfare. Cyberwarfare is more of a strategic issue rather than security one. Sometimes it is argued that cyberwarfare can only be launched by states. This is a parsimonious concept. Non-state actors (NSAs) also can wage a war against any country. If the state is the referent object for a cyber threat, the source of the threat is not an obvious element to make hard distinctions between cyberwarfare and non-warfare. Cybercrimes add a list of works which affect the web-based technologies. On the other hand, cybersecurity is defined as "having an implicit transnational nature-where the institutions and visitors are in separate nation-states which relies on web-based technologies to undertake the harmful act."[10] In all such cases, security actors need to take emergency measures to tackle unexpected threats in the cyberspace.

Thirdly, securitisation theory denotes that security discourse comprises of other referent objects beyond the state or nation. Since cyberspace is a phenomenon that needs special attention, it can be taken as a referent object. Insecurity in cyberspace produces special security challenges and gains the attention of the relevant audience, therefore, securitisation of cyberspace is not only limited to state or national security, but rather cyberspace itself is a referent object. The securitisation of cyberspace itself needs a comprehensive action plan with all societal and global actors involved. Therefore, securitisation theory is very much relevant to cyberspace.

Fourthly, cyberspace does not exist as an insulated plane. There are a number of stakeholders like states, individuals, private companies and many other organisations. Lene Hansen and Helen Nissenbaum viewed cybersecurity is arising from constellations of referent objects rather than separate referent objects, exemplified by the linkage between "networks" and "individuals" and human

[8] Albert and Buzan, "Securitization, Sectors and Functional Differentiation."
[9] Hansen and Nissenbaum, "Digital Disaster, Cyber Security."
[10] Nicholas Thomas, "Cyber Security in East Asia: Governing Anarchy," *Asian Security* 5, no. 1 (2009): 3-23.

collective referent object present in this discourse.[11] They identified their different modalities for cybersecurity: hyper-securitisation, everyday security practices and technification. The hyper-securitisation amplified the vastness of future security threats, future cascading effects of security and the urge for extreme countermeasures. The everyday securitisation of cyberspace implies an effect on the daily lives of ordinary people. In this case, the referent object is an individual. The referent object is a necessary element in the fight against insecurity as well as the liability to the system as a whole, whether through deliberative action or not.

The last securitisation discourse applies to cyberspace is about technification driving from a computer network, but proper understanding and implementation of measures for effective management of computer networks. In this respect, computer experts must cooperate closely with security experts and other administration representatives. Since cyberspace has cascading effects on other security issues, securitisation has emerged as an essential phenomenon in this discourse. Taking cyberspace as a referent object, the securitisation of cyberspace includes monitoring networks, preventing unusual actions, and maintaining effective networks. There are wide range of actors in securitisation and the audience of the securitisation process are also multiple. Moreover, in the process of securitisation, in many cases, nation-states can individually act as a securitising actor, but in the process of securitisation of cyberspace, nation-states need to come together to act as "security actor" at the regional level as well as in the international arena.

3. Cyberspace in BIMSTEC: Concept and Growth

The word cyberspace was first used by William Gibson in 1982, in a short story titled "Burning Chrome: Referring to the Vital Reality." Gibson's cyberspace was a spaceless world, characterised by the ability for virtual presence of an interaction between people through "icons, waypoints and artificial reality."[12] However, Gibson's "fictional matrix" are not relevant in the contemporary understanding of cyberspace. In the contemporary world, cyberspace is defined as "the fusion of all communication networks, databases and sources of information into avert, tangled and diverse blanket of electronic interchange, which is virtual and immaterial, a bioelectronics environment that is universal." Provvidera et al. identify cyberspace as "fifth domain of warfare, after land, air, sea and space."[13]

However, there is no well-accepted definition of cyberspace. Some of the common features of cyberspace discussed in the contemporary literature can be mentioned: first, cyberspace is a distance-less space, where connection and networking can be done easily by avoiding the distance between and among the people. Second, it is a spaceless world where space-time relations are meaningless. It is claimed that ICT and cyberspace are creating a spaceless world. Third, it is

[11] Hansen and Nissenbaum, "Digital Disaster, Cyber Security."
[12] Rain Ottis and Peeter Lorents, "Cyberspace: Definition and implications," (Paper presented at International Conference on Cyberwarfare and Security, 2010).
[13] Marco R Provvidera, Volha Samasiuk, Richard Peltz-Steele, Mayra Cavazos Calvillo, Adrian Lucio Furman, Renato Opice Blum, Matthew Murphy, and Kyoung Yeon Kim, "Privacy, E-Commerce, and Data Security," *Int'l Law* 50 (2016): 103.

changing the industrial world from "mode of production" to "mode of information." Traditionally, human society was dominated by the "mode of production," but modern world is going to be dominated by "mode of information." Fourth, modern society is divided in two spaces: "public space" and "private space." The expansion of technological development blurred the gap between the two. Rather, a new space known as "privatisation of public space" has emerged. Cyberspace is a place where public issues are easily discussed in private forums. Fifth, traditionally, human interaction was individual communication-oriented, but cyberspace facilitated group-communicaition by a larger extent. Sixth, cyberspace is rapidly blurring reality and developing a virtual world of communication.

However, the cyberspace of the BIMSTEC member states has increased over the years. Table 01 shows the current span of cyberspace in the BIMSTEC area in terms of mobile subscription vs population, internet users vs penetration, active social media users vs penetration and mobile social media users vs penetration.

Table 01: Cyberspace in BIMSTEC[14]

Country	Total Population	Mobile Subscription vs Population	Internet Users vs Penetration	Active Social Media Users vs Penetration	Mobile Social Media Users vs Penetration
Bangladesh	167.2 million	157.2 million 94%	91.82 million 55%	34 million 20%	32 million 19%
Bhutan	821.6 thousand	881.7 thousand 107%	420.0 thousand 51%	420 thousand 51%	410 thousand 50%
India	1.361 billion	1.19 billion 87%	560.0 million 41%	310 million 23%	290 million 21%
Myanmar	54.1 million	56.57 million 105%	21.00 million 39%	21 million 39%	21.1 million 39%
Nepal	29.78 million	39.99 million 134%	16.19 million 54%	9.9 million 33%	9.3 million 31%
Sri Lanka	20.98 million	28.71 million 137%	7.13 million 34%	6.2 million 30%	5.7 million 27%
Thailand	69.24 million	92.33 million 133%	57.60 million 82%	51 million 74%	49 million 71%

From the table, it can be seen that all of the BIMSTEC member states have more than 80 per cent of their population subscribed to mobile phones. The highest mobile subscription vs population ratio can be found in Sri Lanka, where the number of mobile-network subscribers (28.71 million) exceeds the number of

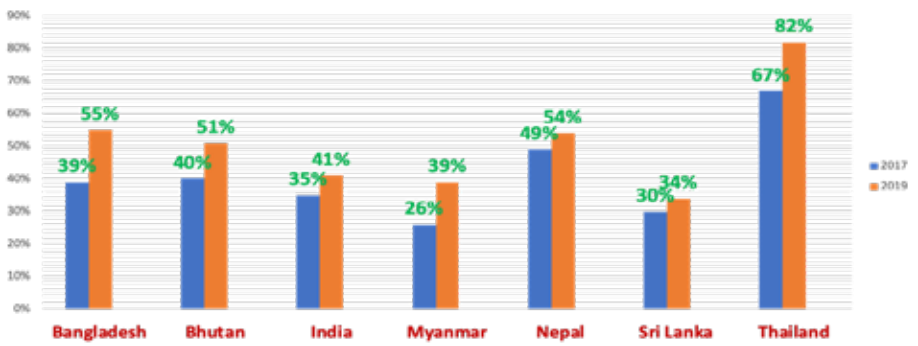
[14] "Statistics and Indicators," International Telecommunication Union, 2020, https://www.itu.int/itu-d/reports/statistics/.

population (20.98 million), making the ratio 137 per cent. Similar cases can be seen in Bhutan (107%), Myanmar (105%), Nepal (134%), and Thailand (133%). The lowest mobile subscription vs population ratio can be found in India, where 87 per cent of its 1.361 billion citizens are subscribed to mobile networks.

Nevertheless, based on internet usage, the penetration rate is comparatively low among the BIMSTEC countries. The ratio also varies from one state to another. Sri Lanka has the lowest (34%) internet users vs penetration ratio since only 7.13 million of its 20.98 million population have access to the internet. Among the other member states, the ratio wavers between 30 per cent and 50 per cent, except for Thailand, where 57.6 million of the 69.24 million citizens have internet access making the ratio 82 per cent.

In the cases of active social media users and mobile social media users, only Thailand and Bhutan hold rates equal to or higher than 50 per cent. Thailand, hence, has both the highest active social media users vs penetration ratio and the mobile social media users vs penetration ratio among the BIMSTEC countries, having 51 million active social media users (74% of the population) and 49.00 million (71% of the population). The rest of the countries belong to 20 per cent to 40 per cent ratio in terms of both of the categories. Among the countries, Bangladesh has the lowest ratio as only 20 per cent of its entire population actively use internet and only 19 per cent are social media users.

Figure 01: The Growing Number of Internet Users among the BIMSTEC Countries[15]



The figure shows that all of the BIMSTEC member states had a significant increase in the percentage of internet users vis-á-vis the population. Thailand had the highest percentage (67%) in 2017, which increased to even more (82%) in 2019, signifying a 15 per cent increase in two years. Notably, Bangladesh had the highest level of increase (16%) in two years as the percentage of internet users grew from 39 per cent to 55 per cent. More than 50 per cent of the citizens in Bangladesh, Bhutan, Nepal and Thailand have access to the internet. In the rest of

[15] "Global Internet Users," International Telecommunication Union, Statistics and Indicators, 2020, https://www.itu.int/itu-d/reports/statistics/2020/11/15/internet-use/.

the countries, the ratio stays between 30-40 per cent. However, in all countries, the percentages have risen between 2017 and 2019. Apart from Bangladesh's 16 per cent and Thailand's 15 per cent increase in the number of internet users; Bhutan saw an 11 per cent rise, India saw a 6 per cent rise and Myanmar, Nepal and Sri Lanka respectively had 13, 5 and 4 per cent increase in the number of internet users among the citizens. This kind of statistical and empirical evidence demonstrates that the overall breadth of cyberspace of the BIMSTEC countries has extended over the years.

4. Opportunities and Threats

Given the enormous coverage and popularity of information technology, the extended cyberspace has created opportunities for all of the BIMSTEC countries. Meanwhile, several threats have also penetrated the countries. The opportunities and threats together lay out the need for securitisation of the cyberspace and how they can facilitate both industrial and security-driven policies. One thing has to be kept in mind that the cyber industry is a very big industry and before the entire concept of the cyber threat became relevant for the state, the cyber industry had dominated the global platform as a technical avalanche. This is how these two sectors and the state machinery can merge and collaborate for the securitisation measures.

4.1 *The Opportunities: Development-Security Dynamics*

Following the worldwide trends, the BIMSTEC countries are also looking forward to establishing a data-driven economy. It is estimated that by 2023, the cybersecurity industry will be worth US$639 billion. On the other hand, the increased cyberspace can be used as a means for wealth creation, growth of employment opportunities and leveraging technological talent.

E-commerce has already become a buzzword in the industrial vocabulary and an increasing trend of e-commerce can be seen in the BIMSTEC countries along with similar ventures like m-commerce (mobile commerce) and f-commerce (Facebook commerce). Financial Technology or FinTech platforms have facilitated Digital Finance Services (DFS) and Mobile Financial Services (MFS), where monetary transactions, purchases, and sales are completely coordinated in the digital space. Thailand has the sturdiest e-commerce industry with 62 per cent penetration.[16] On the other hand, with a Compound Annual Growth Rate (CARG) of 53 per cent in between 2013 and 2017, India has established itself as the fastest-growing e-commerce market in the world.[17] With a current estimated worth of US$1.6 billion, the e-commerce market of Bangladesh is expected to be US$04 billion by 2023.[18] The online fashion industry has become a huge contributor in this regard with an estimated worth of US$598 million, followed by US$457

[16] Ashish Chhibbar, "BIMSTEC: An Unprecedented Opportunity for Collaboration and Cooperation in Cyberspace," accessed February 17, 2020, https://idsa.in/idsacomments/bimstec-collaboration-and-cooperation-in-cyberspace-achhibbar-181218.
[17] "India is Fastest Growing E-Commerce Market: Report," *The Times of India*, November 29, 2018.
[18] Muhammad Zahidul Islam, "E-commerce Sales to Reach $3b in 4 Years," *The Daily Star*, December 17, 2019.

million worth of electronic products and US$196 million worth of furniture and appliances.[19]

In the cases of Nepal, Bhutan, Sri Lanka and Myanmar, e-commerce is still in an incipient stage; however, notable efforts have been made for its growth from each of the governments. Nepal joined the e-commerce ecosystem through the arrangements of two big online platforms—Daraz Nepal and eSewapasal along with other small ventures.[20] The country's central bank, Nepal Rastra Bank also gave license to 28 banks regarding online banking and allowed pay-pal for international payment in 2018 which led to 5 million mobile banking clients within the country.[21] Sri Lanka made legal advancements by introducing the Electronic Transactions Act, No.19, which significantly removed legal barriers for the penetration of e-commerce in the mainstream industry.[22] With a US$6 billion worth of market value, Myanmar looks forward to having a decisive shift by getting involved with Alibaba, the parent organisation of popular e-commerce platforms operating within South Asia.[23] In short, e-commerce has become the commercial trend among the BIMSTEC countries and this opportunity is further utilised and promoted by the respective states and relished by the consumers.

Another opportunity that the booming cyberspace has brought is the possibility of technology being used as a means of wealth creation. The ICT sector has globally become an area of potential wealth creation for all countries. Both individuals and industries are facilitated through the utilisation and transaction of information technology which, in turn, can contribute to the growth of the country. According to the World Economic Forum, around 120 companies in Bangladesh are now engaged in the export of information worth US$1 billion, which will supposedly increase to US$5 billion by 2021.[24] As a United Nations Conference on Trade and Development (UNCTAD) report demonstrates, this extended scope of engagement for ICT-based organisations is ensuring an annual 40 per cent growth of the ICT sector.[25] The IT-BPM sector of India had US$177 billion in 2019 and the estimated annual growth was 6.1 per cent.[26] With the highest-ever revenue generated by the Indian IT firms worth US$181 billion in the 2018-19 FY, the revenue from the Global In-House Centre (GIC) is expected to reach around US$50 billion by 2025.[27]

Even beyond the direct accumulation of IT sector wealth, each BIMSTEC country has embarked on massive technological development or using technology as a primal tool for facilitating other areas. As the first Southeast Asian country, Thailand adopted biotechnology in the mainstream agricultural practice, which

[19] Islam, "E-commerce Sales."
[20] Sikuma Rai, "Nepal's Budding E-commerce Ecosystem," *Nepali Times,* September 20, 2018.
[21] Rai, "Nepal E-commerce."
[22] "Major Boost for Electronic Transactions with New Amendment," *Daily Mirror,* October 25, 2017.
[23] Soe Lin Myat, "Solid Prospects for E-commerce," *Myanmar Times*, September 12, 2019.
[24] "Export Earning from IT Sector: Bangladesh on right track to earn $5b," *The Daily Star,* December 09, 2019.
[25] "Bangladesh's ICT Industry Grows 40% Annually, Says UNCTAD," *bdnews24.com*, July 26, 2019, https://bdnews24.com/business/bangladeshs-ict-industry-grows-40-annually-says-unctad
[26] "IT & ITeS Industry in India," India Brand Equity Foundation, December 2019, https://www.ibef.org/industry/information-technology-india.aspx.
[27] Foundation, "IT & ITeS".

elevated the scope of wealth generation, diversification in agriculture and employment. The impact and popularity of robust technological appliances can be found in the number of applications received by the Thailand Board of Investment (BOI) in 2017 which is valued over US$1.9 billion.[28] On the other hand, BOI has also noted how computer components constituted 56 per cent of the US$32 billion worth of export revenues generated from the electronics industry in 2014.[29] This includes various hardware manufacturers, including Western Digital and Seagate, two pivotal names in the industry popular for hard storage drives.[30] The "Thailand 4.0" Vision initiated in 2016, along with the "Startup Thailand" project by the Thai Ministry of Science and Technology (MOST), also reflected the country's reverence for technological adaptation in subsequent industries like tourism. The impact led to a record 38.27 million tourists in 2018 and secured an estimated 41 million in 2019, spending THB 2.21 trillion or US$67.6 billion.[31]

India has also been utilising technology in multiple areas, and many industries have boomed by making proper use of it. One of the exciting areas is India's food-tech industry which is expected to turn into an equivalent of US$8 billion by 2020, marking 25-30 per cent annual growth.[32] India has also planned to subscribe to blockchain technology which is a significant revolution in the agriculture industry. It uses Distributed Ledger Technology (DLT) to reduce middlemen's role and ensures further transparency and immutability by establishing a digital identity.[33] As Observer Research Foundation (ORF) states, a blockchain-focused software company named BanQu has successfully experimented with the technology in eight countries until September 2018 and India is following the same route.[34]

All of these positive changes have opened up a huge market for leveraging technological talent and the creation of the job market. The National Association of Software and Service Companies (NASSCOM) has reported that around 1100 GICs in India are now working as a sector of employment for 800,000 people. Beyond the ample opportunity provided by Facebook and other digital marketplaces, innovative tech platforms not only have created scope for employment but also have created scope for employment and secured the future of the employees too. Through blockchain technologies, Sri Lanka has pushed itself further by experimenting with cyber-insurance (insurtech) policies.[35] Hence, insurtech opportunities also created a job market for aspirant innovators where companies like Fairfax Financial Holdings Ltd., InsuraGuest Technologies Inc., and Berkshire Hathaway Inc. are sponsoring research and innovations.

---

[28] "How Thailand Is Bringing Technology to The Table," *CNBC,* June 18, 2018, https://www.cnbc.com/advertorial/2018/06/18/how-thailand-is-bringing-technology-to-the-table.html.
[29] "The Report: Thailand 2016," Oxford Business Group.
[30] "The Report: Thailand 2016," Oxford Business Group.
[31] "Record 38.27m Tourists in 2018; 41m Expected in 2019," *The Bangkok Post*, January 28, 2019.
[32] "India's Food-tech Industry to Grow at 25% CAGR to $8 Billion by 2022-end: Google-BCG report," *Financial Express*, January 28, 2020, https://www.financialexpress.com/industry/indias-food-tech-industry-to-grow-at-25-cagr-to-8-billion-by-2022-end-google-bcg-report/1837786/.
[33] Sarah C Schoeffel, "Blockchain Technology: Agriculture's next revolution?," *Observer Research Foundation (ORF) Issue Brief*, No. 314, 2019.
[34] Schoeffel, "Blockchain Technology."
[35] "Technology Transforms the Insurance Market," *PRNewswire,* March 31, 2020, https://www.prnewswire.co.uk/news-releases/technology-transforms-the-insurance-market-879845988.html.

4.2 *The Threats: Crime-Security Dynamics*

With the increasing cyberspace of the BIMSTEC countries, along with the manifold opportunities, a number of threats have also been in question. The threats can come from both state and non-state actors. Depending on the motivations, the threats can have diverse impacts on the perceived security of any country.

Although cyberspace operates in an intangible sphere beyond the typical Westphalian concept of border and geopolitical frontiers, still a nation-state can become a threat for another state due to geopolitical motivations. Often this kind of rivalries include direct or indirect sponsorship of hackers or hacktivists. Both Pakistan and India have been engaged in information warfare taking advantage of online campaigns against each other. In 1998, India's Atomic Research Centre was infiltrated by Pakistani hackers.[36] Bihar Education Department's website was hacked on 18 August 2019, where the hackers were found uploading messages praising Pakistan on the webpage.[37] The official website of Pakistan's Ministry of External Affairs was also hacked on 17 February 2019, for which the ministry sources blamed India.[38] A North Korean hacker group reported being affiliated with the government also carried out cyber espionage in April 2018 using Thai servers.[39] The Commercial Bank of Ceylon, Sri Lanka's website was targeted in July 2016 as well.[40]

At times, the motivations are not always based on a geopolitical or ideological endeavour. Often the motivation becomes entirely profit-driven, where cyber criminals would operate individually or through an organised network to carry out cyber infiltrations. According to the Bank of Thailand (BOT), hackers stole information of around 120,000 customers from Kasikornbank and Krung Thai Banks, two prominent commercial banks in Thailand, in August 2018.[41]

Threats can also come from terrorists carrying out attacks to spread ideological violence and terror financing. Moreover, there can be mere thrill-seekers who might organise a cyber-attack to achieve satisfaction. There can also be cyber threats emerging from inside the country. Hindu nationalist political organisation Rashtriya Swayamsevak Sangh (RSS) in India was found to be targeting around 1400 WhatsApp user accounts of Indian journalists and

[36] Kate Fazzini, "In India-Pakistan conflict, There's a Long-simmering Online War, and Some Very Good Hackers on Both Sides," *CNBC,* February 27, 2019, https://www.cnbc.com/2019/02/27/india-pakistan-online-war-includes-hacks-social-media.html.
[37] "Bihar Govt Website Hacked, Hackers Post message praising Pak," *India Today,* August 28, 2019, https://www.indiatoday.in/india/story/bihar-govt-website-hacked-hackers-post-message-praising-pak-1582104-2019-08-18.
[38] "Pakistan's Ministry of External Affairs website hacked, officials blame India," *The Economic Times,* February 17, 2019, https://economictimes.indiatimes.com/news/politics-and-nation/pakistans-ministry-of-external-affairs-website-hacked-officials-blame-india/articleshow/68032628.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
[39] "North Korean Hackers Used Servers in Thailand to Carry Out Large Scale Global Cyber-attacks," *The Nation Thailand,* April 27, 2018, https://www.nationthailand.com/breakingnews/30344100.
[40] Jason Murdock, "Commercial Bank of Ceylon Website Hit by Hack Attack," *International Business Times,* July 14, 2016, https://www.ibtimes.co.uk/commercial-bank-ceylon-website-hit-by-hack-attack-1560271.
[41] "Two Major Thai Banks Hacked, Personal Details from Over 120,000 Customers Stolen," *Xinhua,* August 02, 2018, http://www.xinhuanet.com/english/2018-08/02/c_137363825.htm.

activists.[42] This type of insider threat can be motivated by political or ideological discontent.

As globalisation and the spread of information technology have made national borders porous, transnational crime has become a major concern. Given that national governments do not have full-fledged control over cyberspace, a large share of transnational criminal activities is organised and operated through cyberspace. Terror groups operating in the BIMSTEC area are known to be using mobile applications like Protected App, Threema and Telegram, which help them operate anonymously.[43] Another area of concern is the ongoing peril in the cryptocurrency business.

There is hardly any country that has not been affected by the risk of it. With India withdrawing its ban on cryptocurrency trading on 05 March 2020, the door has been exposed to a new pandora's box. The Economic Times has noted that even government websites like the Director of Municipal Administration of Andhra Pradesh, Macherla Municipality and Tirupati Municipal Corporation had been used to put malicious traps which provide the hackers and cyber-criminals "magic money" off of some apparently harmless websites.[44] Along with cryptocurrency, crypto-markets have also flourished, pushing forth an unimaginable amount of drug trafficking and human trafficking. Within and beyond the web pages' common surface lies a dark network of the online transaction of drugs, weapons and illegal and forced human mobility. A 21-year-old person was arrested in Alambagh, Lucknow, India, in February 2020 for selling drugs over the dark web.[45] Another youth from Mysuru, Chennai, was arrested for his attempts to smuggle illegal party drugs from the Netherlands.[46] The drugs were worth INR 30 lac and were ordered through the dark web.[47]

The Bangkok Post mentions the mischievous world of the crypto-market as a "godsend" for paedophiles. The Thai government, hence, has shown crucial concern over the encrypted world of cyberspace as kids aged between eight and 12 have an average of 35 hours of online usage of the internet (three hours more than the global average) and 60 per cent of them are under the risk of being exposed to sexual exploitation.[48] Julian Broséus, Damien Rhumorbarbe, Marie Morelato and

[42] "WhatsApp Confirms Indian Journalists and Activists Targeted in Hack," *The Economic Times,* November 1, 2019, https://economictimes.indiatimes.com/tech/internet/whatsapp-confirms-indian-journalists-and-activists-targeted-in-hack/articleshow/71833170.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
[43] Iftekharul Bashar, "The Evolving Threat in Bangladesh," *Counter Terrorist Trends and Analyses* 9, no. 3 (March 2017): 15-18.
[44] Nilesh Christopher, "Hackers Mined a Fortune from Indian Websites," *The Economic Times,* September 17, 2018, https://economictimes.indiatimes.com/small-biz/startups/newsbuzz/hackers-mined-a-fortune-from-indian-websites/articleshow/65836088.cms?from=mdr.
[45] "How 21-year-old Lucknow Lad Ran Global Drug Racket in Garb of Selling Online Medicines," *Times of India*, http://timesofindia.indiatimes.com/articleshow/74109646.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.
[46] "Man Held in Chennai for Selling Illegal Party Drugs," *The Times of India,* March 14, 2020, https://timesofindia.indiatimes.com/city/chennai/man-held-in-chennai-for-smuggling-illegal-party-drugs/articleshow/74625166.cms.
[47] "Man Held in Chennai," *The Times of India*.
[48] "Dark Net, Cryptocurrency A Godsend for Paedophiles," *Bangkok Post*, February 18, 2020, https://www.bangkokpost.com/thailand/general/1860354/dark-net-cryptocurrency-a-godsend-for-paedophiles.

Ludovic Staehli, in their study named "A geographical analysis of trafficking on a popular darknet market" have identified crucial geographical points include shipping countries and shipping destinations of illicit trade via the darknet.[49] Among the groups, except for Nepal and Myanmar, the vendors have mentioned the rest of the BIMSTEC countries as destination points.[50] However, it is, by no means, a relief for the former ones. The Kathmandu Post has posited serious concern over Nepal's future considering the organised crime known as the Nigerian-19 scam, of which around 38 Nepalese citizens became victims between 2014 and 2016.[51] The number of sex trafficking of Nepalese women is around 15,000 every year, as the UN estimates.[52]

The dark web has also become a nirvana for propaganda operations and the spreading of fake news. With the rise of global populism, individuals and groups are being targeted for injecting hate speech and seeds of radicalisation while ensuring anonymity. Sri Lanka's concern over the radicalisation in the Southern Karnataka, Kerala, Telangana, and Tamil Nadu states owes to the major exposure to social media websites and the widespread propaganda indoctrinated via the dark web, as per the Sri Lankan intelligence agencies.[53] The agencies have also identified the *modus operandi* of propagandisation as "stealth technology" and upgraded to the traditional form of radicalisation.[54]

Similarly, the autonomous system has opened itself up for Denial of Service (DoS) attack, which is initiated by flooding the target with traffic attacks resulting in a shut-down of the network and making it inaccessible to the user base. At the beginning of the previous decade, Myanmar's Ministry of Post and Telecommunication (PTT) official website faced disruption, which had a notable impact on the tourism industry.[55] In 2015, a number of Thai government's official websites were victims to DoS attack as a part of protest against its decision to limit inappropriate sites.[56] The source of the threat was completely 'internal' and the popular discontent was manifested in a public petition titled "Great Firewall of Thailand" comparing the government's decision to that of the Chinese government.[57] In 2014, India became the top destination for origination of such attacks, accounting for 26 per cent DoS attack aimed against gaming, software as

[49] Julian Broséus, Damien Rhumorbarbe, Marie Morelato, Ludovic Staehli, and Quentin Rossy, "A Geographical Analysis of Trafficking on A Popular Darknet Market," *Forensic Science International* 277, (2017): 88-102.
[50] Broseus et al., "A Geographical Analysis," 88-102.
[51] Dipesh Khatiwada, "Into the Dark Web," *The Kathmundu Post,* February 27, 2016, https://kathmandupost.com/miscellaneous/2016/02/27/into-the-dark-web.
[52] Bimal Pratap Shah, "Dark Matter," *The Kathmundu Post*, June 21, 2015, https://kathmandupost.com/opinion/2015/06/21/dark-matter.
[53] Rohini Swamy and Revathi Krishnan, "Now Linked to Sri Lanka Terror, Here's How South India Became a Hotbed of Radicalization," *The Print,* May 09, 2019, https://theprint.in/india/now-linked-to-sri-lanka-terror-heres-how-south-india-became-a-hotbed-of-radicalisation/233228/.
[54] Swamy and Krishnan, "Now Linked to Sri Lanka Terror."
[55] Paul Roberts, "Massive Denial Of Service Attack Severs Myanmar From Internet," *Threat Post,* November 03, 2010, https://threatpost.com/massive-denial-service-attack-severs-myanmar-internet-110310/74638/.
[56] "Thai Government Websites Hit by Denial-of-service Attack," *BBC News,* October 01, 2015, https://www.bbc.com/news/world-asia-34409343.
[57] "Thai Government Websites Hit," *BBC News*.

well as media websites and services.[58] Mumbai and Pune-based Internet service providers (ISPs) of India also reported being targeted in a distributed denial of service (DDoS) attack, twice between September 2015 and January 2016 and the victims were anxious about a potential connection of the event to cyber-terrorism.[59]

On the other hand, the IoT has become another buzzword in the academic and practical world of securitisation. The phrase refers to a web-based technical network that operates through a number of interrelated devices facilitating transactions without any human interaction.[60] While globally and regionally IoT is expanding in a massive way, breaching of privacy has also become a severe concern. NASSCOM predicts that IoT will become worth of US$15 billion by 2020, keeping pace with the estimated US$1.2 trillion of global spending.[61] Recent evidence of recording and transferring data without the user's consent have become a burning question regarding the associated risk and reliability even concerning major companies like Google or Microsoft and areas like the healthcare segment.[62] The National Broadcasting and Telecommunications Commission (NBTC) of Thailand has also shown concern over the issue as the organisation sets up two committees dedicated to regulatory frameworks regarding IoT devices.[63] The key areas would address privacy, security, data arrangement structure and data interoperability, eventually looking forward to a Personal Data Protection Act (PDPA).[64]

The Bangladesh Bank heist on 04 February 2016 showed how every country and every sector is more or less prone to cyber-attacks. The target was to steal around US$101 million from the Bank's account with the Federal Reserve Bank of New York.[65] US$81 million was transacted to four accounts with Rizal Commercial Banking Corporation (RCBC), Manila and US$20 million to Pan Asian Bank in Sri Lanka.[66] The US$20 million amount sent to Sri Lanka and US$15 million to the Philippines was recovered later.[67]

[58] "26 per cent of Distributed Denial of Service Attacks this Year Originated from India: Symantec," *The Economic Times,* October 21, 2014, https://economictimes.indiatimes.com/tech/internet/26-per-cent-of-distributed-denial-of-service-attacks-this-year-originated-from-india-symantec/articleshow/44900739.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst.

[59] "Internet Providers Claim DDoS attack," *The Hindu,* October 17, 2016, https://www.thehindubusinessline.com/info-tech/internet-providers-claim-ddos-attack/article9231035.ece.

[60] Rolf H Weber, "Internet of Things–New Security and Privacy Challenges," *Computer Law & Security Review* 26, no. 1, (2010): 23-30.

[61] Kal Bhushan, "World Internet of Things Day 2019: IoTs are becoming big but so are privacy risks," *The Hindustan Times,* April 09, 2019, https://www.hindustantimes.com/tech/world-internet-of-things-day-2019-iots-are-becoming-big-but-so-are-privacy-risks/story-479VjkFAyC5PXurWwhRBPP.html.

[62] Bhushan, "World Internet of Things Day."

[63] "NBTC Readying Two Drafts for IoT," *The Bangkok Post,* January 24, 2019, https://www.bangkokpost.com/tech/1700732/nbtc-readying-two-drafts-for-iot.

[64] "NBTC readying two drafts," *The Bangkok Post.*

[65] "Report in Bangladesh Bank Heist Case on May 21," *Dhaka Tribune,* April 17, 2019, https://www.dhakatribune.com/business/banks/2019/04/17/report-in-bangladesh-bank-heist-case-on-may-21.

[66] "Report in Bangladesh Bank," *Dhaka Tribune.*

[67] "Report in Bangladesh Bank," *Dhaka Tribune.*

From the aforementioned discussion, it can be easily understood that no country is, indeed, free from a potential threat of cyber-attack. While opportunities have changed the national and transnational industries in a massive way; the threats have also disrupted the security of individuals, private sectors and the states. Thus, both the threats and the opportunities have to be considered parallel and holistic to be facilitated by the extended cyberspace in the BIMSTEC region.

5. Securitisation Strategy

It is undeniable that security is an integral part of development. To ensure a pragmatic securitisation policy, regional efforts have to be complemented by national measures. Following the regulatory frameworks and threat perception from other member states of BIMSTEC and taking influences from good experiences at the international level, the countries can take compatible initiatives.

5.1 *Securitisation of Cyberspace in BIMSTEC: Lessons from Good Practices*

The BIMSTEC states need to create a generic framework for adopting a comprehensive cybersecurity act for all the states. It cannot be ignored that BIMSTEC still has not organised a separate convention on cyber-threat or cybercrime. Moreover, cybersecurity is yet not a subsector under the security-specific area of cooperation.

BIMSTEC states have already taken some policies to address cyber threats. The first meeting of national security chiefs took place in New Delhi on 21 March 2017. The meeting underlined both traditional and non-traditional security challenges faced by the BIMSTEC member states. It also addressed the emerging trends in cyberspace and highlighted their security implications.[68] The meeting looked forward to deepening cooperation among the different cyber institutions in the member states through a joint forum.[69] The second meeting of the national security chiefs was held in August 2018 where a three-day workshop on cybersecurity was proposed.[70] The workshop was held at Institute for Defence Studies and Analyses (IDSA), New Delhi, India on 05-07 December 2018. It primarily focused on regional cybersecurity cooperation. The workshop highlighted the necessity of developing an effective cybersecurity mechanism in BIMSTEC. At the end of the workshop, a roadmap for BIMSTEC cybersecurity cooperation was proposed.[71] In July 2022, the first meeting of the BIMSTEC Expert Group in Delhi[72] captured computer-based emergency response and threat assessments. During the fifth BIMSTEC summit in 2022, the establishment of a joint forum for cybersecurity cooperation was discussed.[73] However, from the

[68] "First Meeting of the BIMSTEC National Security Chiefs," Ministry of External Affairs, The Government of India, March 21, 2017, https://mea.gov.in/press-releases.htm?dtl/28193/First_meeting_of_the_BIMSTEC_National_Security_Chiefs_March_21_2017.
[69] Ministry of External Affairs, "BIMSTEC National Security Chiefs."
[70] "IDSA-BIMSTEC Workshop on Cyber Security Cooperation," BIMSTEC, accessed March 31, 2020, https://bimstec.org/?event=idsa-bimstec-workshop-on-cyber-security-cooperation.
[71] BIMSTEC, "IDSA-BIMSTEC Cooperation."
[72] "Together for Cyber Security," *Dhaka Tribune*, August 02, 2022, https://www.dhakatribune.com/op-ed/2022/08/02/together-for-cyber-security.
[73] "Security," BIMSTEC, https://bimstec.org/security-2/.

aforementioned discussion, it is understandable that there is still room for improvement. Some good examples can be driven from the cases given below:

5.1.1 *European Union (EU)*

The first case can be demonstrated by the European Union (EU) policies. The EU Cybersecurity Act 2019 looks forward to strengthening the EU Agency for cybersecurity (ENISA) by granting a permanent mandate, providing resources and associating with new tasks. ENISA EU-wide cybersecurity certification framework focused on digital products, services and processes.[74] ENISA works together with both the state and private organisations and promotes and ensures implementation of the pan-European cybersecurity exercises, development of national cybersecurity strategies, focuses on capacity building of Computer Security Incident Response Team (CSIRT), carrying out studies on IoT and smart infrastructures, enhancing privacy, secure eIDs and trust services etc.[75] Council of Europe's Convention on Cybercrime 2001 or the Budapest Convention, was the first international treaty solely focused on crimes committed via computer networks. It sought to generate common criminal policies against cybercrime in the form of appropriate legislative and cooperative measures, including infringements of copyright, cyber-fraud, child pornography and invasion of privacy.[76]

5.1.2 *ASEAN*

The ASEAN region was hit by a number of cyber-attacks ranging from the North Korean cryptocurrency invasion to the information leakage from the database of Singapore's healthcare institutions. However, ASEAN took the crisis to its heart, and took a number of other measures as well. The Singaporean effort can be considered as a paramount example as apart from the ACCP, the country also announced a probable allocation of SS$ 30 million (US$22 million) for the establishment of the ASEAN Singapore Cybersecurity Centre of Excellence (ASCCE).[77] A combination of these mutual efforts led to the formulation of the ASEAN Cybersecurity Cooperation Strategy in 2017. The strategy focuses on coordination of cyber policies along different dimensions—political, strategic, economic, and socio-cultural ensuring rapid implementation of norms of cooperation and capacity building regarding cyberspace in the region.[78] The Association of Southeast Asian Nations (ASEAN) Cyber Capacity Program (ACCP) was launched by Singapore in 2016 with an investment worth US$10

[74] "The EU Cybersecurity Act," European Commission, accessed March 31, 2020, https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-act.
[75] "ENISA," EU Agency for Cybersecurity, accessed March 31, 2020, https://www.enisa.europa.eu/about-enisa.
[76] "Council Gives Mandate to Commission to Negotiate International Agreements on E-evidence in Criminal Matters," Council of the European Union, accessed March 31, 2020, https://www.consilium.europa.eu/en/press/press-releases/2019/06/06/council-gives-mandate-to-commission-to-negotiate-international-agreements-on-e-evidence-in-criminal-matters/.
[77] "Centre for ASEAN to Jointly Tackle Cyber Threats," *The Straits Times,* October 03, 2019, https://www.straitstimes.com/tech/centre-for-asean-to-jointly-tackle-cyber-threats.
[78] "Can ASEAN Continue to Improve Cybersecurity in the Region and Beyond?," *Council on Foreign Relations*, March 22, 2018, https://www.cfr.org/blog/can-asean-continue-improve-cybersecurity-region-and-beyond.

million with the purpose of organising resources, expertise and training in cybersecurity as well as support discussion and consultancy work.[79]

5.1.3 *African Union (AU)*

The African Union (AU) Convention on Cybersecurity and Personal Data Protection was adopted in June 2014 and comprehended a number of issues like electronic commerce, principles of processing sensitive data, subjects' rights, security and sustainability obligations of data controllers, legal measures, including the development of a national cybersecurity framework.[80] The Executive Council of the AU had also looked forward to a specialised technical committee to create an Africa Cybersecurity Collaboration and Coordination Committee.[81] The first AU cyber-security experts' group meeting held on 10 to 13 December 2019 in Addis Ababa, Ethiopia, also emphasised developing its own regional philosophy, ethics, policy, strategies and accountability framework dedicated to sustainable cyber-security and maintenance of Artificial Intelligence (AI).[82]

Comparing the good practices in other regional forums and the initiatives taken by BIMSTEC, it is essential to recognise that the member countries in this sub-regional group have to go for a more robust, tacit and comprehensive framework in order to properly address cybersecurity and cyberspace.

5.2 *Securitisation Measures*

Securitisation measures can be advanced in two different ways: regulation and capacity building. Both top-down and bottom-up approaches are equally important to ensure the proper adoption and implementation of the policies. The first area of intervention for the BIMSTEC countries can be identifying common threats faced by all or most of the member states and defining some norms for furtherance. In this regard, creating a BIMSTEC cybersecurity framework can be a vantage point for addressing the ongoing threats. After defining common norms and adopting a common legal resolution, the next step would be ensuring that the member states ratify all the legal frameworks and that the policies are adapted to their national frameworks. In the case of the policies determined by the AU Convention on Cybersecurity and Personal Data Protection, this became a burning question. Mr Sand Mba Kalu, Executive Director, Africa International Trade and Commerce Research (AITCR), in an interview with the national newspaper This Day, opined Nigeria's delay in endorsing the convention is creating a "greater risk of economic isolation and stagnation."[83] Thus, it is very important to organise a genuine willingness among the countries and a sense of regionalism as well as the greater

[79] Prashanth Parameswaran, "Singapore Unveils New ASEAN Cyber Initiative," *The Diplomat,* October 14, 2016, https://thediplomat.com/2016/10/singapore-unveils-new-asean-cyber-initiative/.
[80] "African Union Convention on Cyber Security and Personal Data Protection," African Union, accessed March 31, 2019, https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection.
[81] Mu Xuequan, "Africa Urged to Create Secure Cyberspace to Drive Digital Transformation," *Xinhua,* December 15, 2019, http://www.xinhuanet.com/english/2019-12/15/c_138631762.htm.
[82] Xuequan, "Africa cyberspace transformation."
[83] "AfCTA: Expert Urges FG to Sign Cybersecurity Framework," *This Day,* January 20, 2020, https://www.thisdaylive.com/index.php/2020/01/20/afcta-expert-urges-fg-to-sign-cybersecurity-framework/.

good. For this purpose, the policies should not only address theoretical and normative measures, rather standardised implementation framework should follow suit.

Institutional mechanisms should also be into consideration for making the policies sustainable. BIMSTEC already has a number of institutions dedicated to particular areas: BIMSTEC Energy Centre (BEC) and BIMSTEC Centre on Weather and Climate (BCWC). Given how cybersecurity has become an unavoidable locus of importance, BIMSTEC can consider setting up a BIMSTEC centre on cybersecurity and cyber cooperation.

In order to facilitate confidence-building measures, BIMSTEC can also play the role of coordinator for the member states. Taking the example of Singapore's role in advancing the ASEAN framework, it can also motivate the countries to share individual expertise and technology with other member states as well as provide employment opportunities and scholarships for the countries in a comparatively less advantageous positions. There can be regular workshops like the one arranged by IDSA in 2018 to enunciate further dialogues on cyber-security and future prospects.

It is important to start from the grassroot level for capacity building. As much as it is necessary to provide technological leverage to each of the social strata. The tangible and material resources should be complemented with awareness and technical know-how. Each country's ministries can take the initiative to educate different sectors. There can also be multi-level cooperative measures. For example, the ministry of agriculture in different countries can organise transnational expert meetings and digital outreach programme for the farmers. Public-private partnerships can hold a key potential in this regard. In a 2011 report of Food and Agriculture Organisation (FAO), it was mentioned that in India, private investment would account for up to 16 per cent investment of total agricultural research spending.[84] In this way, food security and cybersecurity can go hand in hand. This conceptualises how all countries can benefit from this kind of cooperation. Coordinating e-learning through proper utilisation of the Learning Management System (LMS) can help the countries address a large portion of the youth and increase awareness. The government of Bangladesh has already established Information and Communication Technology (ICT) division allocating around BDT 19.30 billion for the 2019-20 fiscal year.[85]

Multinational companies and digital farms can be a major source of investment for building up financial capacity. Making ad-hoc or limited concords with prominent Silicon Valley investors can be a profitable strategy. Thus, not only investment in the digital economy but also legal and institutional arenas should be taken into consideration.

[84] "Public-private Partnerships for Agribusiness Development," United Nations, Food and Agriculture Organization, 2016.
[85] Abdullah Al Mamun Bhuiyan, "Codifying e-learning in Bangladesh," *The Financial Express,* February 28, 2020, https://thefinancialexpress.com.bd/views/views/codifying-e-learning-in-bangladesh-1582901375.

Building up intelligence capacity and enhancing sharing of information among the intelligence organisation of the member states can facilitate the security of cyberspace. The financial intelligence units and financial monitoring units of the states can collaboratively work on addressing cyber threats. Other umbrella organisations like the Financial Action Task Force (FATF), Egmont Group, and Asia-Pacific Group (APG) on Money Laundering can be accomplices for traversing the lack of information and other necessities. The cybersecurity and cybercrime departments of the respective countries' internal policing departments can also collaborate.

Professional training courses on cybersecurity can be introduced at the academic level. Bangladesh has already endorsed ICT in the higher academic curricula and is expected to be a compulsory subject at the primary level by 2021.[86] Different organisations like ACIS Professional Center Co., Ltd in Thailand and the Institute of Information Security (IIS) in India also provide consulting services and training on cybersecurity. However, there must be a coordinated venture to bring these institutions under a common platform to necessitate scholarship on cybersecurity and cyber threats at national, local and regional levels.

Finally, it can be said that the risks in cybersecurity must be handled sensitively and imperatively. Thus, while legal frameworks and regulatory mechanisms are obviously important, it is also necessary to make sure that society is prepared eloquently to receive the norms and act out the regulations properly.

6. Conclusion

Defining cyberspace, like the term security, is also very difficult. Securing cyberspace is an emerging concern among almost all countries worldwide. Securitisation theory, as a critical instrument of nationalism, by the Copenhagen School, emerged as a crucial prism for the understanding of national security after the establishment of Westphalian states and how nation-states evolved with newer forms of techniques in protecting national interests. Securitisation is also a popular tool for opinion building and generating extraordinary means that follow the priority of the nation-states' interests. In the twenty-first century, technological advancement increased human dependence on critical networks exponentially. Therefore, the security actors, like state, technology experts, business groups need to focus on the security networks. They feel a compulsion to securitise cyberspace. This paper applied securitisation discourse to cyberspace to explain that cybersecurity should not be all about technification driven by computer networks; rather, it must inherit an understanding and implementation of measures for effective management of networks and security breaches associated with them. There is a wide range of actors in securitisation and the audience of the securitisation process is also multiple and sophisticated. Moreover, in the process of securitisation in many cases, nation-states can individually act as a securitising actors, but in the process of securitisation of cyberspace, nation-states need to

[86] Al Mamun Bhuiyan, "Codifying E-learning in Bangladesh."

come together to act as "security actors" at the regional level as well as in the international arena. As mentioned in the paper, the statistical and empirical evidence demonstrates that the overall breadth of cyberspace of the BIMSTEC countries has extended over the years. Given the enormous coverage and popularity of information technology, the extended cyberspace has created a scope of opportunities for all of the BIMSTEC countries. All the positive changes have opened up a huge market for leveraging technological talent and the creation of the job market. Meanwhile, several threats have also penetrated the countries so far as the security of cyberspace is concerned. Cybercrimes are often motivated based on geopolitical or ideational rivalry, or profit-driven organised cybercrimes are the major threats to securitising cyberspace in the BIMSTEC region. Moreover, there can be mere thrill-seekers who might organise a cyber-attack just to achieve satisfaction. However, no country is, indeed, free from a potential threat of cyber-attack. While opportunities have changed the national and transnational industries in a massive way, the threats have also disrupted the security of individuals, private sectors and the states. Thus, both the threats and the opportunities have to be considered in a parallel and holistic manner to be facilitated by the extended cyberspace in the BIMSTEC region.

To ensure a pragmatic securitisation policy, regional efforts have to be complemented by national measures. Following the regulatory frameworks and threat perception from other member states of BIMSTEC and taking influences from good experiences at the international level, the countries can take compatible initiatives. Comparing the good practices in other regional forums and the initiatives taken by BIMSTEC, it is important to recognise that the member countries in this sub-regional group have to go for a more robust, tacit and comprehensive framework in order to properly address cybersecurity and cyberspace. Countries in the region should not only invest in the digital economy but also in legal and institutional arenas should be taken into consideration. Building up intelligence capacity and enhancing sharing of information among the intelligence organisation of the member states can facilitate the security of cyberspace. After all, though the regulatory framework or mechanisms are sine qua non for more secure cyberspace, regional countries need to be careful about the socio-cultural habitats and to ensure whether the people are willing to accept new norms and act accordingly.