BIPSS Commentary

www.bipss.org.bd

March-2023

BIPSS Towards a Secure World

Asian Cyber Security Community (ACSC):

A collaborative approach to cyber governance and management

- ***Asheer Shah***[1]

Cyber Security, two words, multiple aspects. Currently, a single player exists in the multiverse of cyber security governance, the individual states. Whereas the world of cyber security is like an octopus with multiple tentacles and each tentacle becoming another octopus itself. The cyber arena and its security implications expand like a spider web. The actors governing the very arena need to expand simultaneously. A multiplying variable requires a varied range of governing actors. The cyber world is borderless, and thus, the cyber world's governance and management must be innovative and borderless. It is characteristic of the aspect that influences the governance approach. A 21st-century global village issue must be addressed in a digitalised mindset. In this article, cyber security is the paradigm, and regional integration is the instrument deployed in that paradigm. The independent variable is cyber security, and the dependent variable is the potential of integration/ intergovernmental schemes in Asia. The purpose of this article is to emphasise the role of an integrative or collaborative approach to cybersecurity governance. Initially, the article is nurturing the debates and arguments existing in the scholarly world of cybersecurity. The article then proceeds to assess the importance of international and regional schemes like the Association of Southeast Asian Nations (ASEAN), the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) and the South Asian Association for Regional Cooperation (SAARC) in governing the cyberspace of Asia. Finally, the article innovates a mechanism or strategy to unite Asia's cyberspace, at least at a regional level, by proposing a cyber security community.

[1] Asheer Shah is a researcher, project specialist and negotiator. He specialises in international relations, comparative politics and public policy governance. His research expertise lies in the regional integration of Europe and Asia and further aims to focus on cybersecurity governance aspects of regional integrations. He is a Research Associate at the Bangladesh Institute of Peace and Security Studies (BIPSS).

Introduction

'replace snipers with hackers,

replace bullets with data packets,

replace chemical warfare with computer viruses,

replace anti aircraft guns with firewalls,

replace sentries with intrusion detection systems,

replace military intelligence with auditing tools,

replace physical battlefields with cyber equivalents that

potentially extend conflicts to every point on the planet,

and

replace international treaties, policies, and organizations

with NOTHING'

- *Sam D. Nitzberg*[2]

The vast portfolio of existing literature covers aspects of the digital paradigm, including the classification of cyber attacks, governance models, case studies and so forth. This article mainly focuses on the arguments and debates on cybersecurity governance and management. It is simply because the technical aspects of cyber security can be developed and enhanced when the framework is laid out. The idea is very similar to constructing a building, where a blueprint is the first step for construction. The cyber security governance framework is the first step in securing cyberspace.

Schwartau categorised information warfare into three categories; personal, corporate, and global information warfare.[3] On the other hand, Nitzberg outlined the urgency of governance, management, legislation and framework in the cyber world and information society. In the cyber battlefield (information war), he emphasised the development of information systems

[2] Nitzberg, Sam. 1997. "Cyber battlefield - is this the setting for the ultimate world war?" *International Symposium on Technology and Society*. Ed., Anon. IEEE, Piscataway, NJ, United States. pp. 100-106.

[3] Schwartau, Winn. 1995. "Information warfare: chaos on the electronic super-highway." First Trade paperback edition, Thunder's Mouth Press. pp. 17-19.

security policies, implementing information security measures, the institution of computer crime laws, and international computer crime cooperation. Similar to Nitzberg, Chou et al. also suggested frameworks for managing cyber security through non-technical ways (corporate security policy and educating and training users about that policy) and technical measures (access controls, authentication, encryption, firewall, audit, anti-virus, and self-assessment tools).[4] Axlerod and Jay argued a set of advice for information technology (IT) policy formulators and law enforcement officers (policy implementers) dealing with crime and punishment in cyberspace.[5]

Pawlak and Wendling, similar to other authors, argued the governance structure of cyberspace but critically challenged the capacity of a single government to solve a transborder issue.[6] Challenging the post-Westphalian world order, applying the sovereignty principle in cyber governance has been criticised because, similar to my mindset, Pawlak and Wendling thought along the same lines of a collaborative approach. In their words:

> *"With an increasing number of threats crossing* ***traditionally defined physical borders****, governments' ability to effectively perform their duties is becoming ever more complicated."*

DeNardis argued the techniques used to conduct cyber attacks on commercial and individual entities (computer viruses and worms, unauthorised access to private data and computing resources, identity theft, critical infrastructure attacks, and denial of service attacks).[7] DeNardis further argues the controversiality of cryptography and that security attacks are the new political and warfare instruments. In contrast to DeNardis, Yang and Mueller presented arguments on internet governance in China by focusing on the timeline of internet policy-making.[8] On the other spectrum of the thought process, Lindsay argues the digital war mechanics adopted by China.[9] In the advanced digitised paradigm, the use of digital weapons and schemes is inevitable. Contrastingly, Simon and Goede analysed European cyberspace

[4] Chou, David C., David C. Yen, Binshan Lin and Philip Hong-Lam Cheng. 1999. "Cyberspace security management". *Industrial Management and Data Systems.* Emerald. Vol 99 (8): 353-361.

[5] Axlerod, Harvey and Daniel R. Jay. 1999. "Crime and Punishment in Cyberspace: Dealing with Law Enforcement and the Courts." *Proceedings ACM SIGUCCS User Services Conference*. Association for Computing Machinery. pp. 11-14.

[6] Pawlak, Patryk and Cécile Wendling. 2013. "Trends in cyberspace: Can governments keep up?". *Environment Systems and Decisions*. Kluwer Academic Publishers. Vol. 33 (4): 536-543.

[7] DeNardis, Laura. 2014. "The global war for internet governance." Yale University Press. Chap. 4, pp. 86-106.

[8] Yang, Feng and Milton L. Mueller. 2014. "Internet governance in China: a content analysis." *Chinese Journal of Communication.* Routledge. Vol. 7 (4): 446-465.

[9] Lindsay, Jon R. 2015. "The impact of China on cybersecurity: Fiction and friction". *International Security.* MIT Press Journals. Vol. 39 (3): 7-47.

governance.[10] Two agencies working in the European Cybersecurity paradigm have been assessed by the authors: European Union Agency for Cybersecurity [ENISA (2009, Crete, Greece)] and European Cybercrime Centre [EC3 (2012, Hague, Netherlands)].

According to Pawlak, to secure cyberspace, sharing good practices among countries and regional organisations can better aid the governance of the digital world.[11] The same idea is sitting in the back of my mind when writing this article. Regional organisations must coordinate and collaborate in the digitised global village. For instance, North Korean hackers are popular for their notorious cyber stealings of traditional and digitised currencies like cryptocurrency. For instance, the North Korean hackers conducted a cyber heist and almost stole $1 billion from Bangladesh's national bank.[12] According to the media, North Korea grooms cyber-warriors.[13] It is said even today, North Korea fosters, nurtures and shapes tech-genius criminals for launching cyber heists every day all around the globe. Global cyberspace is vulnerable to 'tech-forces' like North Korean programmers and hackers.

ASEAN, BIMSTEC, SAARC & ITU

Evidence of Paradigm {ITU}

The overview and complete knowledge of the International Telecommunication Union (ITU) can be easily accessed online. This heading exists to simplify and clarify to the audience that governance of the internet in a united manner already exists on this earth, and that too since 1865.

> *"Every time you make a phonecall via the mobile, access the Internet or send an email, you are benefitting from the work of ITU. ITU is* ***committed to connecting all the world's people*** *– wherever they live and whatever their means. Through our work, we protect and support everyone's right to communicate." - ITU*[14]

The goal of ITU is to simplify access to information through radio, submarine cable, satellite and similar connecting materials. This innovative research aims to focus on securing the

[10] Simon, Stephanie and Marieke de Goede. 2015. "Cybersecurity, Bureaucratic Vitalism and European Emergency". *Theory, Culture & Society.* Vol. 32 (2): 79-106.

[11] Pawlak, Patryk. 2016. "Capacity Building in Cyberspace as an Instrument of Foreign Policy". *Global Policy.* Blackwell Publishing Ltd. Vol. 7 (1): 83-92.

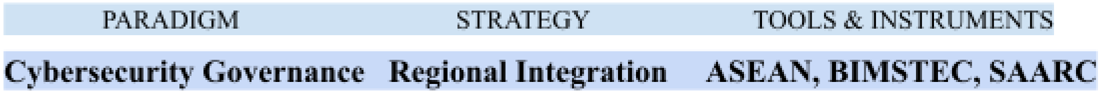
[12] Explained: The story of how North Korea hackers stole $81 million from Bangladesh Bank | Explained News,The Indian Express

[13] How N Korea trained hackers to almost steal $1bn from Bangladesh | undefined (tbsnews.net)

[14] About ITU

world that develops from access and usage of the internet, radio signals, telecommunication, artificial intelligence and so forth. And to secure the cyber world, this research implements integrational strategies using Asia's regional integration schemes as tools and instruments.

If and when positioned in a formula, it develops into the equation below:



PARADIGM	STRATEGY	TOOLS & INSTRUMENTS
Cybersecurity Governance	**Regional Integration**	**ASEAN, BIMSTEC, SAARC**

Analysing Tools & Instruments {testing potentials}

This heading analyses the potentials and scopes for ABS[15] in fostering a cyber security community in Asia. ASEAN is the oldest and most functional scheme existing in Asia currently. BIMSTEC is relatively newer, performing better than SAARC but lagging way behind ASEAN. This is because all member states participate in BIMSTEC Summits, which is different for SAARC. Analysing, comparing and contrasting the performance of ASEAN, BIMSTEC and SAARC is another dimension, route and scope of research. This research heading solely focuses on comparing and contrasting the cybersecurity governance sector of the three.

The data below shows that BIMSTEC is the most functional in cyber security cooperation compared to ASEAN. SAARC has yet to be addressed since no possible pathway exists in the organisation to secure cyberspace. ASEAN is collaborating mostly on cybercrime, whereas BIMSTEC is collaborating on cyber security. It can be comprehended that ASEAN focuses on the legal frameworks and governance of post-cybercrimes, and BIMSTEC focuses on enhancing cybersecurity governance to abstain from cybercrime. One is a post-cybercrime approach, and the other is a pre-cybercrime approach. The characteristics of the organisations' approaches are perfect when any expert aims to integrate the actions of the regional intergovernmental schemes, which is the whole purpose of the concluding heading.

[15] ASEAN, BIMSTEC and SAARC

ASEAN[16]	**BIMSTEC**[17]	**SAARC**
Three Communities Political-Security Community Economic Community Socio-Cultural Community *“The Senior Officials Meeting on Transnational Crime (SOMTC) Working Group on CyberCrime was established in September 2013 at the 9th ASEAN Ministerial Meeting on Transnational Crime (AMMTC) in September 2013 in Vientiane, Lao PDR to brainstorm practical cooperation in combating cybercrime among ASEAN Member States as well as between ASEAN and its Dialogue Partners.”[18]- ASEAN*	14-15 July 2022: First Meeting of the BIMSTEC Expert Group on Cyber Security Cooperation.[19][20] Lead Country: INDIA[21] Originates from the 2019 agreement made during the meeting of the BIMSTEC National Security Chiefs in Bangkok.[22] 05-07 December 2018, Institute for Defence Studies and Analyses (IDSA), New Delhi, India: BIMSTEC Workshop on Regional Cyber Security Cooperation proposed a roadmap for Cyber Security Cooperation.[23]	Among SAARC nations in the National Cyber Security Index (NCSI), Bangladesh has secured the top spot .[24] ***Existence of expert group or framework?*** **NOT AVAILABLE**

Table 1: Potentials of ABS in fostering ACSC

Asian Cyber Security Community (ACSC)

Innovation

One of the key strategies applied by hackers in the 2016 cyber heist conducted in Bangladesh was timing. The hackers applied the time difference strategy of Bangladesh Bank and the Federal Reserve Bank of New York. As a result, ASEAN and BIMSTEC must maintain a cybersecurity unit which is active 24/7. The two units can function well together if the decision-makers think pragmatically.

Another strategy that worked out for the hackers was the reclaiming procedure's complicacy. Bangladesh Bank officials wanted to reclaim the funds from the Philippines, but it required a court order that gave the hackers time to turn the money traceless. ASEAN and BIMSTEC must construct a feasible and simple fund reclaiming procedure as a cyber crime response. However, ASEAN and BIMSTEC cannot simply function independently since, in the 2016

[16] Read (PDF) Cybersecurity Policy in ASEAN Countries (researchgate.net)

[17] Read Digital forensics and evolving cyber law: case of BIMSTEC countries | Request PDF (researchgate.net)

[18] Senior Officials Meeting on Transnational Crime (SOMTC) - ASEAN Main Portal

[19] First Meeting of the BIMSTEC Expert Group on Cyber Security Cooperation met in New Delhi on 14-15 July 2022 – Home-The Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC)

[20] Together for cyber security (dhakatribune.com)

[21] Bimstec meeting: India takes the lead in setting up Bimstec cyber-response team - The Economic Times (indiatimes.com)

[22] BIMSTEC Expert Group on Cyber Security Cooperation (adda247.com)

[23] IDSA-BIMSTEC Workshop on Cyber Security Cooperation – Home-The Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC)

[24] Bangladesh tops SAARC countries in National Cyber Security Index (unb.com.bd)

cyber heist, the state actors Bangladesh belonged to BIMSTEC and the Philippines belonged to ASEAN. This argument pushes the urgency of collaboration between ASEAN and BIMSTEC in cyberspace.

BIMSTEC-ASEAN partnership is mandatory to undertake the cosmopolitan approach to cyberspace. The partnership satisfies the theory where regionalism takes place from sub-regionalism. The parameters of BIMSTEC and ASEAN are in a suitable position to foster this particular collaboration. As mentioned previously in this research, ASEAN has a post-cybercrime approach, and BIMSTEC has a pre-cybercrime approach. Collaboration leads to the construction of the formula below:

pre-cybercrime approach + post-cybercrime approach = cybersecurity assurance

The idea is explicitly implementable because India is the leading member state of BIMSTEC cyber security cooperation. Intriguingly, India is a dialogue partner[25] of ASEAN. Intriguingly, India and Indonesia are Group of Twenty (G20) members. Fostering collaboration between ASEAN and BIMSTEC is now just a matter of observation since pragmatic routes exist. Borrowing the aspects of quantum mechanics, now that the collaboration aspects between ASEAN and BIMSTEC have been observed, the existence of the Asian Cyber Security Community (ACSC) is inevitable. All that remains is the ideas to put in the documents.

Conclusion: *featuring Recommendations*

The case presented above acknowledges the characteristics of cybersecurity and the circumference of the matter. It is not astonishing that the circumference of cybersecurity is expanding at the same rate as the galaxy. As a fact, this research piece justified the implementation of sub-regional and regional integration strategies in governing the ever-expanding cyberspace. To prove the valid rationale of my idea, I presented the case of ITU. In my analysis, ITU is far geographically, as well as (mentally) in understanding Asian, South Asian and Southeast Asian thought processes. Given such, BIMSTEC and ASEAN were the best tools to be applied in this case.

BIMSTEC and ASEAN connect, hosting two common members; Myanmar and Thailand. The two centre countries of BIMSTEC and ASEAN are India and Indonesia, also G20 members. India, Indonesia, along with Thailand must sit at the steering wheel to initiate this

[25] Cooperation with Dialogue Partners - ASEAN Main Portal

collaboration between the two organisations. These countries are affluent in terms of economy, leadership and governance of the region. Exchanging the ideas among the policy actors and elites of the countries will give a new dimension to regional integration.