International Journal of Business, Arts and Scientific Study (IJBASS)
ISSN: 2709-0825 (Print), ISSN: 3078-2775 (Online), Volume-05, Issue-01, November, 2024
A multidisciplinary journal of Bangladesh Center for Research and Planning (BCRP)

The Role of International Collaboration in Enhancing Cybersecurity in Bangladesh Lessons from Global Best Practices

Mohammad Shahrair Khan
CEO, NexKraft Limited
Founder, ICT Olympiad Bangladesh

Keywords:

Cybersecurity, Bangladesh, Digital Transformation, Global, Cyber Threats

Abstract: This study examines the critical role of international collaboration in strengthening Bangladesh's cybersecurity capabilities as the country undergoes rapid digital transformation. While Bangladesh has made significant strides through initiatives like "Digital Bangladesh," it faces substantial cybersecurity challenges including rising cyber-attacks, limited expertise, and infrastructure vulnerabilities. The research analyzes global best practices in cybersecurity collaboration and identifies key challenges specific to Bangladesh, including technological gaps, resource constraints, and cultural barriers. The study offers strategic recommendations for enhancing Bangladesh's cyber resilience through international partnerships, emphasizing the importance of regional cooperation, capacity building, and participation in global cybersecurity initiatives. The findings suggest that by leveraging international collaboration effectively, Bangladesh can not only strengthen its national cyber defenses but also emerge as a regional leader in cybersecurity, supporting its broader digital development goals while contributing to global cybersecurity efforts.

INTRODUCTION

In an increasingly interconnected world, cybersecurity has become a critical concern for nations across the globe. Bangladesh, as a rapidly developing country with a growing digital landscape, faces significant challenges in securing its cyber infrastructure. This article examines the role of international collaboration in enhancing cybersecurity in Bangladesh, drawing lessons from global best practices.

The primary objective of this study is to analyze the role of international collaboration in enhancing Bangladesh's cybersecurity capabilities and to propose strategic recommendations based on global best practices for strengthening the country's cyber resilience through effective international partnerships.

The digital transformation of Bangladesh has been remarkable, with the country making significant strides in areas such as e-governance, digital financial services, and information technology-enabled services (ITES). However, this rapid digitalization has also exposed the country to various cybersecurity threats, including data breaches, financial fraud, and cyber

attacks on critical infrastructure. As these threats continue to evolve and become more sophisticated, it is evident that Bangladesh cannot tackle these challenges in isolation.
International collaboration offers a promising avenue for Bangladesh to strengthen its cybersecurity posture. By leveraging the expertise, resources, and experiences of other nations and international organizations, Bangladesh can accelerate its efforts to build a robust cybersecurity ecosystem.

OBJECTIVE OF THE STUDY

The primary objective of this study is:
To analyze the role of international collaboration in enhancing Bangladesh's cybersecurity capabilities and to propose strategic recommendations based on global best practices for strengthening the country's cyber resilience through effective international partnerships.

CURRENT CYBERSECURITY LANDSCAPE IN BANGLADESH

Bangladesh has made significant progress in its digital transformation through the "Digital Bangladesh" initiative, launched in 2009 as part of the country's "Vision 2021" plan. This initiative aims to leverage information and communication technologies (ICTs) to drive socio-economic development and improve the quality of life for citizens (a2i Programme, 2020). Key achievements include the expansion of internet connectivity, implementation of e-governance services, growth of the IT and ITES sectors, and rapid adoption of digital financial services.

Despite these advancements, Bangladesh faces numerous cybersecurity challenges. The Bangladesh Computer Security Incident Response Team (BGD e-GOV CIRT) reported a significant rise in cyber-attacks, with over 870 incidents in 2020 alone (BGD e-GOV CIRT, 2021). There is a general lack of awareness about cybersecurity best practices among citizens and organizations, making them vulnerable to social engineering attacks and data breaches (Islam & Rahaman, 2016). While Bangladesh has enacted the Digital Security Act 2018, there are concerns about its effectiveness and potential misuse (Human Rights Watch, 2020). The country also faces a shortage of cybersecurity professionals with the necessary expertise to address complex cyber threats (Rashid et al., 2020). Key sectors such as banking, energy, and telecommunications remain vulnerable to cyber-attacks (Hasan et al., 2019).

The Government of Bangladesh has taken several steps to address these challenges, including the launch of the National Cybersecurity Strategy in 2014, the establishment of BGD e-GOV CIRT, the creation of the Digital Security Agency under the Digital Security Act 2018, and the implementation of cybersecurity training programs (Bangladesh Government, 2014; Digital Security Agency, n.d.; a2i Programme, 2020). However, despite these efforts, Bangladesh still faces significant challenges in building a comprehensive and effective cybersecurity ecosystem.

THE IMPORTANCE OF INTERNATIONAL COLLABORATION IN CYBER SECURITY

International collaboration is essential for addressing the complex and transnational nature of cyber threats. For Bangladesh, engaging in international partnerships can bring numerous benefits. Collaboration allows for the exchange of knowledge, best practices, and lessons learned from other countries' experiences in cybersecurity. This can help Bangladesh gain insights into emerging threats and attack vectors, learn about effective cybersecurity strategies and frameworks, and access cutting-edge research and technological advancements.

International partnerships can support capacity-building efforts in Bangladesh by providing training and skill development opportunities for cybersecurity professionals, offering technical assistance in implementing cybersecurity measures and supporting the development of cybersecurity curricula in educational institutions. Participating in international threat intelligence sharing networks enables Bangladesh to receive timely information about global cyber threats, contribute to and benefit from collective threat analysis, and enhance its ability to detect and respond to cyber-attacks.

Collaboration can facilitate the alignment of Bangladesh's cybersecurity policies and standards with international best practices, leading to improved interoperability with global cybersecurity systems, enhanced trust and cooperation with international partners, and increased compliance with international cybersecurity norms and regulations. By leveraging international resources and expertise, Bangladesh can optimize its limited cybersecurity resources, avoid duplication of efforts in research and development, and access advanced technologies and tools that may be otherwise unavailable or costly.

Engaging in international cybersecurity collaborations can yield diplomatic and economic advantages for Bangladesh, including strengthened bilateral and multilateral relationships, increased opportunities for participation in global cybersecurity initiatives, enhanced reputation as a responsible actor in the digital domain, and potential for attracting foreign investments in the country's digital economy.

GLOBAL BEST PRACTICES IN CYBERSECURITY

To effectively enhance its cybersecurity posture through international collaboration, Bangladesh can learn from global best practices in this field. Several countries and international organizations have developed successful approaches to cybersecurity that can serve as models for Bangladesh.

Nations worldwide have developed robust strategic frameworks to combat emerging cyber threats. The United States' cybersecurity approach emphasizes four key pillars: citizen protection, economic growth, military strength, and global leadership (White House, 2018). Similarly, Britain's strategic vision from 2016 to 2021 focused on building defensive capabilities while actively discouraging potential cyber adversaries (HM Government, 2016).

The effectiveness of these national initiatives relies heavily on public-private partnerships. For instance, British critical infrastructure benefits from the coordinated efforts between the NCSC and commercial organizations, facilitating crucial threat intelligence sharing (NCSC, n.d.). This collaborative model is also evident in Belgium, where a tripartite alliance between government bodies, industry players, and academic institutions works to enhance national cyber defenses (Cyber Security Coalition, n.d.).

Several international frameworks and initiatives promote cybersecurity collaboration. The Budapest Convention on Cybercrime, the first international treaty addressing internet and computer crime, provides a framework for international cooperation in combating cybercrime (Council of Europe, 2001). The Global Forum on Cyber Expertise (GFCE) serves as a global platform for countries, international organizations, and private companies to exchange best practices and expertise on cyber capacity building (GFCE, n.d.).

Addressing the cybersecurity skills gap is a global priority. Israel's Cybersecurity Education Program integrates cybersecurity education into the national curriculum from an early age (Baram & Lim, 2019). The U.S. National Initiative for Cybersecurity Education (NICE) is a partnership between government, academia, and the private sector to promote cybersecurity education and workforce development (NIST, n.d.).

Specialized intelligence exchange platforms known as ISACs enable industry-specific collaboration on cybersecurity challenges. In the banking sector, the FS-ISAC serves as a worldwide network where financial institutions can exchange security insights and defensive strategies (FS-ISAC, n.d.). To strengthen operational preparedness, organizations conduct frequent cybersecurity drills and simulations. A notable example is the ENISA-led Cyber Europe program, which coordinates large-scale security exercises across European nations to test regional incident response capabilities (ENISA, n.d.).

CHALLENGES IN IMPLEMENTING INTERNATIONAL COLLABORATION FOR BANGLADESH

While international collaboration offers significant benefits for enhancing Bangladesh's cybersecurity, several challenges need to be addressed:

i. Technological Gap

Bangladesh faces a considerable technological gap compared to many developed countries in terms of cybersecurity infrastructure and capabilities. This disparity can hinder effective collaboration and implementation of advanced cybersecurity measures.

Challenges:

- Limited access to state-of-the-art cybersecurity technologies
- Insufficient technological infrastructure to support advanced threat detection and response systems
- Difficulty in integrating legacy systems with modern cybersecurity solutions

ii. Resource Constraints

As a developing country, Bangladesh has limited financial and human resources to allocate to cybersecurity initiatives, which can impact its ability to engage in international collaborations effectively.

Challenges:

- Insufficient budget allocation for cybersecurity programs and international engagements
- Shortage of skilled cybersecurity professionals to participate in and benefit from international collaborations
- Limited capacity to invest in research and development in cybersecurity

iii. Language and Cultural Barriers

Language differences and cultural nuances can pose challenges in effective communication and knowledge transfer during international collaborations.

Challenges:

- Limited English language proficiency among some Bangladeshi cybersecurity professionals
- Cultural differences in approaches to problem-solving and decision-making
- Potential misunderstandings in interpreting and implementing international best practices

iv. Legal and Regulatory Harmonization

Aligning Bangladesh's legal and regulatory framework with international standards and practices can be complex and time-consuming.

Challenges:

- Differences in legal systems and approaches to cybersecurity governance
- Potential conflicts between national sovereignty concerns and international cooperation requirements
- Need for extensive legislative reforms to accommodate international cybersecurity norms

v. Trust and Information Sharing

Building trust with international partners and overcoming reluctance to share sensitive information are crucial challenges in cybersecurity collaboration.

Challenges:

- Concerns about data sovereignty and national security when sharing threat intelligence
- Lack of established trust relationships with potential international partners
- Potential reluctance of some countries to share advanced cybersecurity knowledge with Bangladesh

vi. Geopolitical Considerations

Bangladesh's geopolitical position and relationships with various countries can influence its ability to engage in certain international cybersecurity collaborations.

Challenges:

- Balancing collaborations with different countries and regional blocs
- Navigating potential conflicts of interest among international partners
- Ensuring that cybersecurity collaborations align with Bangladesh's foreign policy objectives

vii. Sustainability of Initiatives

Ensuring the long-term sustainability of international collaboration initiatives can be challenging, particularly when dealing with project-based or time-limited engagements.

Challenges:

- Maintaining momentum and commitment to collaborative efforts over time
- Securing ongoing funding and resources for long-term initiatives
- Retaining knowledge and skills gained through short-term international programs

viii. Domestic Coordination

Effective international collaboration requires strong domestic coordination among various government agencies, private sector entities, and academic institutions.

Challenges:

- Fragmented responsibilities for cybersecurity across different government agencies
- Limited mechanisms for public-private partnerships in cybersecurity
- Insufficient coordination between policymakers and technical experts

Addressing these challenges will be crucial for Bangladesh to maximize the benefits of international collaboration in enhancing its cybersecurity capabilities. Overcoming these obstacles will require a strategic approach, sustained commitment, and the development of tailored solutions that consider Bangladesh's unique context and needs.

RECOMMENDATIONS FOR ENHANCING BANGLADESH'S CYBERSECURITY THROUGH INTERNATIONAL COLLABORATION

Based on the analysis of global best practices, challenges, and opportunities, several recommendations are proposed to enhance Bangladesh's cybersecurity through international collaboration. Bangladesh should develop a comprehensive international cybersecurity collaboration strategy aligned with its national cybersecurity objectives and Digital Bangladesh vision. This strategy should identify priority areas for international collaboration and define clear goals, timelines, and performance indicators.

Strengthening regional cybersecurity cooperation is crucial. Bangladesh should take a leadership role in promoting cybersecurity cooperation within the South Asian Association for Regional Cooperation (SAARC) and engage actively in ASEAN-led cybersecurity initiatives as a dialogue partner. Establishing bilateral cybersecurity partnerships with technologically advanced countries, focusing on knowledge transfer and capacity building, can accelerate Bangladesh's progress in cybersecurity.

Bangladesh should enhance its participation in global cybersecurity initiatives, such as the Global Forum on Cyber Expertise (GFCE) and the Internet Governance Forum (IGF). Contributing to the development of international cybersecurity norms and standards through engagement with the United Nations and other multilateral organizations can raise Bangladesh's profile in the global cybersecurity community.

Establishing a National Cybersecurity Collaboration Hub can facilitate coordination of international cybersecurity collaborations and serve as a focal point for international partners seeking to engage with Bangladesh on cybersecurity matters. Investing in cybersecurity education and workforce development through collaboration with international partners is essential for building a skilled cybersecurity workforce.

Enhancing critical infrastructure protection through international cooperation, including participation in sector-specific international Information Sharing and Analysis Centers (ISACs) and conducting joint cybersecurity assessments, can significantly improve Bangladesh's cyber resilience. Strengthening legal and regulatory frameworks through harmonization with international best practices and engagement in international efforts to combat cybercrime is crucial for creating a robust cybersecurity ecosystem.

Fostering innovation and research collaboration through joint research programs with international universities and participation in global cybersecurity challenges can drive the development of local cybersecurity solutions. Improving cybersecurity incident response capabilities through partnerships with international CERTs and participation in multinational cybersecurity exercises can enhance Bangladesh's ability to handle cyber incidents effectively.

CONCLUSION

The role of international collaboration in enhancing cybersecurity in Bangladesh is both crucial and multifaceted. As the country continues its rapid digital transformation, the need for a robust and resilient cybersecurity ecosystem becomes increasingly apparent. By leveraging global best practices, engaging in strategic partnerships, and actively participating in international cybersecurity initiatives, Bangladesh can accelerate its progress in building strong cyber defences.

The recommendations provided offer a roadmap for Bangladesh to maximize the benefits of international collaboration in cybersecurity. From developing a comprehensive collaboration strategy to investing in education and workforce development, these recommendations address the key areas where international partnerships can have the most significant impact.

Looking to the future, the potential outcomes of enhanced international collaboration in cybersecurity are promising. Bangladesh has the opportunity to not only strengthen its national cyber resilience but also to emerge as a regional leader in cybersecurity. The prospects of a thriving cybersecurity ecosystem, increased innovation, and a more secure digital economy are within reach.

As Bangladesh continues its journey towards becoming a digital nation, international collaboration in cybersecurity will play a pivotal role in ensuring that this transformation is secure, sustainable, and inclusive. By embracing the lessons from global best practices and fostering strong international partnerships, Bangladesh can build a cyber-resilient future that supports its national development goals and contributes to global cybersecurity efforts.

REFERENCES

1. a2i Programme. (2020). Digital Bangladesh Vision 2021. https://a2i.gov.bd/digital-bangladesh-vision-2021/
2. Bangladesh Computer Security Incident Response Team (BGD e-GOV CIRT). (2021). Annual Report 2020. https://www.cirt.gov.bd/
3. Bangladesh Government. (2014). National Cybersecurity Strategy of Bangladesh. https://www.dpp.gov.bd/upload_file/gazettes/14079_75510.pdf
4. Baram, G., & Lim, I. (2019). Israel and Singapore: An evolving cybersecurity partnership. S. Rajaratnam School of International Studies.
5. Council of Europe. (2001). Convention on Cybercrime. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
6. Cyber Security Coalition. (n.d.). About us. https://www.cybersecuritycoalition.be/about-us/
7. Digital Security Agency. (n.d.). About Digital Security Agency. https://dsa.gov.bd/
8. ENISA. (n.d.). Cyber Europe. https://www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme
9. Financial Services Information Sharing and Analysis Center. (n.d.). About FS-ISAC. https://www.fsisac.com/about
10. Global Forum on Cyber Expertise. (n.d.). About GFCE. https://thegfce.org/about-the-gfce/
11. Hasan, M. M., Yajuan, L., & Ullah, N. (2019). Cybersecurity in Bangladesh: Emphasis on Financial Institutions. International Journal of Science and Business, 3(5), 161-171.

12. HM Government. (2016). National Cyber Security Strategy 2016-2021. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf
13. Human Rights Watch. (2020). Bangladesh: Repeal Abusive Law Used in Crackdown on Critics. https://www.hrw.org/news/2020/07/01/bangladesh-repeal-abusive-law-used-crackdown-critics
14. Islam, M. S., & Rahaman, M. (2016). A review on cybercrime and digital forensic awareness in Bangladesh. International Journal of Modern Education and Computer Science, 8(9), 1-8.
15. National Cyber Security Centre. (n.d.). About the NCSC. https://www.ncsc.gov.uk/section/about-ncsc/what-we-do
16. National Institute of Standards and Technology. (n.d.). National Initiative for Cybersecurity Education (NICE). https://www.nist.gov/itl/applied-cybersecurity/nice
17. Rashid, A., Danezis, G., Chivers, H., Lupu, E., Martin, A., Lewis, M., &Peersman, C. (2020). Scoping the Cyber Security Body of Knowledge. IEEE Security & Privacy, 18(3), 12-16.
18. White House. (2018). National Cyber Strategy of the United States of America. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf