Scientific Research Publishing

Beijing Law Review, 2026, 17(1), 158-167
https://www.scirp.org/journal/blr
ISSN Online: 2159-4635
ISSN Print: 2159-4627

Cybersecurity, Public-Private Partnership, and the Protection of Critical Information Infrastructure in Bangladesh: A Comparative Study

Golam Moula[1], Md. Shafikul Alam[2]

[1]Department of Law, Cox's Bazar International University, Cox's Bazar, Bangladesh
[2]Appellate Division, Supreme Court of Bangladesh, Dhaka, Bangladesh
Email: golammoulasuhag@gmail.com, shafiklaw197@gmail.com

How to cite this paper: Moula, G., & Alam, Md. S. (2026). Cybersecurity, Public-Private Partnership, and the Protection of Critical Information Infrastructure in Bangladesh: A Comparative Study. *Beijing Law Review, 17,* 158-167.
https://doi.org/10.4236/blr.2026.171009

Received: January 5, 2026
Accepted: February 27, 2026
Published: March 2, 2026

Abstract

This article explores the importance of public-private partnerships in enhancing cybersecurity for critical information infrastructure in Bangladesh, while also providing a comparative analysis of the experiences of the US, UK, and EU. In 2013, hackers successfully infiltrated the Sonali Bank of Bangladesh, leading to the theft of US$250,000. The cyber theft at Bangladesh Bank in 2016 reaffirmed the pressing need for robust cybersecurity legislation to protect key infrastructure. This incident was not the first of its kind; in the last week of August 2025, a coordinated fraud scheme targeted the credit card holders of Standard Chartered Bank, unlawfully extracting approximately BDT 27 lakh through a series of unauthorized transactions. The proliferation of personal computers, mobile phones, tablets, and digital sensors has significantly improved network connectivity and transformed global operations. However, these advancements have also resulted in an increase in the volume of data generation and storage.

Keywords

Cyber Threat, Cybersecurity, Public-Private Partnership, Critical Information Infrastructure

1. Introduction

Cyber technology has revolutionized communication systems across the world. However, this revolution did not come alone; it brought with it the associated challenges of the cyber age, giving rise to recurring debates about cyber warfare

and cybersecurity. The extent of these challenges is evident from the fact that these terms have become buzzwords in strategic circles over the past few years (Noor, 2014). Modern societies are highly dependent on the continuous functioning of critical infrastructures (CI). These ensure the availability of important goods and services such as energy, communication, or transport. Failures of critical infrastructures have severe repercussions for the economy and the population. Such a failure could even jeopardize the safety and well-being of a country (Brem, 2015). In light of the growing threats to critical infrastructure, it has become increasingly important for nations to ensure the cybersecurity and resilience of the critical infrastructure that people and nations rely on every day (Hashimoto, 2024). Cybersecurity requirements and regulations for critical infrastructure vary by sector, and there are variations in maturity levels across sectors and among companies of different sizes within the same sector (Hashimoto, 2024).

2. Research Methodology

This study adopts a qualitative research design based on secondary data analysis. The research relies exclusively on existing literature to examine, interpret, and synthesize knowledge related to the research topic. A literature-based approach is appropriate because it allows for a comprehensive understanding of theoretical perspectives, empirical findings, and scholarly debates without collecting primary data. Secondary data were collected from academic journal articles, newspaper reporting, reports from recognized institutions and organizations, and reputable online databases (e.g., Google Scholar, JSTOR, Scopus, Web of Science).

3. The Concept of Cybersecurity

Cybersecurity is used to refer to the integrity of our personal privacy online, to the security of our critical infrastructure, to electronic commerce, to military threats, and to the protection of intellectual property. These areas range extremely widely and are united only by the technology with which they engage (Carr, 2016). Cybersecurity is emerging as one of the most challenging aspects of the information age for policymakers and scholars of International Relations (IR). It has implications for national security, the economy, human rights, civil liberties, and international legal frameworks. Although politicians have been aware of the threats of cyber insecurity since the early years of internet technology, anxiety about the difficulties in resolving or addressing them has increased rather than abated. In response, national governments have begun to develop cybersecurity strategies to outline the ways in which they intend to address cyber insecurity (Carr, 2016). The history of cybersecurity as a securitizing concept begins with the disciplines of Computer and Information Science. One, if not the first, usage of cybersecurity was in the Computer Science and Telecommunications Board's (CSTB) report from 1991, Computers at Risk: Safe Computing in the Information Age, which defined "security" as the "protection against unwanted disclosure, modification, or destruction of data in a system and also the safeguarding of systems them-

selves". Security comprised technical as well as human aspects, and "it has significant procedural, administrative, physical facility, and personnel components". Crucially, threats to cybersecurity do not only arise from (usually) intentional agents but also from systemic threats. These systemic threats, defined by Hundley and Anderson as "cyberspace safety", stem from the inherent unpredictability of computers and information systems, which by themselves "create unintended (potentially or actually) dangerous situations for themselves or for the physical and human environments in which they are embedded". Threats arise from software as well as hardware failures and cannot be corrected through perfecting digital technology and programming; in short, there is an inherent ontological insecurity within computer systems (Hansen & Nissenbaum, 2009). In our day-to-day lives, we all rely on data, making purchases in a supermarket, making phone calls, sending emails, ordering goods from an online store, or booking flights and hotels. This data allows the smooth use of all these and many other services. But there is a downside to these benefits too. Our data is a boon for criminals, terrorists, hacktivists, and intelligence agencies worldwide (Gehem, Usanov, Frinking, & Rademaker, 2015).

4. Critical Information Infrastructure of Bangladesh

Critical Information Infrastructure (CII) constitutes the backbone of Bangladesh's technological framework, encompassing sectors vital for national security, economy, and public welfare. This includes telecommunications, energy, transportation, banking, and healthcare systems. In the context of Bangladesh, where digital transformation is rapidly reshaping socio-economic paradigms, the security of CII assumes paramount importance. Any breach or disruption within these crucial systems not only poses immediate risks to public safety and economic stability but also threatens the nation's developmental aspirations. Thus, safeguarding CII is imperative to ensure sustainable growth and resilience in the face of evolving cyber threats (Wahid, 2025).

Elements of Critical Information Infrastructure (CII) in Bangladesh are intricately intertwined with citizen life, so much so that we fail to notice any aspect of these systems until they are actively hampered. For instance, the telecommunications sector, represented by entities like the Bangladesh Telecommunication Regulatory Commission (BTRC), facilitates crucial communication channels for emergency response coordination, law enforcement activities, and dissemination of public safety information during crises. Moreover, the energy sector, embodied by the Bangladesh Power Development Board (BPDB), ensures the uninterrupted supply of electricity, powering essential services such as hospitals, transportation systems, and financial institutions. Additionally, the banking sector, exemplified by the Bangladesh Bank, plays a pivotal role in facilitating secure financial transactions, vital for sustaining economic activities and public confidence. The role of CII is indispensable in sustaining essential services and fortifying Bangladesh's national security framework, which is why safeguarding this infrastructure against

emerging threats like evolving cyber adversities is of paramount importance (Wahid, 2025).

5. Cybersecurity Challenges and the Bangladesh Experience

Bangladesh faces a myriad of cybersecurity challenges stemming from its rapid digitization and evolving threat landscape. One prominent issue is the prevalence of malware and phishing attacks targeting government agencies, businesses, and individual users, leading to data breaches and financial losses. Furthermore, the inadequate degree of cybersecurity infrastructure and skilled workforce exacerbates vulnerabilities, hindering effective threat detection and response mechanisms (Wahid, 2025). One poignant example is the notorious cyber heist targeting the Bangladesh Bank in 2016. Hackers attempted to siphon off nearly $1 billion from the bank's reserve account held at the Federal Reserve Bank of New York, succeeding in absconding with $81 million. This, among several other breaches, not only highlights the immediate ramifications for the concerned establishments but also raises questions about the broader implications of inadequate cybersecurity measures for safeguarding critical infrastructure (Wahid, 2025).

Bangladesh's Response to Cybersecurity Challenges

Despite these challenges, Bangladesh has made essential strides in bolstering cybersecurity measures to safeguard its critical infrastructure. The government has enacted relevant, needed policies such as Bangladesh's Digital Commerce Operation Guideline 2021, which sets out regulations and standards for secure digital transactions and e-commerce operations. Furthermore, the Bangladesh Cyber Security Ordinance, 2025 provides a comprehensive legal framework for addressing cyber threats, ensuring accountability, and protecting digital assets. In alignment with global cybersecurity initiatives, Bangladesh has developed the Bangladesh Cybersecurity Strategy for 2021-2025, outlining strategic objectives and action plans to enhance cyber resilience and mitigate cyber risks. Moreover, Bangladesh's collaboration with international partners extends to aligning its policies with the European Union's Digital Services Act (DSA), fostering interoperability and harmonization of cybersecurity standards. These concerted efforts underscore Bangladesh's commitment to strengthening its cyber resilience and fostering a secure digital ecosystem for its citizens and businesses (Wahid, 2025).

In the Critical Information Infrastructure of the power sector in Bangladesh, where the consistent, reliable, and secure operation of energy grids is essential for sustaining economic activities and public services, cybersecurity is of immense importance. As the backbone of Bangladesh's industrial and commercial sectors, the power sector relies heavily on interconnected digital systems for the generation, transmission, and distribution of electricity, making it a prime target for cyber threats. Identified vulnerabilities within Bangladesh's CII, particularly in the power sector, include outdated legacy systems, inadequate cybersecurity protocols, and a shortage of skilled cybersecurity professionals, leaving critical infra-

structure susceptible to exploitation by malicious actors. Cybersecurity threats in the power sector CII have been observed globally, underscoring the magnitude of potential disruptions and economic repercussions. Notable incidents, such as the 2015 cyberattack on Ukraine's power grid, where hackers remotely disrupted electricity distribution to hundreds of thousands of homes, serve as poignant reminders of the devastating impact cyber threats can have on critical infrastructure. Such incidents highlight the imperative of fortifying cybersecurity measures within the power sector's CII to mitigate risks and ensure the uninterrupted supply of electricity, which is crucial for sustaining economic activities and public services (Wahid, 2025). Past cybersecurity incidents in Bangladesh's CII, notably within the power sector, serve as stark reminders of the vulnerabilities inherent in digital infrastructure. One such case study involves the attack on the Bangladesh Power Development Board (BPDB) in 2015, where hackers breached the board's systems, disrupting electricity distribution across several regions and causing widespread power outages. Another notable incident occurred in 2017 when the ransomware attack known as "WannaCry" infected computers at the Bangladesh Energy Regulatory Commission (BERC), compromising sensitive data and disrupting regulatory operations. These incidents underscore the urgent need for robust cybersecurity measures and investments in the power sector to safeguard critical infrastructure and mitigate potential disruptions to essential services (Wahid, 2025). The underreported CII events in Bangladesh, such as the "DESCO prepaid meter hack", unveil vulnerabilities within critical infrastructure, particularly the power sector. With over 18,000 prepaid electricity meters compromised in Sylhet, the incident not only threatens revenue streams for utility providers but also raises concerns about the reliability of the power grid. The ability for consumers to access electricity despite negative balances showcases the potential for widespread disruptions and financial losses, highlighting the urgent need for robust cybersecurity measures to safeguard critical infrastructure (Wahid, 2025). Responses to underreported CII incidents in Bangladesh have been marked by a lack of transparency and accountability. For instance, the negotiation reports following the ransomware attack on Biman Bangladesh Airlines' email servers underscore the challenges in effectively managing cyber threats. Despite warnings and vulnerabilities identified by government agencies, the airline's failure to implement adequate cybersecurity measures leaves critical infrastructure sectors vulnerable to exploitation by threat actors. This opacity not only undermines public trust but also hampers efforts to address systemic vulnerabilities and prevent future cyber incidents (Wahid, 2025). Indifference to failures arising from underreported Critical Information Infrastructure (CII) in Bangladesh's cybersecurity landscape poses significant risks to national security and public safety. The prevalence of underreported incidents exacerbates vulnerabilities within critical infrastructure sectors, hindering efforts to build resilience against increasing cyber threats. Without transparent reporting mechanisms and accountability measures, critical infrastructure operators may remain unaware of systemic vulnerabilities, leaving

their systems susceptible to exploitation. Moreover, the neglect of underreported CII failures exacerbates challenges in threat intelligence sharing and incident response coordination, further hindering efforts to prioritize investments in cybersecurity capabilities and infrastructure modernization (Wahid, 2025).

6. Cybersecurity Challenges and US Experience in Public-Private Partnership (PPP)

In the US under the Bush administration, a separate office in the White House was established in 2001 to handle its coordination of cybersecurity matters, led by a special adviser for cybersecurity. The US has had many false starts in trying to bring together the various strands of its work on cybersecurity during the 2000s, and it took most of that decade to create the impetus for policymakers to begin to formulate a relatively unified position on the issues. In 2009, President Obama commissioned a 60-day review of cybersecurity, and one of the key recommendations was to establish a permanent position in charge of cybersecurity. This position of cybersecurity coordinator (often referred to as the "cyber czar"), with the rank of special adviser, is part of the White House staff and reports to the Deputy National Security Advisor (Clarke & Knake, 2010). The role was filled by Howard Schmidt until May 2012, when Michael Daniel took over. Although part of the White House national security team, the cyber czar also consults with the President's top economic advisers and has direct access to the President. The cyber czar has a coordinating role involving all of the defense and civilian agencies with a stake in cyber matters, including the Department of Defense, the National Security Agency, the Federal Bureau of Investigation, the State Department, the US Computer Emergency Readiness Team and the Department of Homeland Security. The czar implements policies across all of the organizations involved, which is no easy task. The position doesn't carry any direct budgetary power for these areas, and has been criticized for holding large-scale responsibility but no real authority (Singel, 2010). The coordinator's role isn't confined to the government sector. It also carries responsibilities for liaising with the private sector to help businesses manage security risks. Obama's February 2013 executive order on improving critical infrastructure cybersecurity has been welcomed as a major policy development. It came at a time when the US was struggling to create sufficiently mature information-sharing machinery within its critical infrastructure networks that could increase cyber resilience. The order, which doesn't have the same power as law, did three things. First, it directed federal authorities to improve information sharing on cyber threats with companies that provide vital support to critical infrastructure, even if that data could be classified, and gave them 120 days to do so. Second, it directed government, led by the Director of Homeland Security, to create a flexible, risk-based framework of core practices for cyber, and allowed 240 days for a preliminary version of the framework to be presented to the President. Finally, the order put a high priority on the protection of privacy and civil liberties even as cybersecurity is strengthened (Jennings & Feakin, 2013). The fun-

damental policy framework for critical infrastructure protection is based on NSM-22 (Hashimoto, 2024). This memorandum replaced PPD-21 of 2013, making the first update to the framework in 11 years. The document is also intended to formalize the efforts made by the U.S. government during this period. This includes defining the role and responsibilities of CISA as the national coordinator for critical infrastructure protection, which did not exist at the time, as well as defining the role and responsibilities of the SRMAs. This requires SRMAs to conduct sector-specific risk assessments and develop sector-specific risk management plans every two years. CISA/DHS is required to conduct cross-sector risk assessments based on input from the SRMAs and develop a National Infrastructure Risk Management Plan (NIRMP) every two years. It is assumed that the National Infrastructure Protection Plan (NIPP) 2013, developed under PPD-21, will remain effective until the release of NIRMP, which is due by April 2025. NSM-22 also requires the development of minimum cybersecurity and resilience requirements for critical infrastructure and the implementation of these requirements using regulatory and other authorities. In addition, it requires the government to understand critical infrastructure interdependencies, analyze systemic risk, identify Systemically Important Entities (SIEs) and enhance collaboration with the intelligence community, including the timely sharing of declassified information. In June 2024, DHS released the Strategic Guidance and National Priorities for U.S. Critical Infrastructure Security and Resilience (Hashimoto, 2024). This guidance aligns with NSM-22 and identifies risk areas that the nation should prioritize over the next two years to build secure and resilient critical infrastructure. The priority areas include addressing cyber threats posed by China, managing the evolving risks presented by AI, and identifying and mitigating supply chain vulnerabilities. The document then outlines the priorities for mitigating those risks, including adopting baseline requirements, incentivizing service providers to reduce risk, and identifying SIEs (Hashimoto, 2024). The public–private partnership has been employed widely by states including the US as a mechanism to deal with a range of other issues, including security-related ones. The practice intensified from the 1990s, when the privatization of critical infrastructure was regarded as economically beneficial to the state, freeing up capital and drawing more heavily on the efficiencies and business practices of the private sector (Carr, 2016). The United States has a long history of close PPPs in critical infrastructure protection, with a variety of collaborative initiatives currently in place. JCDC, one of the most notable initiatives in recent years, is a cross-sector, operational collaborative framework composed of key government agencies and selected private-sector companies. This enables members to share and analyze unique threat intelligence and information from both the government and the private sector, as well as jointly develop countermeasures in a timely manner. The initiative was launched in 2021 with the participation of approximately 10 companies, primarily in the IT, communications, and cybersecurity industries. The number of participating companies has since expanded to other sectors, and there are now over 300 members,

including NTT, a major telecommunications carrier in Japan, as the first member in the Asian region. As indicated in the National Cyber Security (NCS), one of the current focuses is to enhance the speed and scale of operations. This would need to include cooperation with major foreign companies to address growing global-scale threats posed by state-sponsored actors. Other sector-based operational co-operation includes the Department of Energy's Energy Threat Analysis Center, the DOD's Defense Industrial Base Collaborative Information Sharing Environment, and the NSA's CCC. The government plans to further strengthen and integrate these individual efforts into a federal cybersecurity center. Another key initiative is the ICT Supply Chain Risk Management (SCRM) Task Force, which was launched in 2018. It is a PPP program that identifies challenges and develops solutions to enhance the resilience of the global ICT supply chain. The group is primarily composed of private companies in the communications and IT sectors, as well as CISA, and works on specific topics such as AI, SMBs, and software, providing guidance and other deliverables to the public (Carr, 2016). Thus it is clear that only cross-sector cooperation and coordination in a pragmatic and ongoing public-private partnership can increase the CI's resilience. In the future, more explicit rules and regulations will be necessary to support this collaboration and particularly clarify current areas of open legal issues. This should be done with a sense of proportion and the overall goal to foster, not to encumber, collaboration across responsibilities and disciplines as well as between public and private actors (Brem, 2015).

7. Cybersecurity and UK Experience

In the "landscape review" of the UK cyber-security strategy, Amyas Morse makes the point that if the internet were a national economy, it would be the fifth largest in the world (Dean, Digrande, Field, Lundmark, O'Day, Pineda, et al., 2012). In addition, he writes, the UK has one of the world's largest online economies, with 8 per cent of GDP generated online—a higher proportion than for any other G20 country. To this end, the UK National Cyber Security Strategy specifically addresses the financial cost to businesses of security breaches. The UK Cyber Security Strategy states that it is the effective functioning of cyberspace that is of vital importance. This introduces some conflation of ideas about cybersecurity, because in addition to being an object to be protected, the internet is also, of course, the source of threats (from what?) and the mechanism through which those threats can be addressed (by what means?). However, it is clear in these strategies that the network itself is a primary referent object for conceptions of security. It is the security of the technology itself, as well as the security of those who use the technology, that concerns the UK government here; and the two forms of security are linked. Citizens, businesses, and government can enjoy the full benefits of a safe, secure, and resilient cyberspace. The technology becomes an artefact to be protected, an asset essential to broader state security (Carr, 2016).

8. Cybersecurity and EU Experience

Protecting the EU's critical infrastructure, spanning both physical and cyber domains, presents a complex challenge, and several initiatives have been undertaken to address these vulnerabilities. The EU's 2020 Cybersecurity Strategy built upon earlier efforts (e.g., the European Programme for Critical Infrastructure Protection [2006] and Directive 2008/113/EC) by addressing cyber threats to critical services and establishing the Joint Cyber Unit to coordinate responses across Member States. In 2022, the Council's Recommendation on Strengthening Critical Infrastructure Resilience promoted a Union-wide approach to enhance coordinated preparedness, response strategies, and international cooperation (Slakaityte & Surwillo, 2024). The 2023 Critical Entities Resilience Directive extended coverage to all critical sectors, mandating national strategies and risk assessments for service continuity. At the same time, legislation like the European Cyber Resilience Act (2022) strengthened cybersecurity amidst evolving threats. While the NIS 2 Directive (2022) concerns 180,000 critical infrastructure organizations, requiring them to implement measures for cybersecurity, including incident handling, business continuity, supply chain security, and encryption, by October 2024. Member States must also establish systematized lists of vital entities by April 2025, to be reviewed at least every two years. Furthermore, international cooperation through exercises like Nordic Pine 2024, involving NATO members from the Nordic-Baltic region, and ENISA's Cyber Europe, a biennial pan-European exercise with public and private sectors, underscores the critical importance of cross-border cybersecurity coordination (Slakaityte & Surwillo, 2024).

9. Recommendation and Conclusion

Running parallel to government policy initiatives, citizen-focused cybersecurity measures and awareness campaigns need to be adopted for a cyber-secure society. The cybersecurity awareness programme may be organized by public-private initiative in order to educate citizens about common cyber threats and the best practices for safeguarding personal information and digital assets. Initiatives like the Cyber-Maitree 2023 programme, engaging collaboration between government agencies, industry stakeholders, and the public to enhance cybersecurity awareness, skills, and resilience at the grassroots level, need to be continued. It is essential for the government to work with stakeholders in Bangladesh to prioritize CII cybersecurity measures, ensuring accountability to secure the resilience and security of critical infrastructure in the face of evolving cyber threats. The Bangladesh government can also establish a National Cyber Security Commission by taking expertise from the IT sector, corporate personnel, and personnel from law enforcement agencies. In many countries, where critical infrastructural systems in areas such as utilities, finance, and transport have been privatized, these policy documents rely heavily upon what is referred to as the "public-private partnership" as a key mechanism to mitigate the threat. In the United States and United Kingdom, the public-private partnership has repeatedly been referred to as the

"cornerstone" or "hub" of cybersecurity strategy. The Bangladesh government can learn a lesson from the USA, UK, and EU practices in this regard.

Acknowledgements

Extremely grateful to Professor Quazi Mostain Billah, Dean, Cox's Bazar International University; Md. Al Amin, Associate Professor, Department of Law, Northern University Bangladesh; and Md. Gajiur Rahman, Assistant Professor, Department of Law, University of Barishal, Bangladesh, for their cordial support and assistance in writing the article.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

Brem, S. (2015). Critical Infrastructure Protection from a National Perspective. *European Journal of Risk Regulation, 6,* 191-199. https://doi.org/10.1017/s1867299x00004499

Carr, M. (2016). Public-Private Partnerships in National Cyber-Security Strategies. *International Affairs, 92,* 43-62. https://doi.org/10.1111/1468-2346.12504

Clarke, R. A., & Knake, R. K. (2010). *Cyber War: The Next Threat to National Security and What to Do about It*. Harper Collins.

Dean, D., Digrande, S., Field, D., Lundmark, A., O'Day, J., Pineda, J. et al. (2012). *The Internet Economy in the G-20: The $4.2 Trillion Growth Opportunity*. Boston Consulting Group.

Gehem, M., Usanov, A., Frinking, E., & Rademaker, M. (2015). *Comparing Cyber Threat Assessments*. Hague Centre for Strategic Studies.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53,* 1155-1175. https://doi.org/10.1111/j.1468-2478.2009.00572.x

Hashimoto, T. (2024). *Operationalizing Japan-U.S. Cooperation on Critical Infrastructure Cybersecurity and Resilience*. Center for Strategic and International Studies (CSIS).

Jennings, P., & Feakin, T. (2013). *The Emerging Agenda for Cybersecurity*. Australian Strategic Policy Institute.

Noor, S. (2014). *Cyber (In)Security, Strategic Studies, Vol. 34, No. 2/3 (Summer and Autumn)*.

Singel, R. (2010). *White House Cyber Czar: "There Is No Cyberwar"*. Wired Magazine.

Slakaityte, V., & Surwillo, I. (2024). *Protecting EU's Critical Infrastructure: The Fight Intensifies in the Cyber Realm*. Danish Institute for International Studies.

Wahid, S. S. (2025). *Cyber Security in Critical Information Structure in Bangladesh*. https://thefinancialexpress.com.bd/