BIPSS Commentary
www.bipss.org.bd September-2025
BIPSS Towards a Secure World

The Digital Divide as a Geopolitical Fault Line: What it means for Bangladesh

Jannatul Toba[1]

Introduction

In the 21st century, digital technologies have emerged as pivotal drivers of global development, fundamentally reshaping economic, educational, healthcare, and social landscapes[2]. Information and Communication Technology (ICT) has become central to fostering innovation, enabling structural transformation, and promoting sustainable growth across diverse sectors[3]. Beyond facilitating efficiency and convenience in societal operations, these technologies play a strategic role in determining global power relations. Access to advanced digital infrastructure, data, and technological expertise increasingly defines national competitiveness, influencing how countries engage in international trade, diplomacy, and security.

For developing countries, digital technologies present a dual reality. On one hand, they offer unprecedented opportunities for rapid socio-economic development, allowing nations to enhance

[1] Jannatul Toba is a Reseach Assistant at Bangladesh Institute of Peace and Security Studies (BIPSS). She completed her BSS and MSS in Development Studies from Bangladesh University of Professionals (BUP).
[2] Jannatul Toba, "Digital Divide in Bangladesh: A Constraint in Achieving SDGs," *DCCI Journal of Business and Economic Policy* 1, no. 1 (2024): https://doi.org/10.63784/djbep2024v1n1a6.
[3] Danica Radovanović, Christine Holst, Sarbani Banerjee Belur, Ritu Srivastava, Georges Vivien Houngbonon, Erwan Le Quentrec, Josephine Miliza, Andrea S. Winkler, and Josef Noll, "Digital Literacy Key Performance Indicators for Sustainable Development," *Social Inclusion* 8, no. 2 (2020): 151–67

education delivery, expand healthcare access, improve governance, and stimulate entrepreneurship. On the other hand, limited technological infrastructure, uneven access, and low levels of digital literacy make these countries vulnerable to geopolitical and economic marginalization. The resulting digital divide—characterized by unequal access to technology, knowledge, and digital services—reinforces pre-existing social and economic inequalities. It constrains human capital development, limits participation in the global knowledge economy, and reduces the ability of nations to shape international norms around technology and cybersecurity. In this context, bridging the digital divide is not merely a domestic development issue but a matter of strategic significance, as it directly impacts a country's ability to compete, innovate, and assert influence on the global stage.

Defining Digital Divide

The concept of the digital divide can be understood from multiple perspectives, often shaped by the focus of specific research. Some studies conceptualize it as the gap between those who possess information and those who do not, while others approach it from an economic perspective, distinguishing between the information-rich and information-poor[4]. Webster (2014) argues that such a dichotomous framing oversimplifies the complexities inherent in the digital divide. Socio-economic background, geographic disparities, and structural inequalities are key factors contributing to this divide[5].

The Organization for Economic Co-operation and Development (OECD) provides one of the most comprehensive definitions. According to OECD (2001), the digital divide refers to disparities in access to and use of digital technologies—particularly internet access—across different socio-economic, geographic, and demographic groups[6]. This divide can be examined through two dimensions: access to digital devices, internet, and services, and digital literacy[7]. Even with

[4] William Wresch, *Disconnected: Haves and Have-Nots in the Information Age* (New Brunswick, NJ: Rutgers University Press, 1996).
[5] Frank Webster, *Theories of the Information Society* (Abingdon, UK: Routledge, 2014).
[6] OECD, *Understanding the Digital Divide,* OECD Digital Economy Papers (Paris: OECD, 2001), https://doi.org/10.1787/236405667766
[7] Clifford Sparks, "What Is the 'Digital Divide' and Why Is It Important?" *Javnost—The Public* 20, no. 2 (2013): 27–46.

physical access to technology, a lack of digital literacy may prevent effective utilization of digital services, making digital literacy as critical as access itself.

From a geopolitical lens, the digital divide is not merely a domestic socio-economic issue but a strategic factor shaping global power dynamics. Countries with limited access to digital technologies face constraints in innovation, economic competitiveness, and participation in global knowledge networks. Vulnerable populations within these nations, due to gender, socio-economic status, or geographic location, often bear the brunt of this divide[8]. Disparities in digital literacy and skills further amplify inequalities, affecting a country's capacity to leverage technology for development, secure digital sovereignty, and strengthen its influence in international affairs.

The Digital Divide as a Global Geopolitical Fault Line

The geopolitical digital divide is characterized by a stark asymmetry of power, where a handful of technologically advanced nations and their dominant multinational corporations form the digital core, exerting control over the critical layers of cyberspace—from submarine cables and 5G infrastructure to cloud computing and data flows. Developing states, constituting the digital periphery, are relegated to positions of technological dependency, exposed to risks that transcend mere economic disparity.

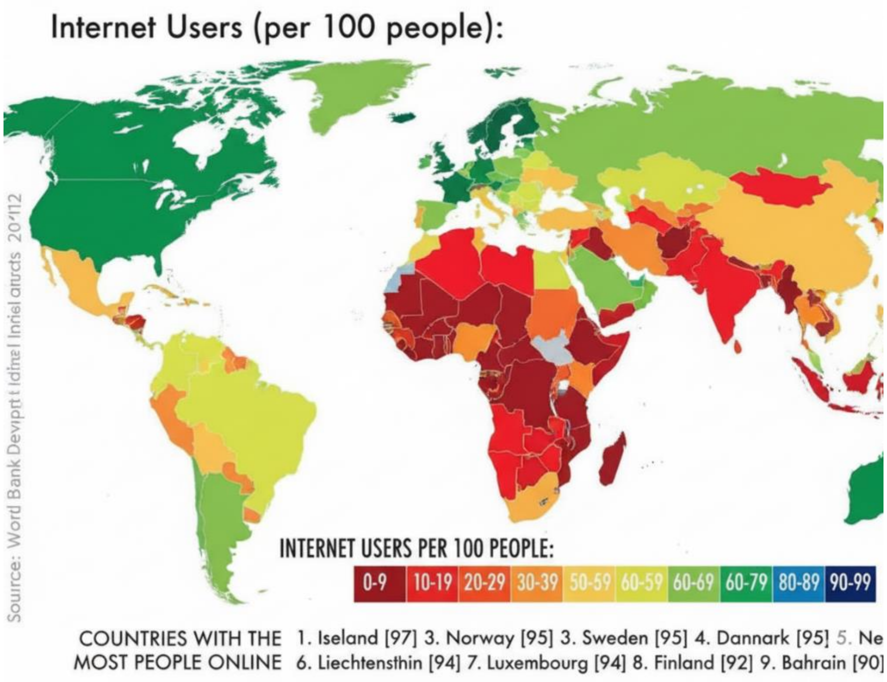
Power Asymmetry and Cyber Security

The most acute manifestation of this fault line lies in international security and cyber power. The digital divide is fundamentally a cyber-security issue for developing countries. Nations with low digital literacy, limited infrastructure, and weak regulatory frameworks are less capable of defending their critical national infrastructure (CNI) against sophisticated state and non-state threat actors. The cost of cyberattacks globally reached trillions of dollars in 2020, and for developing countries, poor cyber hygiene and a lack of skilled personnel perpetuate vulnerability[9].

[8] Nir Kshetri, "Diffusion and Effects of Cyber-Crime in Developing Economies," *Third World Quarterly* 31, no. 7 (2010): 1057–79.

[9] Ellada Gamreklidze, "Cyber Security in Developing Countries, a Digital Divide Issue: The Case of Georgia," *The Journal of International Communication* 20, no. 2 (2014): 200–17.

This deficit in defensive capabilities translates directly into diminished strategic political standing. The ability to exercise effective digital sovereignty—the capacity for a nation to control its own digital destiny, including its data, hardware, and software—is concentrated within the core.


Internet Users (per 100 people):
Source: Word Bank Deviptt idme l Inriel arurds 20'l12
INTERNET USERS PER 100 PEOPLE:
0-9
10-19
20-29
30-39
50-59
60-59
60-69
60-79
80-89
90-99
COUNTRIES WITH THE MOST PEOPLE ONLINE
1. Iseland [97] 3. Norway [95] 3. Sweden [95] 4. Dannark [95] 5. Ne
6. Liechtensthin [94] 7. Luxembourg [94] 8. Finland [92] 9. Bahrain [90]

Source: World Bank Indicators

Fragmentation and Dependency

Technological development has become a key tool for nations to gain power and influence. Countries invest in technology to maintain leadership in geopolitical and geoeconomic arenas, facing complex challenges in managing strategic advantages, threats, and opportunities[10]. These challenges affect both great powers like the US, China, India, and Russia, and middle powers such as Australia, which must balance competitiveness with social, economic, and ethical concerns.

The geopolitical fault line is further intensified by the growing trend of Internet fragmentation, which poses a threat to the cohesion and security of global cyberspace. Countries are increasingly forced to align with competing technological standards and ecosystems, limiting interoperability

[10] Glenn Diesen, *Great Power Politics in the Fourth Industrial Revolution* (2021): 1–272.

and increasing reliance on dominant digital powers. This dependency can constrain national autonomy in digital governance, reduce access to cutting-edge technologies, and create structural imbalances in global digital influence.

Technological Neo-Colonialism and the AI Revolution

Technological neo-colonialism has emerged as a defining feature of the digital age, particularly as internet fragmentation and the AI revolution reshape global power relations[11]. Internet fragmentation—driven by technical issues such as routing failures and gaps in IPv6 adoption, alongside geopolitical interventions like state-imposed firewalls and data localization mandates—compels nations to align with competing digital standards, increasing their dependence on Global North powers[12]. This dependency is further entrenched by the AI revolution, where the Global South often becomes a testing ground for new technologies, while corporations and states in the Global North extract data, talent, and resources, leaving developing countries technologically and economically reliant on external actors[13]. Illustrative cases, such as the Cambridge Analytica operations in Kenya and Nigeria, highlight the political and social risks posed by such extractive practices[14]. Scholars identify three key dimensions of this technological neo-colonialism. First, data exploitation, or "data colonialism," occurs as Global South countries supply vast datasets but receive little benefit, often facing heightened privacy concerns andalgorithmic biases in return. Second, control over AI infrastructure remains concentrated in the Global North, where advanced computational power, platforms, and research ecosystems are monopolized, restricting the capacity of developing nations to independently innovate or shape global technological norms[15]. Third, talent migration contributes to a "colonial supply chain of AI," as skilled labor flows toward the Global North, depriving the Global South of its human capital and excluding it from broader economic benefits. Together, these dynamics deepen existing inequalities in digital infrastructure,

[11] Jerry John Kponyo, Dickson Marfo Fosu, Frederica Efia Birago Owusu, Musah Ibrahim Ali, and Maxwell Mawube Ahiamadzor, "Techno-Neocolonialism: An Emerging Risk in the Artificial Intelligence Revolution," *Trayectorias Humanas Trascontinentales* 18 (2024).

[12] Abeba Birhane, "Algorithmic Colonization of Africa," *SCRIPTed* 17 (2020): 389

[13] James Muldoon and Boxi A. Wu, "Artificial Intelligence in the Colonial Matrix of Power," *Philosophy & Technology* 36, no. 4 (2023): 80

[14] Danielle Coleman, "Digital Colonialism: The 21st Century Scramble for Africa through the Extraction and Control of User Data and the Limitations of Data Protection Laws," *Michigan Journal of Race & Law* 24 (2018): 417.

[15] Tyler Stevenson, "Navigating Digital Neocolonialism in Africa," *Digital Policy Hub*, Centre for International Governance Innovation (CIGI), 2024.

AI readiness, and internet access, reinforcing asymmetric dependencies between the Global North and South and perpetuating a new form of technological domination.

Source: Substack

The Internal Fault Lines of “Digital Bangladesh”

Before Bangladesh can navigate the external geopolitical digital divide, it must first address its profound internal digital gaps, which constrain its aspiration to become a knowledge-based, digitally inclusive economy by 2041. These internal disparities exist across multiple dimensions. At the first level, access remains uneven: while urban areas have benefited from the "Digital Bangladesh" initiative, rural communities lag significantly in internet penetration, hardware availability, and bandwidth, reflecting historical challenges faced by LDCs (e.g., only 5% of households in LDCs had internet in 2015). As of 2022, only 45% of Bangladesh’s population had internet access, with rural connectivity at 29.7% versus 63.4% in urban areas[16], and just 37.3% of

[16] Bangladesh Bureau of Statistics (BBS) and United Nations Children’s Fund (UNICEF), *National Survey of Children’s Education Bangladesh 2021: Key Findings Report* (Dhaka: BBS & UNICEF, 2022)

women online[17]. At the second level, inequalities in digital skills and effective usage prevent citizens from fully leveraging e-governance, remote work, and educational resources, thereby constraining progress toward SDG 4 (Quality Education) and SDG 8 (Decent Work and Economic Growth)[18] [19]. Gender and socioeconomic disparities further exacerbate this divide: women and low-income populations remain disproportionately affected despite some improvements in female internet use. During the COVID-19 pandemic, only 18.7% of students could access remote learning due to lack of devices or connectivity. This combination of access limitations and skill gaps weakens Bangladesh's digital foundation, slowing the adoption of advanced technologies such as 5G and increasing dependence on foreign expertise and platforms, ultimately impeding the country's ability to participate as an equal player in the global digital economy.

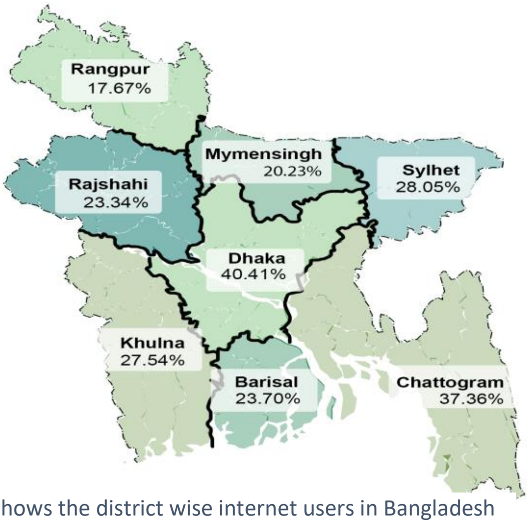


Figure 1: The figure shows the district wise internet users in Bangladesh

[17] World Bank, *World Development Indicator*, "Individuals Using the Internet, Female (% of Female Population) – Bangladesh," 2023, https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BD.

[18] Eszter Hargittai and Amanda Hinnant, "Digital Inequality: Differences in Young Adults' Use of the Internet," *Communication Research* 35, no. 5 (2008): 602–21.

[19] Muhammad Shahadat Hossain Siddiquee and Md Saiful Islam, "Understanding the First and Second Digital Divides in Rural Bangladesh" (2020).

Navigating the Geopolitical Crosscurrents

Bangladesh's position at the intersection of its internal digital deficiencies and the global geopolitical fault line forces a strategic balancing act in its foreign and domestic policy.

Cybersecurity and National Security

Bangladesh experiences around 630 cyberattacks daily, disproportionately targeting banks, NBFIs, and MFS services, with many attacks originating abroad (24% from China, 13% from North Korea, 12% from Russia, and 7% each from the US and Pakistan). These attacks often exploit weak digital infrastructures and limited preparedness. Additionally, data storage of vital records such as NIDs, passports, and driving licenses has been compromised by hackers, while private institutions remain particularly exposed due to weak safeguards and unregulated data-sharing practices. The Cybercrime Awareness Foundation (CAF) highlights that 75% of victims are aged 18–30, with cyber-bullying alone accounting for over half of reported crimes, signaling the severe social consequences of weak digital literacy. Moreover, the spread of misinformation, phishing scams, crypto-financing of extremist networks, and the use of AI-generated deep fakes further expand the threat landscape[20].

Inadequate cybersecurity infrastructure, low digital literacy, and fragmented internet governance make the country particularly susceptible to cyber warfare, disinformation campaigns, and critical infrastructure attacks—threats that are linked to geopolitical instability[21]. In a global environment where hybrid warfare is increasingly common, Bangladesh's digital weakness is not only a technological issue but a direct national security liability. A poignant local example is the July 2024 student uprising, where a critical lack of digital literacy allowed disinformation and misinformation to spread rapidly through social media and messaging platforms. This orchestrated campaign successfully fabricated and amplified anti-India sentiments, severely straining diplomatic relations and damaging the long-standing people-to-people connections between the two nations. This incident indicates how digital illiteracy can be exploited to manipulate public

[20] Lieutenant Colonel Saifullah Siddiqui, "Cyber Security in Bangladesh: Existing Threats and the Way Forward," *The South Asian Times*, February 24, 2024.

[21] Vladimer Svanadze, Maksim Iavich, and Viktoriia Lukashenko, "Geopolitical and Technical Dimensions of Internet Fragmentation," in *CEUR Workshop Proceedings*, vol. 3991 (2025).

opinion, destabilize social harmony, and directly impact foreign policy, turning the domestic information space into a frontline for geopolitical proxy conflict.

Digital Sovereignty and Dependency

The greatest geopolitical meaning of the digital fault line for Bangladesh is the challenge of data and technological sovereignty amidst the rivalry between global tech giants. Like many nations in Southeast Asia, Bangladesh is highly reliant on foreign technology, cloud services, and digital platforms a situation that leads to the extraction of valuable data by foreign entities and risks national security through unprecedented surveillance capabilities.

To mitigate this dependency, Bangladesh has recently taken initiatives to strengthen its digital capacity, including expanding cooperation with the EU under the Global Gateway strategy on cybersecurity and digital economy goals, as well as exploring diverse partnerships for 5G and cloud services[22]. However, these steps remain insufficient.

Source: Global Finance Magazine

[22] BSS, “EU, BTRC Discuss Cybersecurity, Digital Economy,” *Bangladesh Sangbad Sangstha*, August 20, 2025

Economic Vulnerability

Digital literacy and infrastructure are prerequisites for participation in the global digital economy. Without them, countries risk becoming consumers rather than creators of technology, deepening dependency on foreign tech giants and more digitally advanced nations.

Digital skills are essential for achieving SDG 8 (decent work and economic growth). Bangladesh's growing freelancing sector—ranked second globally—generates over $100 million annually[23]. However, without inclusive digital upskilling, this potential remains untapped for many, especially in rural areas. The digital economy is increasingly dominated by a few tech monopolies. Without strong public-private partnerships and local innovation ecosystems, Bangladesh may struggle to retain economic sovereignty in the digital age.

Way Forward

For Bangladesh, the digital divide is no longer merely a developmental gap; it is the frontline of its 21st-century sovereignty**.** Bridging the digital divide and navigating the evolving geopolitical digital landscape requires Bangladesh to pursue a multidimensional strategy. At the domestic level, urgent investment in digital literacy, inclusive connectivity, and resilient cyber infrastructure is essential to ensure that citizens across rural and urban areas, as well as across gender and socio-economic groups, can equally benefit from digital transformation. At the policy level, Bangladesh must strike a balance between robust cyber security frameworks and the protection of fundamental rights, creating a trusted and innovation-friendly digital environment.

Externally, diversifying technological partnerships and reducing overreliance on single foreign providers will be key to strengthening digital sovereignty. By embracing a "strategic autonomy" approach, Bangladesh can leverage cooperation with multiple partners—regional, global, and private sector actors—while safeguarding its data and critical infrastructure.

Finally, long-term resilience will depend on nurturing a strong domestic innovation ecosystem that promotes local startups, encourages research in AI and emerging technologies, and incentivizes

[23] Jannatul Toba, "Digital Divide in Bangladesh: A Constraint in Achieving SDGs," *DCCI Journal of Business and Economic Policy* 1, no. 1 (2024): https://doi.org/10.63784/djbep2024v1n1a6.

public-private collaboration. Only through this holistic approach—balancing inclusion, security, sovereignty, and innovation—can Bangladesh position itself as a digitally empowered nation capable of competing, cooperating, and shaping its own digital destiny in the 21st century.