Chapter-11
Cybersecurity and Emerging Security Challenges: A SAARC Perspective on Regional Cooperation

Pradeep Kumar Patel[1], Anita Patel[2]
[1]Assistant Professor Sociology
Government Naveen College Saragaon Janjgir Champa Chhattisgarh
[2]Assistant Professor Sociology
Naveen Government College Kusmura Raigarh Chhattisgarh
Email- ppradeep730@gmail.com

Abstract

Cybersecurity has emerged as one of the most important non-traditional security challenges in contemporary international relations, particularly in regions undergoing rapid digitization such as South Asia. SAARC nations have expanded digital systems in governance, banking, healthcare, education, communication and trade. While this transformation has strengthened service delivery and connectivity, it has also introduced vulnerabilities such as cybercrime, ransomware, data breaches, cyber espionage, critical infrastructure attacks, and information warfare. Unlike conventional threats, cyber threats are borderless, instantaneous and often anonymous, enabling hostile actors to disrupt national security without crossing physical borders.In SAARC countries, cybersecurity risks are intensified due to unequal technological capacities, weak legal frameworks, limited institutional coordination, shortage of trained cyber professionals, and gaps in public awareness. The emergence of Artificial Intelligence (AI), Internet of Things (IoT), cloud computing, digital payment infrastructure and 5G networks further increases vulnerability by expanding the "attack surface" available to malicious actors. Additionally, the region's geopolitical tensions and trust deficit between some member states reduce possibilities of intelligence sharing and joint cybercrime investigation. Consequently, cyber threats not only harm national security but also weaken regional trust and cooperation—two essential requirements for SAARC's success.

This chapter examines cybersecurity and emerging security challenges in the SAARC context from an international relations perspective. It highlights key threat categories, governance gaps and cyber diplomacy needs. The chapter argues that SAARC requires a cooperative cyber-security framework involving regional CERT coordination, cyber law harmonization, joint response mechanisms, critical infrastructure protection and digital literacy programs. A secure digital South Asia can become a foundation for regional integration, economic stability and confidence building. Cyber cooperation may also provide SAARC a neutral platform for collaboration beyond traditional political disputes.

Keywords: Cybersecurity, SAARC, emerging security challenges, cybercrime, cyberterrorism, cyber diplomacy, information warfare, critical infrastructure security

Introduction

The concept of security in international relations has significantly changed in the 21st century. Earlier, security was largely interpreted through military threats, territorial disputes, and traditional warfare. In South Asia, security discourse historically

focused on cross-border conflicts, terrorism, insurgency and political instability. However, globalization and digitization have created new domains of insecurity. Today, cyber threats represent one of the most serious and rapidly evolving forms of non-traditional security threats. These threats operate beyond conventional geographical boundaries and can destabilize states by targeting digital infrastructure, citizen data, financial systems and strategic communication networks.SAARC countries are simultaneously experiencing development opportunities and security vulnerabilities created by digitization. E-governance initiatives have expanded access to services; mobile banking and fintech platforms have strengthened financial inclusion; online education and digital media have transformed social interaction. Yet, all these systems rely on digital networks that can be attacked. Cybercrime rates in South Asia have increased, with rising incidents of online fraud, identity theft, phishing scams, and malicious hacking. Ransomware attacks have targeted institutions, causing financial losses and disrupting essential services. Similarly, state-sponsored cyber espionage and strategic cyber operations are increasingly shaping security relations in the region.

Cybersecurity is also closely linked to sovereignty. Data is now a strategic asset, and control over data flows influences power relations. Many SAARC nations have limited cyber infrastructure protection and uneven institutional strength. Some countries have advanced national CERTs and cyber policies, while others still lack robust emergency response frameworks. Another challenge is that cyber threats often require cross-border investigation and cooperation. Yet, the SAARC region has limited cyber collaboration due to political mistrust and institutional stagnation.

Therefore, cybersecurity in SAARC nations must be understood not only in technical terms but also as a major international relations issue involving diplomacy, trust-building, strategic stability, and regional cooperation. This chapter presents a structured analysis of cybersecurity threats and emerging security challenges in SAARC, emphasizing why regional cyber cooperation is essential for peace and sustainable development.

Cyber Threats as Emerging Non-Traditional Security Challenges in Saarc

Cyber threats represent a new class of security challenges that differ fundamentally from traditional threats. In conventional warfare, the attacker is often identifiable, conflict occurs in a defined space, and military forces respond. In cyber conflict, attackers remain anonymous, operations occur remotely, and the targets can be civilians, institutions, and infrastructure. Cybersecurity threats in SAARC are therefore not isolated technical incidents; they are systemic security challenges.

The first major dimension is **cybercrime**. Across SAARC nations, the growth of internet access and smartphone use has expanded cyber victimization. Phishing, online banking fraud, SIM swapping, identity theft, and fake e-commerce scams are increasing. These crimes harm citizens directly and reduce trust in digital systems, weakening digital economies. Financial inclusion projects become insecure when citizens fear digital theft.

Second, **ransomware** has become a high-impact threat. Ransomware attacks encrypt data and demand payment. Hospitals, universities, and local governments are particularly vulnerable because they often have weak cybersecurity. When hospitals are attacked, the

damage becomes a human security issue. When universities are attacked, research data is destroyed. This shows that cyber threats can harm development goals.Third, **cyber terrorism** and extremist activity in cyberspace are emerging concerns. Terror groups use social media and encrypted communication for recruitment, propaganda, fundraising, and radicalization. Cyber terrorism may also include attacks on critical infrastructure, causing panic. SAARC nations already face terrorism-related challenges; digital terrorism strengthens extremist networks and complicates counter-terror operations.

Fourth, cyber threats are creating **social instability** through misinformation. Fake news and manipulated content can fuel communal tensions, trigger riots, and influence elections. Deepfakes and AI-generated misinformation make this threat far stronger. South Asia's cultural diversity and political polarization increase the impact of information warfare.Thus, cybersecurity in SAARC must be treated as a major security concern connected to human security, economic stability, and political order. It requires urgent policy intervention and regional coordination.

Geopolitics, Cyber Espionage, and Trust Deficit In South Asia

In international relations, security is deeply shaped by power competition, strategic mistrust, and diplomatic conflicts. South Asia is a region where political tensions have historically been high. These tensions influence cyber policies and cyber cooperation. Cybersecurity becomes part of geopolitical rivalry in multiple ways.The most significant issue is **cyber espionage**. Cyber espionage refers to clandestine operations to steal sensitive information from governments, military institutions, research labs, and strategic industries. It is cheaper than conventional spying and can be carried out without physical presence. In SAARC region, where security competition exists, cyber espionage increases suspicion and diplomatic tensions. It also weakens the possibility of collaborative frameworks because states hesitate to share cyber intelligence.

Another serious issue is **state-sponsored or state-supported cyber operations**. Many cyberattacks worldwide are allegedly linked to state or proxy actors. In SAARC context, when countries suspect each other, cyber incidents escalate into political disputes. Attribution is difficult; thus, accusations may be politically motivated, and cyber incidents may become propaganda tools. This damages trust.Cybersecurity also intersects with **border and terror narratives**. When cyberattacks target defense systems or strategic institutions, they are interpreted as national security assaults. When misinformation spreads during political crises or elections, it may be interpreted as foreign interference. Therefore, cyber threats intensify traditional security dilemmas.

Trust deficit remains the biggest obstacle. SAARC nations lack a functioning collective security framework. Even if a cyber threat impacts the entire region, countries respond individually. Without trust, cross-border digital investigation becomes impossible. Cybercriminals exploit this institutional weakness.Hence, cybersecurity cooperation in SAARC requires cyber diplomacy and confidence-building mechanisms. Cyber dialogue must be separated from traditional disputes and framed as a mutual security requirement. Without reducing mistrust, cybersecurity cooperation cannot evolve.

Critical Infrastructure Vulnerability and National Security Risks

Cybersecurity threats become highly dangerous when they target critical infrastructure. Critical infrastructure includes power grids, water supply systems, railways, airports, telecom networks, banking systems, and national identity databases. These systems are essential for state functioning. Attacks on these systems can disrupt daily life, weaken governance, and create chaos.SAARC nations are modernizing infrastructure through smart technologies. Smart grids, digital ticketing, e-payment, GPS-based transport systems and cloud-based government databases are expanding. However, modernization often focuses on efficiency rather than security. In many cases, institutions lack security audits, cyber drills, and incident response capacity. Legacy systems are connected to new networks without proper safeguards, making them vulnerable.

Critical infrastructure attacks can lead to **economic shocks**. If banking systems are compromised, markets panic. If ports and trade systems are disrupted, supply chains break. For SAARC nations, where economies are developing and inflationary pressures exist, such attacks can create serious instability. Tourism-dependent nations like Maldives and Sri Lanka can suffer reputational damage if their digital security collapses.

Critical infrastructure attacks can also create **national security emergencies**. If defense communication networks are targeted or satellite systems are interfered with, military preparedness is affected. Cyberattacks can disrupt border surveillance or intelligence networks. This means cyber threats can indirectly affect traditional security and defense.

Therefore, SAARC nations must prioritize critical infrastructure protection by implementing cyber standards, security protocols, encryption, redundancy systems and regular cyber drills. At a regional level, SAARC cooperation could focus on sharing best practices for protecting critical infrastructure, establishing emergency response communication channels, and building regional incident response networks.

Emerging Technologies, Digital Economy, and the Future of Saarc Cyber Cooperation

Emerging technologies are reshaping cyber threats and opportunities simultaneously. Artificial Intelligence (AI), IoT, cloud computing, blockchain, 5G networks and big data analytics offer solutions for governance and economic growth, but they also introduce new security risks.AI is being used for both defense and attack. Cyber attackers can use AI to automate phishing campaigns, generate malware, and create deepfakes. Deepfakes can be used to spread fake speeches of political leaders, trigger panic, and disturb elections. AI-driven misinformation becomes extremely difficult to detect quickly. For SAARC nations with high social media use and limited digital literacy, this threat is very serious.IoT expansion increases vulnerability because smart devices often lack strong security features. Smart city initiatives, surveillance cameras, home devices, smart meters, and connected industrial machines can be hacked. A small device can become an entry point for attackers into larger networks. The more digitized a society becomes, the higher the vulnerability.

Cloud computing introduces sovereignty issues. Many SAARC countries depend on foreign cloud service providers. Data storage in foreign servers creates privacy concerns, national security concerns, and jurisdictional challenges. Cyberattack on cloud systems can affect multiple institutions simultaneously. Cross-border data sharing laws are often unclear in SAARC nations, which complicates cybercrime investigation.On the positive side, these technologies also provide opportunities. SAARC nations can develop cooperative digital security frameworks. For instance, a **SAARC CERT network** could enable sharing of cyber threat intelligence and rapid alert mechanisms. SAARC can create regional training centers, joint cyber drills, and collaborative cybersecurity research. Cyber diplomacy can allow South Asia to develop shared norms for responsible state behavior in cyberspace.To strengthen cooperation, SAARC can focus on neutral practical areas such as cybercrime prevention, child online safety, ransomware response, and protection of financial systems. Because these issues affect every country, they can serve as trust-building platforms. In long-term, cybersecurity can become a foundation for regional integration and economic cooperation.

Conclusion

Cybersecurity and emerging security challenges have become central to contemporary international relations and regional cooperation, particularly in digitally transforming regions such as South Asia. SAARC nations are expanding their digital ecosystems for governance, banking, education, healthcare, communication and trade. This transformation improves connectivity and development but also exposes states and societies to new vulnerabilities. Cybercrime, ransomware, digital fraud, misinformation warfare, cyber terrorism and cyber espionage are now among the most serious threats facing South Asian nations. These threats are unique because they are borderless, rapid, anonymous and capable of causing large-scale disruption without conventional military conflict.

The SAARC region faces specific cybersecurity difficulties including unequal cyber capabilities, low digital literacy, legal gaps, weak institutional coordination and geopolitical mistrust. These factors prevent the formation of an effective regional cyber-security system. Yet, cyber threats cannot be effectively managed through isolated national approaches. Cybercriminal networks operate across borders, and attacks frequently involve foreign servers, cross-border data flows and international financing routes. This requires cooperation in legal frameworks, intelligence sharing and technical incident response.

This chapter argues that cybersecurity cooperation can become one of the most important trust-building mechanisms in SAARC. A SAARC-wide cybersecurity framework should include regional CERT collaboration, joint cyber drills, harmonized cyber laws, rapid incident response protocols, capacity-building programs and public awareness campaigns. Cyber diplomacy should be promoted to reduce mistrust and establish norms of responsible behavior in cyberspace. As cyber threats grow with emerging technologies like AI and IoT, SAARC nations must shift from reactive policies to preventive and collaborative cyber governance. A cyber-secure SAARC region will

not only protect national security and economic stability but will also strengthen regional integration and cooperative development in South Asia.

References

1. Arquilla, J., & Ronfeldt, D. (2001). Networks and netwars: The future of terror, crime, and militancy. RAND Corporation.
2. Betz, D. J., & Stevens, T. (2013). Cyberspace and the state: Toward a strategy for cyber-power. Routledge.
3. Buzan, B., Wæver, O., & de Wilde, J. (1998). Security: A new framework for analysis. Lynne Rienner.
4. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62.
5. Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). Council of Europe Treaty Series No. 185.
6. Deibert, R. (2019). Reset: Reclaiming the internet for civil society. House of Anansi Press.
7. Dunn Cavelty, M. (2008). Cyber-security and threat politics: US efforts to secure the information age. Routledge.
8. European Union Agency for Cybersecurity (ENISA). (2023). ENISA threat landscape report. ENISA.
9. Glaser, C. L. (1997). The security dilemma revisited. World Politics, 50(1), 171–201.
10. International Telecommunication Union. (2024). Global Cybersecurity Index 2024. ITU.
11. Kello, L. (2013). The meaning of the cyber revolution. International Security, 38(2), 7–40.
12. Kissinger, H. (2014). World order. Penguin.
13. Libicki, M. C. (2009). Cyberdeterrence and cyberwar. RAND Corporation.
14. Nye, J. S. (2010). Cyber power. Belfer Center for Science and International Affairs, Harvard Kennedy School.
15. Rid, T. (2013). Cyber war will not take place. Oxford University Press.
16. SAARC Secretariat. (n.d.). Areas of cooperation: Cyber security. SAARC Secretariat.
17. SAARC. (1987). SAARC Regional Convention on Suppression of Terrorism. United Nations Treaty Collection.
18. SAARC. (2004). Additional Protocol to the SAARC Regional Convention on Suppression of Terrorism. Refworld.
19. Singer, P. W., & Friedman, A. (2014). Cybersecurity and cyberwar: What everyone needs to know. Oxford University Press.
20. Slaughter, A.-M. (2004). A new world order. Princeton University Press.
21. South Asian Futures Fellowship. (2025). Cybersecurity cooperation in South Asia: Measures that can work in a geopolitically fraught region. South Asian Futures Fellowship.
22. UNODC. (2013). Comprehensive study on cybercrime. United Nations Office on Drugs and Crime.

23. World Economic Forum. (2023). Global cybersecurity outlook 2023. World Economic Forum.
24. Zittrain, J. (2008). The future of the internet and how to stop it. Yale University Press.
25. CERT-In. (2024). CERT-In and Mastercard India sign MoU for collaboration in cybersecurity. Press Information Bureau, Government of India.