# Analysis of Cyber Security Challenges in Developing Countries

**Mohammad Salem Hamidi[1], Baldev Singh[2]**

*[1]PhD Scholar, Faculty of Engineering and Technology, Department of Computer Science, VGU-Jaipur, India, sshamidi13@gmail.com*
*[2]Faculty of Engineering and Technology VGU-Jaipur, India, baldev_singh@vgu.ac.in*

The interconnection of socioeconomic cleavages, the widespread use of computers and other sophisticated gadgets and equipment, and the melting of geographical barriers have all contributed to the world's shrinking size and the consequent shrinking distance between individuals. "Netizens," a newly invented term for individuals who live on the internet, now number in the millions throughout the globe. Internet and information technology usage has undeniably become a critical strategic issue. The significance of cyberspace to national development has led several nations to allocate substantial funds towards cyberspace applications. Cybersecurity is only one of many potential issues that Afghanistan may encounter as it works to integrate information and communication technologies into its key information infrastructure, according to government papers. Afghanistan needs an all-encompassing cyber security infrastructure and plan because of the many dangers and threats that might compromise cyberspace.
Cybersecurity in Afghanistan, along with all the difficulties and obstacles that come with it, is the subject of this critical article.
The reason for this paper is to offer a more designated investigation and foundation for this work by conducting a qualitative literature review of pertinent studies in this area and related literatures; to gain a deep comprehension of Cyber Security concepts and the associated challenges and threats; and to conclude with a conclusion.

**Keywords:** Cyber security threats, Cyber security challenges, Afghanistan ICT.

## 1. Introduction

The report is organized into three main sections to make it easier to understand. The first section covers the current state of internet penetration and the increased user base in Afghanistan.

Second part shall highlight the threats to cyber security and the third part is the thorough analysis of the probable solutions. Based on the studies conducted for the least developing countries of Asia during the recent preceding years to the difficulties and dangers Afghanistan is looking in the internet and security and strategies to combating cybercrimes.

The status of internet availability and connectivity in Afghanistan at present.

According to Bernadas and Soriano (2018), there is a correlation between a family's and an individual's economic level and their access to technology, the internet, and digital resources [4]. The digital world is unfamiliar and poorly understood by the people of LDCs (least developed nations), which is a result of widespread illiteracy, poverty, and a weak economy.

Teaching the next generation to be digitally literate and cyber-savvy is crucial, according to Smith et al. (2018)[22]. At the beginning of 2023, when internet penetration was 18.4%, a notable study states that almost 7.67 million people in Afghanistan were using the internet. In January 2023, 3.15 million people, or 7.6 percent of the entire population, were active on social media in Afghanistan. According to Ookla's statistics, fixed internet connection speeds in Afghanistan increased by 0.58 Mbps (a growth of 34.7%) over the same time period.

During Covid 19 pandemic many countries had to make sudden change for imparting education and almost all of them have switched to online tools. In response to the unique demand for online education in Afghanistan, the Ministry of Higher Education (MoHE) developed a platform called Higher Education Learning Management System (HELMS). However, the reality was very different, and educators encountered enormous obstacles when attempting to offer online instruction. Afghanistan's IT infrastructure was ill-prepared for the abrupt transition.[Ashmi, Hashimi (2021)]. Smith et al. (2018)[22] and Jones and Brown (2020) agree that cybersecurity education is crucial for dealing with new digital threats.

Afghanistan Telecommunication Regulatory Authority, which was an independent authority in Telecommunications and is currently working under the supervision of Ministry of Communication and IT has been given limited resources and technical capacity in order to implement open access. These limitations have been a hurdle in the way of implementing FTTH (Fiber to the Home) in Afghanistan.[Akmal Elam et. al.;(2023)][13]

## THREATS TO CYBERSECURITY TO AFGHANISTAN

The United Nations has prioritized cyber defense because of the critical role it plays in the global economy and society. Combating Criminal Use of ICTs (A/RES/55/63 and A/RES/56/121), Culture of Cybersecurity (A/RES/57/239), Critical Infrastructure (A/RES/58/199), and Global Culture of Cybersecurity (A/RES/64/211) are the five cybersecurity concerns that the United Nations has published resolutions on. [27] Daily, there are about 230,000 new malware infections and over 4,000 ransomware assaults, as reported by Hammond [9]. On a worldwide scale, a number of national CSIRTs have been established. In order to serve its constituents, the Afghan Computer Emergency Response Team (AFCERT) has been working closely with Afghan law enforcement to raise awareness about cybercrime and to develop strategies to fight it [10], [11].

According to Avanti Kumar (2013), cybersecurity encompasses more than simply the information technology business when it comes to protecting data.[5]. The term "cyber-attack" may refer to any kind of assault that targets our digital devices and is carried out over the internet. According to Al Mazari et. al. (2018), cyber threats may be a major concern since cyberattacks can cause power outages, malfunctions in military equipment, and the disclosure of sensitive national information.[7].

## THREATS FOR AFGHANISTAN CYBER SECURITY

According to the Global Cybersecurity Index, Afghanistan ranks 176th out of 193 nations. Broadly Afghanistan has three challenging issues regarding cybersecurity. After its formal naming as AFCERT in 2009, Afghanistan's first Cyber Emergency Response Team (CERT) was created by the US-led interim government's Ministry of Communications and Information Technology (MCIT). As a government and commercial sector organization, AFCERT's mission was to combat cybercrime and threats while also raising public and business sector awareness of the issue and offering solutions. The AFCERT reported that the threats to Afghanistan's cyber space is increasing and needed strong committed actions to safeguard public, private and individual's entities. [Wafa, Z. M. A. R. I. A. L. A. I. (2014)][18]

Cyberspace security is a topic that requires a thorough CSS in Afghanistan. Cybersecurity is only one of many potential issues that Afghanistan may encounter as it works to integrate ICT into its vital information infrastructure. Afghanistan needs a thorough cyber security plan because of all the dangers and threats it faces [Salamzada, K., Shukur, Z., & Bakar, M. A. (2015)].[14]. Abdul Musawer [12] reported in his article that during 2022, Afghanistan experienced over 100 million cyberattacks and the most common amongst these cyberattacks in Afghanistan are phishing, malware, and denial-of-service attacks.

Two serious cyber security vulnerabilities have been identified in Afghanistan, according to studies from the International Telecommunication Union (ITU) (2012). To start, the government does not have a system in place to monitor for, recognize, and prevent cyber risks and threats. In a similar vein, antivirus software—which is essential for protecting computers from malicious software—is missing from certain government agency computers.

In the US national cyber security strategy, Dlamini, Taute, and Radebe (2011)[24] claim that it includes initiatives such as cyber security awareness programmes, efforts to raise public knowledge on cyber security concerns, and support for cyber security research via financing.

## POSSIBLE SOLUTIONS TO THE CYBER SECURITY CHALLENGES OF AFGHANISTAN

To address cyberspace security challenges, Afghanistan need an all-encompassing cybersecurity architecture and infrastructure. Given that Afghanistan is now working to incorporate ICT into its key information infrastructure, the nation may encounter several cyberspace-related difficulties. As a result, Afghanistan needs a thorough cybersecurity architecture and plan. Because of the many cyber applications that have made their way into the public and private sectors, the internet has become an integral part of both. Because of this, the nation has to implement a thorough and suitable cybersecurity strategy and infrastructure to deal with all the issues and dangers in this field.

If Afghanistan's information and communication technology (ICT) industry is to realize its vision of a safe cybersecurity framework and strategy, it must overcome the following critical obstacles [Ministry of Communication and IT, E-Government Directorate]:

1) In politics and ongoing ICT initiatives, cybersecurity isn't given enough emphasis. Furthermore, no governmental nor non-governmental entities have embraced cyber security concepts.

2) No comprehensive plan exists to handle and lessen the impact of cybersecurity crises in the event of a coordinated cyberattack on the nation's most vital data centers, and the Critical National Information Infrastructure (CNII) has not been officially acknowledged. It was suggested that the country ought to make a public network safety methodology outlining how different parties may work together to safeguard critical national infrastructure information (CNII).

3) The cybersecurity issues that exist today are unaddressed by the current cybersecurity laws, rules, and regulations.

4) The fourth point is that everyone involved in cybersecurity—from regulators and law enforcement to judges and prosecutors—as well as service providers, financial institutions, and service providers themselves—needs better training in this area. In a recent publication by Bechara and Schuch (2021),[21]

5) At the national level, there is a lack of adequate coordination and mechanisms for managing cyber-attack and cyber threat monitoring, identification, tracking, and mitigation.

6) The establishment of a National Computer Emergency Response Team is necessary to effectively monitor and detect cyber dangers, as well as to provide public education on the matter. Since there is no cooperation about cybersecurity concerns, this recommendation has been made [Lewis, T. G. (2019)].[20].

7) Seventhly, the government should launch education initiatives to raise public consciousness on cyber laws, the consequences of cybercrime, and ways to prevent it. The Republic of Botswana's Ministry of Transport and Communications has a national cybersecurity strategy. Cybersecurity Policy at the National Level. Unknown Publication: Botswana's Ministry of Transport and Communications, National Cybersecurity Strategy.[26].

## 2. CONCLUSION

Afghan information and communication technology (ICT) services have undergone tremendous social and financial development in the ten years following the inauguration of a new government, according to an analysis of document content and interviews, as well as the cyber protection strategies of a number of developed and developing nations (including the United States, the United Kingdom, Israel, Japan, South Korea, Malaysia, Singapore, and India). Despite the country's cybersecurity vulnerabilities, no infrastructure or framework was discovered to be in place. As a result, a thorough cybersecurity strategy, infrastructure, and framework is necessary for Afghanistan to address the difficulties posed by cyber attacks, given that the country is increasingly offering ICT-based solutions and is emerging on the international stage.

## 3. SUGGESTIONS & RECOMMENDATIONS

There are a lot of moving parts when it comes to national cybersecurity governance and management programs, including encryption, application security, and disaster recovery,

among many others. Issues related to meeting regulatory standards, such as HIPAA and PCI DSS.

The establishment of the National Cyber Security Agency (NACSA) by the Malaysian government in January 2017 shows how seriously the government takes the need for a more coordinated approach to cybersecurity threats.[28]

To make sure the cybersecurity program follows the policy document's stated goals, objectives, and recommendations, a set of guiding principles is created. According to T. Benzel (2015), there are some rules of thumb that apply only to the field of cybersecurity.Page 16:

1) Plan studies in a way that makes methodical strides towards attaining the characteristics and ideal condition of a robust cyber ecosystem.

2) Labs in the social sciences to supplement "hard computer science" studies with an understanding of the social scientific aspects of cybersecurity.

3) The third area of focus should be the study of thorough scientific methods that can support the necessary security policies.

4) Investigation of viable scientific methods that firmly and thoroughly support the quantitative evaluation of cybersecurity risks to complex systems, particularly vital infrastructure. investigation of potential scientific methods for automating collaborative tasks among dispersed systems in order to safeguard specific computer systems and Internet connections.

5) Studies that acknowledge cybermilitary forces, maybe focusing on Manichean sciences.

6) Occupy movement research facilities to seek for unfilled research needs in cybersecurity and to identify new scientific methods and technology solutions.

7) The seventh point is to rely on current cybersecurity-related information.

8) Eighth, put more resources toward studies that deal with cyber and big data issues..

INTERNATIONAL COOPERATION AND PUBLIC-PRIVATE PARTNERSHIP

We must prioritize cyber security. With the development of their own national cyber security agendas, more than 75 nations have made it a high priority to address.[29]

There is no physical border between nations in the cyber world. International collaboration is essential for the success of cybersecurity programs. To better protect its vital national information infrastructures, Afghanistan can benefit by sharing best practices, gathering intelligence, debating obstacles, and learning from the errors of others; contributing to the development and direction of international policy; and taking the initiative. According to Spencer (2017)[17]. To help ensure the availability and stability of vital information and communication technologies, it may be helpful for government agencies to develop partnerships with infrastructure owners and operators. Government agencies may better understand the resilience of critical infrastructure, coordinate efficient incident management, and distribute crucial information about security threats and vulnerabilities when they work

with industry partners.[25]

In order to make cyberspace a safer environment for everyone, the Afghan government will work toward consensus, agreement, and collaboration:

- Coordinate efforts on a global scale to combat cybercrime and threats: - We will maintain our tight collaboration with global allies and partners to fortify cyber event reporting and response systems.

- In order to coordinate the regional response against cybercrime, we will collaborate with Member States from across the world. Cybercrime is a global problem, thus we will also increase funding to connect with operational networks and capacities throughout the globe. (Carr, 2016)[19].

- Help share ideas on cyber policies and laws: We will keep taking part in regional and worldwide conversations about cyber laws and policies, cyber deterrence, and cybercrime collaboration. In order to initiate, encourage, and facilitate discussions on cybercrime and cybersecurity, we will be holding an annual Afghanistan International Cyber Week (AICW).

**References**


1. Romanoff, M., F. Vacarelu, P. Biggs, S. Raja, E. Gasol Ramos, M. Minges, P. Lal Das, C. M. Rossotto, T. Nadyseva, M. F. Badran, R. F. Fukui, G. K.-P. Edman, R. S. Firestone, B. R. Larson, E. Clemente Miranda, T. J. C. Kelly & M. Luengo-Oroz (2018). Information and Communication for Development 2018: Data-Driven Development (English).
2. Hatakka, M., Thapa, D., & Sæbø, Ø. (2020). Understanding the role of ICT and study circles in enabling economic opportunities: Lessons learned from an educational project in Kenya. Information Systems Journal, 30(4), 664-698.
3. Aruleba, K., & Jere, N. (2022). Exploring digital transforming challenges in rural areas of South Africa through a systematic review of empirical studies. Scientific African, 16, e01190.
4. Bernadas, J. M. A. C., & Soriano, C. R. (2018). Online privacy behavior among youth in the Global South: A closer look at diversity of connectivity and information literacy. Journal of Information, Communication and Ethics in Society, 17(1), 17-30.
5. Avanti Kumar. ("July/ Aug 2013. 7. CIO Asia, September 3rd, H1 2013"). IEEE Security and Privacy Magazine–IEEECS "Safety Critical Systems – Next Generation": Cyber security in Malaysia.
6. Al Mazari, A.; et al. (2018). Cyber terrorism taxonomies: definition, targets, patterns, risk factors, and mitigation strategies. Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications, pp. 608–621. IGI Global, Hershey
7. Hashemi, A. (2021). Online teaching experiences in higher education institutions of Afghanistan during the COVID-19 outbreak: Challenges and opportunities. Cogent Arts & Humanities, 8(1), 1947008.
8. A. Hammond. (2018). February 16, 2018. Three Issues to Address. The Data Center Journal Cybersecurity 2018 http://www.datacenterjournal.com/cybersecurity-2018-three-issuesaddress.
9. Profile, I. C. (n.d.). ITU. Retrieved 2014, from ITU [Online]. Available: http://www.itu.int/en/ITUD/Cybersecurity/Pages/default.aspx
10. Information and Cyber Security Directorate Director Interview.
11. https://www.linkedin.com/pulse/afghanistan-cybersecurity-tremendous-challenge-fragile-

abdul-musawer-51zuc/
12. Elam, A., & Elam, A. W. Technical, Technological and Operational Feasibility of FTTH in Afghanistan.
13. Salamzada, K., Shukur, Z., & Bakar, M. A. (2015). A framework for cybersecurity strategy for developing countries: Case study of Afghanistan. Asia-Pacific Journal of Information Technology and Multimedia, 4(1), 1-10.
14. Ministry of Communication and IT, EGovernment Directorate, E-Government Resource Center. (December 05, 2015) DRAFT CYBERSECURITY PLAN. Unknown Place of Publication: Ministry of Communication and IT. [Online] [Accessed on 28th March 2020] https://mcit.gov.af/sites/default/files/2020-08/DRAFT%20CYBER%20SECURITY%20PLAN% 20%20Dec%205%202015_0.pdf.
15. T. Benzel, "A Strategic Plan for Cybersecurity Research and Development" in IEEE Security & Privacy, vol. 13, no. 04, pp. 3- 5, 2015.doi: 10.1109/MSP.2015.84.
16. Spencer, Fm. (2017). Public-Private Partnerships (PPP) for Cybersecurity Infrastructures. DOI: 10.13140/RG.2.2.22703.59044.
17. Wafa, Z. M. A. R. I. A. L. A. I. (2014). National Cyber Security Strategy of Afghanistan (NCSA). Islamic Republic of Afghanistan Ministry of Communications and IT.
18. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 4362
19. Lewis, T. G. (2019). Critical infrastructure protection in homeland security: defending a networked nation. John Wiley & Sons.
20. Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. Journal of Financial Crime, 28(2), 359-374.
21. Smith, J., et al. (2018). Imparting Digital Literacy and Cybersecurity Skills to Young Learners. Journal of Educational Technology, 14(2), 87-101.
22. Jones, S., & Brown, E. (2020). The Necessity of Comprehensive Cybersecurity Education in a Digital World. International Journal of Information Security, 8(3), 211-225.
23. Dlamini, I. Z., Taute, B., & Radebe, J. 2011. Framework for an African policy towards creating cyber security awareness. Paper presented at the 21st IFIP TC9/TC11 South African Cyber Security Awareness Workshop (SACSAW), May 12th, Garborone, Botswana.
24. https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf.
25. Lebogang, V., Tabona, O., & Maupong, T. (2022). Evaluating cybersecurity strategies in Africa. In Cybersecurity capabilities in developing nations and its impact on global security (pp. 1-19). IGI Global.
26. D. F. Wamala, “ITU National Cybersecurity Strategy Guide.” International Communication Union (ITU), 2011.
27. “Global Cybersecurity Index (GCI) 2017.” International Communication Union (ITU), 2017.
28. Vu, C., & Rajaratnam, S. (2022). Cyber security in Singapore. S. Rajaratnam School of International Studies.