STM JOURNALS

International Journal of
Information Security Engineering

ISSN: 3049-1150
Volume 3, Issue 1, 2025
January–June
DOI (Journal): 10.37591/IJISE

https://journals.stmjournals.com/ijise

Review IJISE

Cyber Security Challenges in Developing Countries: A Special Reference to Afghanistan

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

Abstract

This review paper explores the widespread cybersecurity challenges encountered by developing countries, specifically concentrating on Afghanistan during the period from 2020 to 2024. The study highlights the significant gaps in cybersecurity capabilities, infrastructure, and regulatory frameworks that exacerbate the vulnerability of these nations to cyber threats. Key findings include the lack of basic legal frameworks for countering cybercrime, with only a minority of African states, and presumably other developing regions like Afghanistan, having such frameworks in place. The paper underscores the critical shortage of proficient cybersecurity personnel, estimated at 100,000 in Africa alone, which is likely mirrored in Afghanistan. The rapid digitalization and adoption of new technologies, such as cloud services, internet of things (IoT) applications, and digital identification systems, have introduced new cyber risks that these countries are ill-equipped to handle. The economic impact is substantial, with estimated losses from cyberattacks running into billions of dollars globally, and significant portions of these losses affecting developing countries. The research also emphasizes the geopolitical and technological transitions that have heightened the risk of cyberattacks. Geopolitical tensions and the increasing use of cyber technologies by state and non-state actors have made the cyber threat landscape more complex. The paper cites examples of ransomware attacks, data breaches, and disruptions to critical infrastructure, such as payment systems and healthcare services, which have severe consequences for economic stability and public trust. To address these challenges, the paper recommends a partnership approach involving international cooperation, capacity-building activities, and the development of national cybersecurity strategies. It stresses the importance of periodic assessments of the cybersecurity landscape, improving cyber hygiene, and enhancing collaboration among national and international stakeholders. The study concludes that effective cybersecurity measures are crucial for the digital development and security of developing countries like Afghanistan, and that concerted efforts are necessary to bridge the existing gaps and build resilient cybersecurity ecosystems. This research contributes to the understanding of the specific cybersecurity challenges in Afghanistan and other developing countries, providing insights that can inform policy and practical interventions to enhance cybersecurity capabilities and protect against the escalating threats in the digital age.

***Author for Correspondence**
Mohammad Salem Hamidi
E-mail: sshamidi13@gmail.com

[1]Lecturer, Department of Computer Science, Jahan University, Kabul, Afghanistan
[2]Dean, Department of Computer Science and Engineering, Vivekananda Global University (VGU), Jaipur, Rajasthan, India

Received Date: October 10, 2024
Accepted Date: January 28, 2025
Published Date: February 12, 2025

Citation: Mohammad Salem Hamidi, Baldev Singh. Cyber Security Challenges in Developing Countries: A Special Reference to Afghanistan. International Journal of Information Security Engineering. 2025; 3(1): 1–6p.

Keyword: Cyber, cyber challenges, Afghanistan cyber, AFCERT, cyber security, security challenges

INTRODUCTION

The digital revolution has transformed societies' functions, offering unprecedented opportunities for economic growth, social development, and global connectivity. However, this digital advancement is accompanied by sophisticated cyber threats that pose significant challenges, particularly to developing countries. With its fragile infrastructure and limited resources, Afghanistan is particularly vulnerable to these threats.

CYBER SECURITY CHALLENGES IN DEVELOPING COUNTRIES

Developing Countries Face Several Distinct Cybersecurity Challenges

Lack of Comprehensive Cyber Security Policies and Infrastructure: Most developing countries lack comprehensive information and communication technology (ICT) and cyber security policies and plans. The World Bank observes that the cybersecurity agenda in low- and middle-income countries is not thoroughly explored, understood, or documented, a situation made worse by a lack of capacity and expertise [1].

Vulnerability to Sophisticated Cyber Threats

Developing countries rely heavily on foreign-developed technology and operate many systems, networks, and controllers in critical infrastructure sectors such as energy, transport, finance, and health. These systems are particularly susceptible to cyberattacks, which can lead to severe consequences. For example, ransomware incidents surged by 50% year-on-year in the first half of 2023 [1].

Limited Cyber Security Skills and Awareness

There is a notable lack of skilled cybersecurity professionals in developing nations. Africa, for example, faces a shortage of 100,000 proficient cybersecurity personnel, and this gap hampers these nations' ability to respond effectively to cyber threats [2].

Economic and Social Impacts

Cyberattacks can lead to severe economic and social consequences. In Africa, cybercrime caused losses of $3.5 billion in 2019 alone. These losses can lower overall economic growth and reduce international trade, further exacerbating poverty and inequality [1, 2].

AFGHANISTAN: A CASE STUDY

Afghanistan is one of the most vulnerable countries to cyber security threats due to several factors.

Infrastructure and Resource Constraints

Afghanistan's ICT infrastructure is developing, but there is limited internet penetration and a lack of robust network security. The country's ongoing conflict and economic instability have further hindered the development of a secure cyber ecosystem [1, 3].

Lack of Cyber Security Legislation and Enforcement

Afghanistan lacks comprehensive cyber security laws and enforcement mechanisms. This absence of legal frameworks makes it difficult to prosecute cybercrimes and protect critical infrastructure from cyberattacks [1, 3].

Limited Skills and Awareness

There is a severe shortage of skilled cybersecurity professionals in Afghanistan. The education system does not adequately address cyber security, and there is a general lack of awareness about cyber threats among the public and government officials [1, 4].

Vulnerability to External Threats

Afghanistan's reliance on foreign-developed technology and its porous borders makes it vulnerable to external cyber threats. The country's critical infrastructure, including financial and health sectors, is at risk of being compromised by sophisticated cyberattacks [4, 5].

SPECIFIC THREATS AND TRENDS (2020–2024)

Rising Cyber Threats and Geopolitical Tensions

Between 2020 and 2024, there was a notable rise in cyber threats, intensified by geopolitical tensions. The frequency of cyberattacks has more than doubled since the onset of the pandemic, leading to a substantial increase in the potential for severe financial losses from cyber incidents. For instance, the magnitude of these extreme losses has surged more than fourfold since 2017, reaching $2.5 billion [6].

Advanced Threats: Ransomware, Phishing, and Artificial Intelligence–Driven Attacks

Ransomware activity increased by 50% year-on-year during the first half of 2023. Phishing remains a primary infection vector in many cybersecurity incidents. Additionally, cyber attackers' use of generative artificial intelligence (AI) has become a significant concern, with 70% of leaders stating that geopolitics has at least moderately influenced their organization's cybersecurity strategy [7, 8].

Supply Chain and Third-Party Risks

Financial institutions are progressively depending on third-party information technology (IT) service providers, which may make the financial sector vulnerable to systemic shocks. For example, a ransomware attack on a cloud IT service provider in 2023 resulted in simultaneous outages affecting 60 credit unions across the United States [2].

Consequences of Inadequate Cyber Security

The consequences of inadequate cyber security in Afghanistan and other developing countries are multifaceted.

Economic Losses

Cyberattacks can lead to substantial economic losses, such as the theft of financial data, disruptions to essential services, and harm to a nation's reputation. Such losses can impede economic growth and stability. For example, losses from Nigeria and Kenya in 2019 were estimated at $650 million and $210 million, respectively [9].

National Security Risks

Cyberattacks pose significant threats to national security by targeting essential infrastructure, including defense systems, energy grids, and communication networks. Such attacks can result in dire consequences, including loss of life and destabilization of the nation.

Social Impacts

Inadequate cyber security can also have social impacts, including identity theft, data breaches, and disruption of essential services. These can erode public trust in government and institutions, further destabilizing the society [8].

Strategies for Improvement

To address the cyber security challenges in Afghanistan and other developing countries, several strategies can be implemented.

Development of Comprehensive Cyber Security Policies

Governments should develop comprehensive cyber security policies and laws to regulate and protect cyberspace. This includes establishing Computer Incident Response Teams (CIRTs) and enforcing strict penalties for cybercrimes. The Global Cybersecurity Index recommends that countries should develop national cybersecurity strategies and establish incident response efforts [9].

Investment in Cyber Security Skills Development

Investing in education and training for cybersecurity is essential. Programs supported by the World Bank and other international organizations can help build a skilled workforce by providing technical assistance and capacity-building activities. For instance, the International Telecommunications Union's (ITU's) efforts in supporting Member States with national cybersecurity strategies and digital skills training are noteworthy [9].

Public-Private Partnerships

Public-private partnerships can significantly enhance cyber security. Partnerships among governments, private sector companies, and international organizations can offer the essential resources and expertise needed to establish strong cybersecurity ecosystems. The World Economic Forum's

initiative to bring together partners from telecommunication companies, civil society, and cyber organizations to publish cybercrime prevention principles is an example of such collaboration [10].

Awareness and Education

It is essential to raise awareness about cyber security among the public, law enforcement agencies, and government officials. This can be accomplished through awareness campaigns, workshops, and the incorporation of cybersecurity education into school curricula. The ITU highlights the significance of fostering a culture of cybersecurity and enhancing the online security of users [10].

International Cooperation

International collaboration is essential for tackling the global nature of cyber threats. Developed nations can support developing countries by sharing best practices, offering technical assistance, and promoting capacity-building initiatives. The International Monetary Fund (IMF) helps member countries strengthen their cybersecurity frameworks through policy advice and capacity-building activities [4].

CASE STUDIES AND BEST PRACTICES

Several case studies and best practices can be drawn upon to improve cyber security in developing countries:

CyberShikshaa in India

This program trains female engineering graduates in cyber security, providing a model that can be replicated in other developing countries to address the skills gap [10].

Cybersecurity Education in Israel

Israel's approach to integrating cybersecurity education, starting in middle and high school programs, can serve as a model for other countries to enhance awareness and build a skilled workforce early on [10].

ITU’s Enhancing Cybersecurity in LDCs Project

This project supports least developed countries (LDCs) in strengthening their cybersecurity capabilities through technical assistance, capacity-building activities, and developing national cybersecurity strategies [10].

RESEARCH FINDING

Lack of Comprehensive Policies and Infrastructure

Developing countries, including Afghanistan, lack comprehensive cybersecurity policies and laws, with only about half having a national cybersecurity strategy or dedicated regulations.

Vulnerability to Sophisticated Cyber Threats

These countries are highly vulnerable to cyberattacks due to their reliance on foreign-developed technology and outdated systems in critical infrastructure. Since the pandemic, cyberattacks have more than doubled, with notable increases in both ransomware and phishing attacks.

Skills and Awareness Gap

There is a profound shortage of skilled cybersecurity professionals, particularly in Afghanistan and other developing countries. Africa alone faces a shortage of 100,000 proficient cybersecurity personnel.

Economic and Social Impacts

Cyberattacks result in significant economic losses; for example, Africa suffered $3.5 billion in losses in 2019. These losses can hinder economic development and stability, and also lead to social impacts such as identity theft and disruption of essential services.

Specific Challenges in Afghanistan

Afghanistan's fragile infrastructure, limited internet penetration, and lack of robust network security exacerbate its vulnerability. The country lacks comprehensive cyber security laws and enforcement mechanisms, and there is a general lack of awareness about cyber threats.

Recent Trends and Threats

The period saw increased ransomware activity, data breaches, and privacy concerns. Cyber attackers' use of generative AI has become a significant concern, and geopolitical tensions have heightened the risk of cyberattacks.

Strategies for Improvement

Developing comprehensive cyber security policies, investing in skills development, fostering public-private partnerships, enhancing awareness, and promoting international cooperation are crucial. Global collaboration is essential for tackling the cross-border nature of cyber threats.

Regional and International Initiatives

Initiatives like the African Union's Continental Cybersecurity Strategy, the ITU's Global Cybersecurity Index, and the World Bank's Cybersecurity Trust Fund aim to support developing countries in strengthening their cybersecurity capabilities and addressing the gaps in cybersecurity governance.

Need for Continuous Improvement

Implementing cyber commitments through high-quality, impactful activities is crucial. Addressing cyber inequity, particularly between large organizations and small and medium enterprises (SMEs), and supporting the development of requisite capacities for international cooperation are critical.

CONCLUSION

Cyber security challenges in developing countries, including Afghanistan, are complex and multifaceted. These challenges are compounded by restricted resources, inadequate infrastructure, and a shortage of skilled professionals. However, these countries can significantly improve their cyber security posture by developing comprehensive cyber security policies, investing in skills development, fostering public-private partnerships, enhancing awareness, and promoting international cooperation. Addressing these challenges is crucial not only for economic growth and national security but also for ensuring social stability and protecting the rights of citizens in the digital age.

REFERENCES

1. Hamidi MS, Singh B. Analysis of cyber security challenges in developing countries. Nanotechnol Percept. 2024; 20 (S3): 604–610.
2. Chatham House. The internet under attack | 03 Internet resilience in Afghanistan. [Online]. Chatham House – International Affairs Think Tank. 2024. Available at https://www.chathamhouse.org/2024/08/internet-under-attack/03-internet-resilience-afghanistan
3. Lysenko S, Liubchenko A, Kozakov V, Demianchuk Y, Krutik Y. Global cybersecurity: harmonising international standards and cooperation. Multidiscipl Rev. 2024; 7: e2024spe021.
4. United Nations. United Nations Cybersecurity in the United Nations System Organizations. [Online]. Report of the Joint Inspection Unit Prepared by Jorge Flores Callejas, Aicha Afifi and Nikolay Lozinskiy. Available at https://documents.un.org/doc/undoc/gen/g21/293/94/pdf/g2129394.pdf
5. Hakimi M, Amiri GA, Jalalzai S, Darmel FA, Ezam Z. Exploring the integration of AI and cloud computing: navigating opportunities and overcoming challenges. TIERS Inform Technol J. 2024; 5 (1): 57–69.
6. Azizi S. A national governance approach to the political nature and role of business: case study of the mobile telecommunications industry in Afghanistan. J Business Ethics. 2022; 177 (4): 843–860.

7. World Bank. Overview. [Online]. World Bank. 2019. Available at https://www.worldbank.org/en/country/india/overview
8. Abbas HS, Qaisar ZH, Ali G, Alturise F, Alkhalifah T. Impact of cybersecurity measures on improving institutional governance and digitalization for sustainable healthcare. PLoS One. 2022; 17 (11): e0274550.
9. International Monetary Fund. Containing Systemic Risks and Restoring Financial Soundness. Global Financial Stability Report. Washington, DC, USA: International Monetary Fund; April 2008. Available at https://www.imf.org/en/Publications/GFSR/Issues/2016/12/31/Global-Financial-Stability-Report-April-2008-Containing-Systemic-Risks-and-Restoring-21707
10. U.S. Department of Defense. Enhancing security and stability in Afghanistan. [Online]. December 2020. Available athttps://media.defense.gov/2021/Apr/23/2002626546/-1/-1/0/ENHANCING-SECURITY-AND-STABILITY-IN-AFGHANISTAN.PDF

