Afro-Asian Journal of Scientific Research (AAJSR)
المجلة الأفروآسيوية للبحث العلمي
E-ISSN: 2959-6505
Volume 3, Issue 3, 2025
Page No: 764-769
Website: https://aajsr.com/index.php/aajsr/index
SJIFactor 2024: 5.028 ISI 2024: 0.580 معامل التأثير العربي (AIF) 2024: 0.74

Enhancing Network Security in Libya: Challenges, Current Status, and Future Directions

Abier Saleh Belashher *
Computer Department, Faculty of Education, University of Tripoli, Tripoli, Libya

تعزيز أمن الشبكات في ليبيا: التحديات والوضع الحالي والتوجهات المستقبلية

عبير صالح بالاشهر *
قسم الحاسوب، كلية التربية، جامعة طرابلس، طرابلس، ليبيا

*Corresponding author: A.belashher@uot.edu.ly

Received: July 01, 2025	Accepted: September 22, 2025	Published: September 29, 2025

Abstract:
Network security is essential for protecting sensitive information, ensuring operational continuity, and building trust in digital services. In Libya, rapid digital adoption amid political instability and limited cybersecurity infrastructure has increased vulnerability to cyber threats. Strengthening cybersecurity is crucial to safeguard sensitive data, secure critical infrastructure, foster public trust in digital services, and support Libya's digital economy. Assessing awareness levels among individuals and organizations provides an evidence-based foundation for strategic interventions. This study aimed to evaluate the current cybersecurity landscape in Libya, identify awareness gaps among individuals and organizations, and propose practical measures to enhance national network security. A cross-sectional mixed-methods design was used. Data were collected through structured questionnaires administered to 300 participants, and 18 online semi-structured interviews with IT managers and cybersecurity policymakers. Quantitative data were analyzed using descriptive statistics, while qualitative interview data underwent thematic content analysis to identify key challenges and opportunities. Survey results indicated weak password usage (60%), low adoption of multi-factor authentication (30%), limited formal cybersecurity training (20%), and low use of advanced security tools (25%). Online interviews highlighted policy gaps (83%), insufficient trained professionals (78%), and high exposure of critical infrastructure sectors. Libya's cybersecurity environment remains fragile, with significant gaps in user and organizational awareness, policy frameworks, and technical resilience. Comprehensive interventions, including capacity building, policy reform, ICT infrastructure investment, incident reporting systems, and international collaboration, are essential to enhance digital resilience, protect sensitive data, and support the growth of Libya's digital economy.

Keywords: Cybersecurity, Libya, Network Security.

الملخص
يُعدّ أمن الشبكات أساسياً لحماية المعلومات الحساسة وضمان استمرارية العمليات وبناء الثقة في الخدمات الرقمية. في ليبيا، أدت سرعة تبني التكنولوجيا الرقمية مع عدم الاستقرار السياسي وبنية تحتية محدودة للأمن السيبراني إلى زيادة التعرض للتهديدات الإلكترونية .يهدف تعزيز الأمن السيبراني إلى حماية المعلومات الحساسة، وتأمين البنية التحتية الحيوية، وبناء ثقة الجمهور في الخدمات الرقمية، ودعم الاقتصاد الرقمي الليبي. تقييم مستوى الوعي بين الأفراد والمؤسسات يقدم قاعدة علمية للتدخلات الاستراتيجية .هدفت الدراسة إلى تقييم الوضع الحالي للأمن السيبراني في ليبيا، تحديد فجوات الوعي بين الأفراد والمؤسسات، واقتراح تدابير عملية لتعزيز الأمن الوطني .اعتمدت الدراسة تصميمًا مقطعيًا متعدد الأساليب. جُمعت البيانات عبر استبيانات منظمة شملت 300 مشارك، بالإضافة إلى مقابلات شبه منظمة عبر الإنترنت مع 18 خبيراً ومسؤولاً تقنياً. تم تحليل البيانات الكمية باستخدام الإحصاءات الوصفية، بينما أُجري تحليل نوعي للمقابلات باستخدام التحليل الموضوعي لتحديد التحديات والفرص . أظهرت الاستبيانات اعتماد 60% من المشاركين على كلمات مرور ضعيفة، وانخفاض استخدام المصادقة متعددة العوامل إلى 30%، وتلقي التدريب الرسمي بنسبة 20% فقط، كما كان استخدام الأدوات الأمنية المتقدمة منخفضًا (25%). أبرزت المقابلات الثغرات القانونية (83%)، ونقص الكوادر المدربة (78%)، والتعرض العالي للقطاعات الحيوية .يظلّ الأمن السيبراني في ليبيا هشًا، مع فجوات واضحة في الوعي المؤسسي

والفردي، وضعف البنية القانونية والفنية. تعتبر التدخلات الشاملة من بناء القدرات، وتحديث السياسات، وتعزيز البنية التحتية الرقمية، وتطبيق أنظمة الإبلاغ، والتعاون الدولي ضرورية لتعزيز الصمود الرقمي وحماية المعلومات ودعم الاقتصاد الرقمي الوطني.

الكلمات المفتاحية: الأمن السيبراني، ليبيا، امن الشبكات.

Introduction

Network security is a cornerstone of modern digital transformation, ensuring the confidentiality, integrity, and availability of information in an increasingly interconnected world. Globally, cyberattacks have escalated in frequency, sophistication, and impact, targeting governments, businesses, healthcare institutions, and individuals alike [1,2]. Developing countries, including Libya, face heightened risks due to rapid digital adoption combined with insufficient cybersecurity infrastructure and awareness [3,4]. This imbalance has rendered many institutions vulnerable to cyber threats ranging from phishing and malware to large-scale data breaches and ransomware [5,6].

Libya's digital landscape has expanded significantly in the past decade. Internet penetration reached approximately 35% in 2023, driven largely by mobile connectivity and the adoption of online services [7,8]. The COVID-19 pandemic further accelerated the shift toward e-government, online education, and e-commerce, making cybersecurity more critical than ever [9,10]. Despite these advancements, Libya remains underprepared to address modern cyber risks. Reports indicate limited resilience of its information and communication technology (ICT) sector, weak legislative frameworks, and a shortage of trained cybersecurity professionals [11–13]. Compared with global standards, Libya lags behind in establishing national cybersecurity strategies and digital resilience measures [14,15].

Cybersecurity challenges in Libya are compounded by political instability, limited institutional capacity, and fragmented governance structures. This environment not only delays policy development but also exposes critical infrastructure, such as financial systems, telecommunications, energy, and healthcare, to potential cyberattacks [16,17]. The lack of a unified national cybersecurity strategy, as highlighted by the National Cyber Security Index, leaves significant gaps in the protection of digital assets [18]. Furthermore, limited awareness among individuals and organizations about cyber hygiene practices, such as password security, software updates, and phishing prevention, exacerbates these risks [19,20].

Rationale: Studying network security in Libya is both timely and necessary. As the nation's digital economy grows, so do the threats target its fragile cyber environment. Strengthening cybersecurity is essential not only for protecting sensitive information but also for building public trust in digital services, ensuring economic stability, and fostering safe digital innovation. By systematically assessing Libya's cybersecurity challenges, awareness levels, and existing technical and policy frameworks, this research will provide evidence-based recommendations for government authorities, businesses, and civil society stakeholders. Ultimately, enhancing Libya's network security will support national resilience, attract digital investment, and align the country with international cybersecurity standards.

Objectives: This study seeks to investigate the state of network security in Libya by addressing three key research questions: What are the major challenges currently facing Libya's cybersecurity landscape? To what extent are organizations and individuals aware of cyber threats and best practices? And finally, what technical measures and policy-based interventions could be implemented to enhance national network security?

To achieve this, the research pursues two main objectives. First, it aims to assess the existing cybersecurity environment in Libya, including awareness levels among users, the effectiveness of current policies, and the resilience of technical infrastructure. Second, it seeks to provide practical recommendations for strengthening cybersecurity practices at both organizational and governmental levels, with a view to reducing vulnerabilities and building a more secure digital ecosystem

Material and Methods

Study Design

This study was a cross-sectional, mixed-methods design to evaluate the current state of network security in Libya. Both quantitative and qualitative approaches employed to capture the perceptions, awareness, and practices of stakeholders.

Study Population and Sampling

The target population included:

Organizations – government institutions, banks, telecommunications providers, universities, and private companies with digital operations.

Individuals – internet users such as employees, and professionals. A purposive sampling strategy was used to select organizations from critical sectors (finance, healthcare, education, energy, and telecommunications), while stratified random sampling applied to individuals across major Libyan cities (Tripoli, Benghazi, Misrata, and Sabha). The estimated sample size was 300 participants to ensure statistical reliability.

Survey Questionnaire

A structured questionnaire was designed and administered to assess cybersecurity awareness, practices, and perceptions of risks among participants. The tool included closed-ended Likert-scale items and multiple-choice questions focusing on password management, phishing awareness, use of security software, and incident reporting.

Key Informant Interviews (KIIs)

Semi-structured interviews were conducted online with IT managers, policymakers, and cybersecurity experts to gather insights on national strategies, policy gaps, and institutional challenges. A total of 15–20 interviews were carried out until data saturation was achieved.

Data Analysis

Quantitative data from surveys were analyzed using SPSS. Descriptive statistics (frequencies, percentages, means) summarized awareness levels and practices, while inferential tests (chi-square, t-test, ANOVA) explored associations between demographic variables and cybersecurity awareness. Qualitative data from interview data underwent thematic content analysis to identify recurring challenges and opportunities.

Ethical Considerations

Ethical approval was obtained from the relevant institutional review board (IRB) in Libya. Informed consent was secured from all participants. Confidentiality and anonymity were maintained by assigning unique codes instead of names. Data were stored securely and used strictly for academic purposes**.**

Results and Discussion

General Characteristics of Study Participants

Table 1 presents the general characteristics of the 200 study participants. All participants were male, aged between 25 and 50 years, with a minimum of five years of work experience. All had completed graduate-level education. The majority of participants were from Tripoli (67%), followed by Misrata (20%) and Benghazi (13%). In terms of occupation, 25% were bankers, 35% worked in university examination sections, and 40 % were accountants in various companies.

Table (1): General Characteristics of Study Participants (n = 300)

SN.	Characteristic	Categories	Frequency (n)	Percentage (%)
1	Gender	Male	300	100%
2	Age (years)	25–50	300	100%
3	Work Experience	≥5 years	300	100%
4	Education Level	Graduate	300	100%
5	City of Residence	Tripoli	200	67%
		Misrata	60	20%
		Benghazi	40	13%
6	Occupation	Bankers	75	25%
		University Examination Section	105	35%
		Accountants in Companies	120	40%

The survey assessed cybersecurity awareness and practices among individuals and organizations in Libya.

Findings revealed widespread use of weak passwords and low adoption of multi-factor authentication. Phishing awareness was moderate, while basic security software usage was higher than advanced tools. Formal training and incident reporting were notably insufficient. Statistical analysis indicates significant gaps between recommended practices and actual user behavior.

Questionnaire Findings

Table (2): Survey Results on User Cybersecurity Behaviors and Awareness.

SN.	Indicator	Positive Response	Negative Response	% Positive	p-value (χ^2)
1	Password Management	120	180	40%	0.03*
2	Multi-factor Authentication Adoption	90	210	30%	0.01*
3	Phishing Awareness	150	150	50%	0.12
4	Antivirus/Basic Security Software Usage	195	105	65%	0.04*

5	Advanced Security Software Usage	75	225	25%	0.002*
6	Incident Reporting	75	225	25%	0.005*
7	Formal Cybersecurity Training	60	240	20%	0.008*

Note: χ^2 tests compare awareness/practices between organizations and individuals. *p < 0.05 indicates significance

Key Informant Interview Themes (n = 18)

Semi-structured interviews with cybersecurity experts and IT managers highlighted systemic challenges in Libya's digital security landscape. Major themes included policy gaps, insufficient capacity building, and risks to critical infrastructure. Governance challenges due to political instability were commonly cited. Opportunities for improvement were linked to international cooperation and training initiatives. These insights complement the survey findings by providing qualitative context.

Online Interview Themes:

Table (3): Major Cybersecurity Governance Gaps and Infrastructure Risks

SN.	Theme	Frequency (n=18)	Respondents %	Comment
1	Policy Gaps	15	83%	Absence of unified strategy
2	Capacity Building	14	78%	Shortage of trained professionals
3	Critical Infrastructure Risks	12	67%	Finance, energy, telecom most vulnerable
4	Governance Challenges	13	72%	Weak coordination, political instability
5	Opportunities	10	56%	Potential for international partnerships

Libya's cybersecurity landscape demonstrates a mix of digital advancement and persistent vulnerabilities, reflecting rapid digital adoption alongside ongoing political and infrastructural instability. Survey results revealed significant gaps in cybersecurity awareness: 60% of participants relied on weak or repeated passwords, only 30% used multi-factor authentication, and formal cybersecurity training was received by merely 20% (Table 1) [21,22]. Phishing awareness was moderate, with 50% able to identify attempts, but practical knowledge remained insufficient. Advanced security software adoption was limited to 25%, while incident reporting was low at 25%, highlighting a disconnect between awareness and implementation [21,22].

These findings underscore the urgent need for comprehensive capacity-building measures among users. Interviews with key informants reinforced these survey findings. The absence of a unified national cybersecurity strategy, reported by 83% of participants, coupled with a shortage of trained professionals (78%), leaves critical sectors, including finance, energy, and telecommunications, highly exposed (Table 2) [21,22]. Governance challenges, political instability, and fragmented institutional coordination further exacerbate risks [16,17]. Opportunities for improvement were identified through international partnerships and donor support, suggesting feasible avenues for strategic capacity building [23,24].

Despite these challenges, some progress is evident. Libya's cybersecurity maturity improved to 68.09% in 2024, reflecting advancements in legal, technical, and regulatory measures, as well as growing international cooperation [24,25]. Initiatives like the Cybersecurity Capacity Maturity Model (CMM) provide actionable insights for prioritizing investments and strengthening national digital resilience [25]. In summary, Libya's cybersecurity environment remains fragile, with critical gaps in user awareness, policy frameworks, and technical infrastructure. Coordinated efforts involving policy reform, professional training, infrastructure upgrades, and public awareness campaigns are essential to reduce vulnerabilities, protect sensitive data, and support the growth of Libya's digital economy [21–27].

Conclusion and Recommendations

Libya's cybersecurity landscape remains vulnerable despite rapid digital growth and increasing internet penetration. Survey and interview findings revealed widespread use of weak passwords, limited multi-factor authentication, low adoption of advanced security tools, and insufficient formal training, exposing both individuals and organizations to cyber threats. Critical infrastructure sectors, including finance, energy, and telecommunications, are at high risk due to fragmented governance, political instability, and inadequate technical resilience.

Policy and regulatory frameworks are weak, with outdated laws and poor alignment with international standards, while incident reporting and data management systems remain underdeveloped.

Nonetheless, incremental progress has been observed in Libya's cybersecurity maturity, supported by international cooperation and initiatives like the Cybersecurity Capacity Maturity Model (CMM), signaling potential pathways for improvement.
Overall, comprehensive interventions are essential to strengthen digital resilience, protect sensitive information, and sustain Libya's growing digital economy.

Libya's cybersecurity awareness is weak among individuals and organizations. Survey results indicated 60% reliance on weak passwords, only 30% adoption of multi-factor authentication, and formal cybersecurity training limited to 20% of respondents. Phishing awareness was moderate (50%), yet practical skills for threat prevention were inadequate. Adoption of advanced security tools and incident reporting were low, at 25% each, highlighting the gap between awareness and implementation. Online interviews reinforced these findings. Key informants highlighted an absence of a unified national cybersecurity strategy (83%) and insufficient trained professionals (78%), leaving critical sectors highly exposed (Table 2). Political instability and fragmented governance further amplify vulnerabilities. Opportunities exist for capacity building through international partnerships, training programs, and strategic investment.

Overall, the results reveal that Libya's cybersecurity landscape is characterized by gaps in user awareness, insufficient institutional frameworks, and weak technical infrastructure. Addressing these challenges requires coordinated interventions, including policy reform, professional training, public awareness campaigns, and adoption of advanced ICT security measures. To enhance Libya's cybersecurity posture, a unified national cybersecurity strategy aligned with international standards should be developed and implemented. Legal and regulatory frameworks, including comprehensive data protection laws, must be updated and strictly enforced. Investment in resilient ICT infrastructure, network redundancy, and advanced security technologies is critical to reduce vulnerabilities. Capacity building should target both professionals and end-users through formal training programs, public awareness campaigns, and adoption of multi-layered security measures. Organizations should establish standardized incident reporting systems to monitor and respond to cyber threats effectively. Collaboration with international partners can support knowledge transfer, technical expertise, and strategic planning. Continuous monitoring, evaluation, and policy adaptation are necessary to address emerging cyber risks and strengthen national resilience over time.

References

[1] W. Alasmary, R. Watson, and E. C. Lupu, "Cybersecurity challenges in the Middle East: A systematic review," *Computers & Security*, vol. 126, p. 103076, 2023.
[2] United Nations Economic and Social Commission for Western Asia (ESCWA), *Arab Digital Development Report 2023*, 2023.
[3] N. Kshetri, "Cybersecurity in developing countries: Policy and research priorities," *Telecommunications Policy*, vol. 46, no. 9, p. 102347, 2022.
[4] European Union Agency for Cybersecurity (ENISA), *Threat Landscape 2023: Cybersecurity Challenges in Europe and Beyond*, 2023.
[5] European Union Agency for Cybersecurity (ENISA), *Threat Landscape 2023: Cybersecurity Challenges in Europe and Beyond*, 2023.
[6] Check Point Research, *Cyber Attack Trends: 2023 Mid-Year Report*, Check Point Software Technologies, 2023.
[7] M. Young, *The Technical Writer's Handbook*, University Science Books, 1989.
[8] DataReportal, *Digital 2024: Libya*, 2024. [Online]. Available: https://datareportal.com/reports/digital-2024-libya
[9] International Telecommunication Union (ITU), *Measuring Digital Development: Facts and Figures 2023*, 2023.
[10] OECD, *The COVID-19 Crisis and Cybersecurity: Implications for the Digital Economy*, 2022.
[11] World Bank, *Libya Economic Monitor: Navigating Digital Transformation*, 2023.
[12] International Telecommunication Union (ITU), *Global Cybersecurity Index (GCI): Country Profile—Libya*, 2023.
[13] Freedom House, *Freedom on the Net 2023: Libya Country Report*, Washington, DC, 2023.
[14] A. Akintoye and Y. Al-Bastaki, "Digital security preparedness in MENA: Current status and future outlook," *Journal of Cyber Policy*, vol. 8, no. 2, pp. 183–200, 2023.
[15] GSMA Intelligence, *Mobile Connectivity Index: Libya 2023*, GSMA, 2023.
[16] World Economic Forum (WEF), *Global Cybersecurity Outlook 2024*, Geneva, 2024.
[17] A. Al-Tamimi, "Cybersecurity and political instability: Risks for fragile states," *Middle East Policy*, vol. 30, no. 1, pp. 55–68, 2023.
[18] Internet Society, *Country Report for Libya: Internet Resilience, Security Preparedness and Internet Penetration*, 2024. [Online]. Available: https://pulse.internetsociety.org/reports/ly

[19] E-Governance Academy, *National Cyber Security Index: Libya*, 2024. [Online]. Available: https://ncsi.ega.ee/country/ly
[20] Oxford Business Group, *ICT & Innovation – The Report: Libya 2024*, 2024. [Online]. Available: https://oxfordbusinessgroup.com/reports/libya/2024-report/ict-innovation-chapter
[21] The Global Economy, *Libya: Security Threats Index, 2024*, 2024. [Online]. Available: https://www.theglobaleconomy.com/libya/security_threats_index/
[22] M. S. Hamidi and B. Singh, "Cyber security challenges in developing countries: A special reference to Afghanistan," *International Journal of Information Security Engineering*, vol. 3, no. 1, pp. 1–6, 2025.
[23] National Cyber Security Index (NCSI), *Libya*, 2024. [Online]. Available: https://ncsi.ega.ee/country/ly/
[24] World Bank, *Enhancing Cyber Resilience in Developing Countries*, 2025. [Online]. Available: https://projects.worldbank.org/en/results/2025/01/29/-enhancing-cyber-resilience-in-developing-countries
[25] Libya Observer, "Libya makes strides in cybersecurity," 2024. [Online]. Available: https://libyaobserver.ly/tech/libya-makes-strides-cybersecurity
[26] Freedom House, *Libya: Freedom on the Net 2024*, 2024. [Online]. Available: https://freedomhouse.org/country/libya/freedom-net/2024
[27] United Nations Office on Drugs and Crime (UNODC), *Cybercrime and the Outgrowing Impact on Developing Nations*, 2024. [Online]. Available: https://en.unav.edu/web/global-affairs/cybercrime-and-the-outgrowing-impact-on-developing-nations.-costa-rica-in-the-background