Assessing Entrepreneurial Cyber-Fragility in Algerian AI-Driven Startups

Abdelnacer Ben Abderrezak*[1] and Abderezzak Benzaoui[2] and Safia Khalaf [3] and Imane Namoune[4]

[1]Department of English language and literature, Mohamed khider University - Biskra , Algeria, EROSS laboratory - Dublin University

* a.benabderrazek@univ-biskra.dz

[2]Department of economics, management and commerce, Mohamed khider University - Biskra Algeria,

Abderezzak.Benzaoui@univ-biskra.dz

[3]Institute of Sociology, University Center of Barika, Laboratory: الديناميكيات الاجتماعية في الاوراس Amdoukal Road, Barika, 05001, Algeria.

safia.khalaf@cu-barika.dz

[4]Department of economics, management and commerce, Mohamed khider University - Biskra Algeria.

imane.namoune@univ-biskra.dz

Abstract. This study aims at examining the emerging ecosystem of Algerian AI-driven startups. This sector is rapidly innovating, yet it is exposed to sophisticated digital threats. However, its development often outpaces robust cybersecurity frameworks. This fosters a condition termed entrepreneurial cyber-fragility. The study adopts a quantitative survey-based approach administered to business incubators across Algeria including: startup founders, cybersecurity experts, and ecosystem stakeholders. It mainly assesses the overlapping dimensions of cyber-fragility in Algerian AI-driven startups to explore systemic factors contributing to this vulnerability. Findings illuminate critical areas of weakness and resilience and offer insights into the way(s) Algerian AI-driven startups navigate the complexities of entrepreneurial cyber-fragility.

Keywords: Algerian AI-driven Startups, Business Incubators, Cyber-Fragility, Cybersecurity, Entrepreneurship

1 Introduction

The global economy is currently undergoing significant reconfiguration driven by the rapid proliferation of Artificial Intelligence (AI) as a transformative technological paradigm [1], [2]. This technological ascent cultivates an environment conducive to exceptional innovation within the entrepreneurial domain. Startups, by their inherent nature, are characterized by their propensity to challenge established market structures. They leverage cutting-edge technologies to secure a distinct competitive advantage [3], [4].

D. Agti et al. (eds.), *Proceedings of the International Conference on Artificial Intelligence Applications in Business Administration in MENA Region (ICAIABA 2026)*, Advances in Economics, Business and Management Research 393,

https://doi.org/10.2991/978-94-6239-711-8_23

In emerging economies, exemplified by Algeria, the growing proliferation of Artificial Intelligence (AI)-driven startups signifies a pivotal juncture for fostering economic diversification and sustainable growth. These ventures offer promising avenues for augmenting productivity, pioneering novel service provisions, and stimulating job creation [5]. However, (AI)-driven startups progressively rely on digital interconnectedness. Therefore, they are exposed to a complex spectrum of cyber risks. Within this context, cyber-fragility assumes particular salience. Such fragility poses a significant existential threat to the foundational stability and long-term viability of these entrepreneurial endeavors [6].

The Algerian entrepreneurial ecosystem operates within a complex matrix of geopolitical and socio-economic variables. The exposure to these conditions amplifies its cyber vulnerabilities. It encounters significant impediments in establishing strong cybersecurity infrastructures. These challenges span the development of comprehensive regulatory frameworks, the cultivation of a skilled human capital pool, and the implementation of advanced technological safeguards [7].

For emerging AI-driven enterprises within this ecosystem, the insidious vulnerabilities are further compounded by the inherent complexities intrinsic to AI technologies themselves. Such complexities encompass critical concerns including data privacy infringements, the propagation of algorithmic biases, the pervasive threat of intellectual property theft [8]. Consequently, the imperative to mitigate entrepreneurial cyber-fragility transcends mere technical exigency; it constitutes a strategic cornerstone for safeguarding the digital economic future of Algeria.

This study undertakes an assessment of entrepreneurial cyber-fragility within Algerian AI-driven startups. It endeavors to systematically identify key vulnerabilities and ascertain their potential ramifications for startup resilience and long-term sustainability. Furthermore, a primary objective is the formulation of actionable insights and strategic recommendations aimed at fostering a cyber-resilient entrepreneurial environment across Algeria. This investigation contributes to both the academic discourse concerning cybersecurity in emerging markets and the practical development of informed policy for supporting technology-driven economic advancement.

2 Literature Review

Entrepreneurial ecosystems within emergent economies often contend with inherent vulnerabilities. Algerian AI-Driven Startups grapple with significant deficiencies in establishing comprehensive cybersecurity infrastructures. They operate amidst unique geopolitical and socio-economic conditions coupled with specific infrastructural constraints and an evolving regulatory environment [9], [7].

Several foundational studies have explored various facets of cybersecurity that inform the present investigation into entrepreneurial cyber-fragility. [10] investigated the impact of information security awareness on employee compliance. It utilizes a survey-based methodology to collect data from employees across various organizations. Their findings highlighted a direct correlation between increased awareness and the adherence to security policies. The study illuminated novel strategies to reduce insidious threats and non/human-factor vulnerabilities.

[11] developed an analytical model to determine optimal investments in cybersecurity. Their research employed a theoretical approach and concluded that the level of cybersecurity investment should be proportional to the potential loss from a breach and the effectiveness of the security measure. They provide a framework for organizational preparedness and governance.

[12] examined the cybersecurity milieu in developing countries. He employed a comparative analysis of national policies, technological infrastructure, and threat environments. His work revealed that fragmented regulatory frameworks and a lack of skilled professionals significantly contribute to heightened cyber risks. The study highlights the critical influence of cybersecurity and regulatory environment on overall national cybersecurity maturity.

A significant research gap persists, as existing studies did not offer an integrated framework specifically addressing the multi-dimensional nature of entrepreneurial cyber-fragility (ECF) within the unique context of AI-driven startups in an emerging economy such as Algeria. Prior research often analyzes relevant factors in isolation or within generalized contexts. This oversight leads to a critical gap; it neglects the interconnected vulnerabilities arising from the combination of AI technologies, unique human and organizational behaviors, and cybersecurity conditions present in these environments.

3 Methodology

3.1 Study Population and Sample

The study population consists of Algerian AI-driven startups. They are defined as promising enterprises extensively relying on AI technologies for their products and services. These firms face heightened cyber risks due to their organizational immaturity and significant digital infrastructure dependence. A purposive sampling method specifically targeted founders, managers, and IT/cybersecurity specialists owing to their comprehensive knowledge of strategic and technical cybersecurity aspects. The final sample of 60 valid responses (N=60) was deemed appropriate for exploratory research within emerging entrepreneurial ecosystems. Algerian AI-driven startups are cyber-fragile. They possess limited resources and often lack formal security policies. Their heavy reliance on AI systems further exacerbates this fragility due to a shortage of specialized cybersecurity competencies.

Although the sample size is relatively modest (N = 60), it is considered adequate for exploratory research in emerging entrepreneurial ecosystems where access to specialized respondents remains limited. The purposive selection of knowledgeable stakeholders ensures the collection of relevant and information-rich data.

Purposive sampling enabled the selection of knowledgeable respondents; however, this method introduces potential selection bias. Therefore, the generalization of the findings is interpreted with caution.

3.2 Study Variables and Measurement Axes

The study's model is predicated on one dependent variable and five independent variables. They are derived from the cybersecurity and entrepreneurship literature. The dependent variable represents the level of Cyber-Fragility (CF). It reflects the degree to which AI-driven startups are exposed to cyber threats, their insufficient preparedness to confront these threats and their susceptibility to digital breaches such as data leakage or system disruptions.

The independent variables are defined as follows:

Cybersecurity Awareness (AW): measures the level of knowledge, training, and awareness regarding cyber risks and secure digital practices within the company.

Exposure to Cyber Threats (TH): reflects the frequency and severity of cyberattacks encountered by companies such as: phishing, malware, and ransomware attacks.

Data Protection Practices (DP): refers to the technical and organizational measures adopted to protect sensitive data such as: encryption, access control, and backup procedures.

Cyber-Defense Strategies (DEF): represents proactive and reactive measures including: intrusion detection systems, incident response plans and continuous monitoring.

Security Challenges (CH): encompasses internal and external limitations such as: resource scarcity, lack of competencies, complexity of regulatory frameworks, and technological uncertainty.

These axes were selected because they represent the human, technical, organizational, and environmental dimensions of cybersecurity, which are fundamental in the context of AI-driven startups.

Figure 1. illustrates the conceptual framework of the study. It presents the relationships between cybersecurity-related factors and cyber vulnerability in Algerian AI-driven startups.

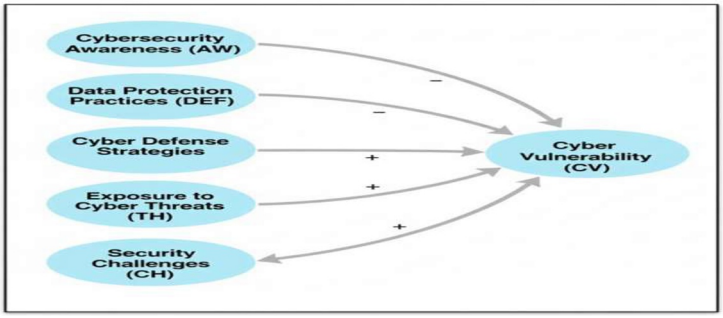

Figure 1. Conceptual Model of Entrepreneurial Cyber-Fragility
Source: Author's own work

3.3 Descriptive Statistics of the Sample

Table 1. Demographic characteristics of respondents

Variable	Category	Frequency	Percentage (%)
Gender	Male	38	63.3
	Female	22	36.7
Age	20–30 years	24	40.0
	30–40 years	29	48.3
	Above 40 years	7	11.7
Education Level	Master'sdegree	18	30.0
	PhD	42	70.0
Job Title	Founder	41	68.3
	Manager	11	18.3
	IT / CybersecuritySpecialist	8	13.4
Firm Age	Lessthan 1 year	21	35.0
	1–3 years	29	48.3
	More than 3 years	10	16.7
Number of Employees	1–5 employees	46	76.7
	More than 5 employees	14	23.3
Level of AI Dependency	Medium	27	45.0
	High	20	33.3
	Very High	13	21.7

Source: Authors' calculation based on survey data (2026).

The analysis of demographic data reveals that the sample predominantly comprises startup founders possessing advanced academic qualifications, notably at the doctoral level. The majority of these ventures are recently established. They are characterized by a lack of experience, limited workforce and demonstrate a moderate to high reliance on Artificial Intelligence technologies. This profile collectively indicates a vulnerable organizational and technological milieu (see table 1).

3.4 Mean Scores and Standard Deviations

Table 2. Descriptive statistics of study variables

Construct	Code	Mean	Standard Deviation	Evaluation Level
CybersecurityAwareness	AW	3.94	0.62	High
Exposure to Cyber Threats	TH	3.67	0.71	Moderate–High
Data Protection Practices	DP	3.21	0.68	Moderate
Cyber DefenseStrategies	DEF	2.89	0.74	Low
Security Challenges	CH	4.02	0.59	High

Cyber Vulnerability	CV	3.58	0.66	Relatively High

Source: Authors' calculation based on survey data (2026).

The results indicate a high level of cybersecurity awareness among respondents; however, cyber defense strategies exhibit comparative weakness. This suggests a discernible chasm between knowledge acquisition and practical implementation. Furthermore, the substantial security challenges encountered coupled with significant threat exposure. It elucidates the relatively elevated degree of cyber vulnerability (see table 2).

3.5 Reliability Test (Cronbach's Alpha)

Table 3. Reliability analysis using Cronbach's Alpha

Construct	Number of Items	Cronbach's Alpha
Cybersecurity Awareness (AW)	5	0.82
Cyber Threats (TH)	5	0.79
Data Protection Practices (DP)	5	0.76
Cyber Defense Strategies (DEF)	5	0.73

Source: Authors' calculation based on survey data (2026).

The computed Cronbach's Alpha coefficients demonstrate strong internal consistency across all constructs within the measurement instrument, with all values surpassing the generally accepted threshold of 0.70. This confirms the satisfactory reliability and constructs validity of the instrument for the present study.

In addition to reliability, the validity of the measurement instrument is supported by grounding the questionnaire items in established cybersecurity and entrepreneurship literature. This theoretical basis reinforces the construct validity of the study variables (see table 3).

3.6 Correlation Analysis

Table 4. Correlation coefficients with cyber-fragility

Variable	AW	TH	DP	DEF	CH	CV
AW	1	-0.41**	0.52**	0.58**	-0.36**	-0.48**
TH	-0.41**	1	-0.39**	-0.44**	0.55**	0.56**
DP	0.52**	-0.39**	1	0.63**	-0.33**	-0.42**
DEF	0.58**	-0.44**	0.63**	1	-0.40**	-0.61**
CH	-0.36**	0.55**	-0.33**	-0.40**	1	0.59**
CV	-0.48**	0.56**	-0.42**	-0.61**	0.59**	

Source: Authors' calculation based on survey data (2026).

Note: Correlation is significant at the 0.01 level (2-tailed)

The analysis reveals statistically significant correlations between the independent variables and cyber vulnerability. Specifically, cyber vulnerability demonstrates a negative correlation with cybersecurity awareness, data protection practices, and cyber-defense strategies. Equally, a positive association is observed between cyber vulnerability and both threat exposure and security challenges (see table 4).

Table 5. Regression results

Independent Variable	Beta (β)	t-value	Sig
AW (CybersecurityAwareness)	-0.21	-2.34	0.022
TH (Exposure to Threats)	0.29	3.11	0.003
DP (Data Protection Practices)	-0.18	-2.01	0.048
DEF (Cyber DefenseStrategies)	-0.35	-4.26	0.000

Source: Authors' calculation based on survey data (2026).

$$R^2 = 0.62$$
$$F = 17.84 \text{ (Sig} = 0.000)$$

The multiple regression analysis indicates that the model accounts for 62% of the variance observed in cyber vulnerability ($R^2 = 0.62$). Notably, cyber defense strategies exert the most substantial negative influence. They, thereby, underscore their critical role in mitigating cyber vulnerability within AI-driven startups (see table 5).

4 Discussion

The findings reveal that Algerian AI-driven startups exhibit a notable level of cyber vulnerability (M = 3.58). This phenomenon is observed despite a comparatively high degree of cybersecurity awareness among personnel (M = 3.94). This apparent paradox highlights a prevalent challenge within emerging entrepreneurial ventures, where heightened awareness does not invariably translate into the adoption of effective security practices and vigorous defensive strategies.

Correlation analysis further elucidates significant interrelationships between the independent variables and cyber vulnerability. Specifically, Cyber Defense Strategies (DEF) evinced the strongest negative correlation with vulnerability (r = -0.61). This suggests that the implementation of vigorous defense mechanisms is inversely proportional to exposure to cyber risks. At the same time as, Cybersecurity Awareness (AW) and Data Protection Practices (DP) demonstrate negative associations with vulnerability, while Exposure to Threats (TH) and Security Challenges (CH) exhibit positive correlations. This indicates that elevated threat frequencies and organizational impediments amplify vulnerability.

The multiple regression analysis corroborates these findings. It establishes that Cyber Defense Strategies (DEF) exert the most significant negative impact on cyber vulnerability (Beta = -0.35, $p< 0.001$). Conversely, Exposure to Threats (TH) presented a positive effect (Beta = 0.29, $p< 0.01$). This contributes to increased vulnerability. Cybersecurity Awareness (AW) and Data Protection Practices (DP) also contribute to vulnerability reduction, albeit with comparatively smaller effect sizes (Beta = -0.21, $p< 0.05$ and Beta = -0.18, $p< 0.05$, respectively). The model collectively account for 62% of the variance in cyber vulnerability ($R^2 = 0.62$). This signifies substantial explanatory power of these factors in comprehending cyber risks within AI-driven startups.

These findings emphasize that mere cybersecurity awareness is insufficient; startups must actively implement tangible defense mechanisms, establish unequivocal data protection protocols, and proactively manage cyber threats to effectively mitigate vulnerability. This aligns with extant research within the Algerian context, which posits that small and emergent technology enterprises are particularly susceptible to cyber risks owing to resource constraints, inadequate security infrastructure, and pronounced reliance on digital technologies. In conclusion, this study accentuates the pivotal role of cyber defense strategies in reducing vulnerability and demonstrates that a holistic approach integrating awareness, protective practices, and threat monitoring constitutes a comprehensive framework for cybersecurity management in AI-driven startups.

Despite its contributions, the present study has certain limitations. The relatively modest sample size and the use of purposive sampling may limit the generalization of the findings. In addition, the study relies on self-reported survey data, which reflect respondents' perceptions rather than objective cybersecurity performance.

These findings are consistent with previous research addressing cybersecurity challenges in developing economies. [12] emphasizes that organizations operating in emerging digital environments often face structural limitations that hinder the effective implementation of cybersecurity measures. Similarly, [7] highlight those limited resources and insufficient technological infrastructure increase organizational exposure to cyber risks. The present study confirms these observations within the context of Algerian AI-driven startups.

5 Conclusion & Recommendations

This study provides empirical evidence concerning the level of cyber vulnerability in Algerian AI-driven startups. It elucidates the pivotal factors influencing this susceptibility. Despite a commendable level of cybersecurity awareness among employees, findings indicate that inadequate cyber defense strategies and suboptimal data protection practices contribute significantly to organizational vulnerability. This precarious situation is further exacerbated by prevalent exposure to cyber threats and the existence of inherent security challenges.

Both regression and correlation analyses consistently highlight that Cyber Defense Strategies (DEF) exert the most substantial impact on mitigating cyber vulnerability. On the other hand, Exposure to Threats (TH) and Security Challenges (CH) increase vulnerability. While Cybersecurity Awareness (AW) and Data Protection Practices

(DP) also contribute meaningfully to vulnerability reduction, their impact is comparatively less pronounced. The explanatory power of the model, accounting for 62% of the variance in cyber vulnerability ($R^2 = 0.62$), affirms the robustness and germane nature of the selected variables in this context. These results highlight that enhancing cybersecurity within AI-driven startups necessitates transcending mere awareness; it mandates the implementation of practical, systemic security measures. Awareness alone is insufficient to effectively mitigate risks within environments characterized by resource limitations and intensive digital operations.

Based on the empirical findings, the following recommendations are proffered for practitioners, policymakers, and researchers:

Strengthen Cyber Defense Strategies:

- Prioritize investment in advanced cybersecurity tools and comprehensive frameworks.
- Develop explicit and actionable defense protocols specifically tailored for startups.
- Implement regular updating and rigorous testing of defense mechanisms to counter evolving cyber threats.

Enhance Data Protection Practices:

- Establish formal data protection policies and rigorously enforce compliance across the organization.
- Provide comprehensive training to employees on secure data handling and robust storage procedures.
- Effectively utilize encryption, stringent access control, and continuous monitoring systems to safeguard sensitive information.

Cultivate Awareness and Training:

- Conduct continuous cybersecurity awareness programs specifically designed to address AI-related risks.
- Foster a proactive culture of threat detection and reporting among all employees.

Address Organizational Challenges:

- Provide targeted technical and financial support to overcome existing infrastructural limitations.
- Facilitate knowledge sharing and collaborative platforms among startups to promote the adoption of best practices.
- Encourage strategic collaboration with cybersecurity experts and external consultants to bolster internal capabilities.

Implement Policy and Regulatory Support:

- Governmental and industry bodies should establish clear guidelines for AI-driven startups to ensure adherence to baseline security standards.
- Incentivize startups to adopt comprehensive cybersecurity measures through mechanisms such as grants, specialized training programs, or industry recognition.

Acknowledgments. The authors express their sincere gratitude to Mohamed Khider University of Biskra, the University Center of Barika, and the EROSS Laboratory for their institutional support.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

[1] D. Leslie et al., "'Frontier AI,' Power, and the Public Interest: Who Benefits, Who Decides?" Harvard Data Sci. Rev., Special Issue 5, 2024. [Online]. Available: https://doi.org/10.1162/99608f92.4a42495c
[2] T. Yigitcanlar et al., "Responsible Urban Innovation with Local Government Artificial Intelligence (AI): A Conceptual Framework and Research Agenda," J. Open Innov. Technol. Market Complex., vol. 7, no. 1, 2021. [Online]. Available: https://doi.org/10.3390/joitmc7010071
[3] C. M. Christensen, The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail. Boston, MA: Harvard Business Review Press, 2016.
[4] S. Shane, A General Theory of Entrepreneurship: The Individual-Opportunity Nexus. Cheltenham, UK: Edward Elgar Publishing, 2003.
[5] S. M. M. Mirahmadi, M. Jahanbakht, and M. H. Rohban, "Mitigating Entrepreneurship Policy Challenges in Developing Countries' Startup Ecosystems Through Machine Learning Analysis," Economies, vol. 13, no. 10, 2025. [Online]. Available: https://doi.org/10.3390/economies13100295
[6] OECD, Harnessing AI in Finance for Financial Inclusion in Africa: Africa Capital Markets Report 2025. Paris, France: OECD Publishing, 2025. [Online]. Available: https://doi.org/10.1787/7d26e1d3-en
[7] M. I. Mutar and K. Al-Ghathian, "Cybersecurity challenges in developing countries: A review," Int. J. Comput. Sci. Netw. Secur., vol. 17, no. 3, pp. 108–115, 2017.
[8] C. O'Neil, Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. New York, NY: Crown, 2016.
[9] M. A. Boutabba, "The entrepreneurial ecosystem in Algeria: A developing country perspective," Int. J. Entrepreneurship Small Business, vol. 35, no. 2, pp. 173–195, 2018.
[10] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of organizational fairness and trust," Decis. Support Syst., vol. 46, no. 4, pp. 939–952, 2009.
[11] L. A. Gordon and M. P. Loeb, "The economics of information security investment," ACM Trans. Inf. Syst. Secur., vol. 5, no. 4, pp. 438–457, 2002.
[12] N. Kshetri, "Cybersecurity in developing countries," IEEE Security Privacy, vol. 16, no. 3, pp. 88–92, 2018