ADISI - CAMEROUN

ifex

# STUDY REPORT ON THE STATE OF DIGITAL SECURITY AND GENDER DYNAMICS IN THE MEDIA AND CIVIL SOCIETY ORGANIZATIONS IN CAMEROON

2025

# STUDY REPORT ON THE STATE OF DIGITAL SECURITY AND GENDER DYNAMICS IN THE MEDIA AND CIVIL SOCIETY ORGANIZATIONS IN CAMEROON

# TABLE OF CONTENTS



STUDY REPORT ON THE STATE OF DIGITAL SECURITY AND GENDER DYNAMICS IN THE MEDIA AND CIVIL SOCIETY ORGANIZATIONS IN CAMEROON

# Executive Summary

This study, commissioned by ADISI-Cameroon, assesses the state of digital security and its gendered implications within the media and civil society organizations (CSOs) in Cameroon. It aims to provide a detailed understanding of the institutional preparation, policy frameworks, and concrete protection mechanisms structuring the digital universe in the run-up to the 2025 elections, with a strong focus on the inclusion of women.

The analysis is based on data from 101 organizations across five regions, covering both English-speaking (45%) and French-speaking (55%) areas. Data collection was carried out using structured questionnaires, administered in person and remotely by trained interviewers, via KoboToolbox, to ensure reliability, anonymity, and contextual adaptation. These questionnaires targeted a wide range of profiles (managers, IT staff, journalists, gender officers, etc.), reflecting varied experiences in urban, peri-urban, and conflict-affected settings.

## Main vulnerabilities identified:

53% of organizations do not have formal digital security policies, and only 42% offer regular cybersecurity training, often ad hoc and reserved for technical staff.

- Only 39% carry out digital security audits, leaving many organizations ill-prepared for growing cyber threats (phishing, ransomware, politically motivated attacks).

Less than 35% feel prepared to deal with digital threats related to elections, despite the rise in disinformation risks during election cycles.

While 67% report providing equal access to digital training, less than 20% of decision-making positions in digital security are held by women, reflecting a significant gender gap in participation.

The study also highlights capacity challenges: 62% of organizations have no dedicated budget for digital security, and less than 25% actively collaborate with cybersecurity experts or relevant public institutions. The Northwest and Southwest regions, particularly affected by conflict, also suffer from a lack of secure communication tools and increased surveillance risks.

The report concludes with context-specific operational recommendations: institutionalize digital security policies, provide gender- and role-sensitive training, encourage multi-stakeholder collaboration, and integrate digital risk assessments into internal processes.

Ultimately, this data-driven research offers a strategic roadmap for building a safer, more inclusive, and resilient civic and media ecosystem in Cameroon, where digital rights and security are guaranteed for all.

# INTRODUCTION

ADISI-Cameroon, a non-profit organization dedicated to transparency, citizen participation, and digital rights in Cameroon, launched this study in partnership with IFEX as part of its overall mission to strengthen governance and democratic resilience through inclusive digital transformation. Recognizing the central role of media and civil society actors in accountability and public dialogue, the study was designed to critically assess the intersection between digital security and gender dynamics in these key sectors.

Cameroon is undergoing a major digital transformation: Internet penetration has increased from around 6% in 2010 to over 35% in 2023 [1](Internet World Stats, 2023), and the number of mobile subscriptions now exceeds 22 million (GSMA, 2023). This growth has fostered civic engagement, media pluralism, and social advocacy. However, it has also brought with it a range of digital threats: in 2022 alone, over 3,800 cases of cybercrime were recorded [2](Minpostel, 2023), including ransomware attacks, phishing attempts, disinformation campaigns, and politically motivated hacks.

These threats are not distributed evenly: urban areas such as Yaoundé and Douala benefit from more robust infrastructure and technical support, while organizations in conflict-affected regions—particularly the Northwest and Southwest—experience increased vulnerabilities (insecurity, surveillance, poor connectivity).

Adding to these challenges are systemic gender inequalities. While the share of women in media and civil society organizations is increasing, their involvement in ICT governance and digital security policymaking remains low. According to [3]UN Women, only 17% of ICT-related decision-making positions in sub-Saharan Africa are held by women (UN Women, 2022). The study confirms this gap: less than 20% of respondents involved in the digital security of organizations identify as women.

*1) Internet World Stats. (2023). Report on Internet usage and telecommunications in Cameroon. Available at: https://www.internetworldstats.com*
*2) Ministry of Posts and Telecommunications (Minpostel), Cameroon. (2023). Cybersecurity incident reports.*
*3) UN Women. (2022). Gender and ICT in Sub-Saharan Africa. Available at: https://www.unwomen.org*

# GOALS

## ASSESS INSTITUTIONAL READINESS

Verify the existence of formal digital security policies, audits and trained personnel.
Measure response capacity to threats such as phishing, malware and data breaches.

### ANALYZING GENDER DYNAMICS IN DIGITAL ENGAGEMENT

Study women's participation in digital access, training and decision-making.

- Identify structural or cultural barriers to inclusive leadership.

## REVIEW CURRENT DIGITAL SECURITY PRACTICES

Review policies, training and protocols in place.

- Evaluate their scope, frequency and effectiveness in the field.

## IDENTIFY KEY OBSTACLES

Highlight budgetary constraints, infrastructure weaknesses, low digital literacy and lack of external support.
Understanding gender and regional specific challenges.

## DEVELOP OPERATIONAL RECOMMENDATIONS

Propose concrete, data-driven actions, adapted to organizational realities.

- Encourage digital resilience, gender equity and multi-stakeholder collaboration.

# METHODOLOGY

Data for this study were collected using a mixed-methods approach, integrating quantitative and qualitative elements to provide a rich and contextualized understanding of digital security and gender dynamics.

## REGIONAL COVERAGE

Structured questionnaires were administered in five major regions: Centre, Littoral, Southwest, Northwest and West. This geographical distribution was designed to reflect Cameroon's linguistic, regional and infrastructural diversity.

## SAMPLING STRATEGY

The sample was deliberately selected to ensure representation from English- and French-speaking areas, as well as urban and peri-urban organizations. A balance was sought between media and CSOs, taking into account the size, scope of action and digital exposure of each entity.

## PROFILE OF RESPONDENTS

Participants included organizational leaders (coordinators, directors), technical staff (IT specialists), journalists, monitoring and evaluation officers, and gender officers. Gender parity was prioritized in the selection of respondents to ensure an inclusive view of digital practices.

In addition to structured surveys, the study used the following tools and processes:

**KoboToolbox for administering questionnaires, in online and offline modes depending on the availability of the Internet in each region.**

**A questionnaire combining multiple-choice questions, Likert scales, and open-ended questions to collect measurable and descriptive data.**

**Training of investigators on:**

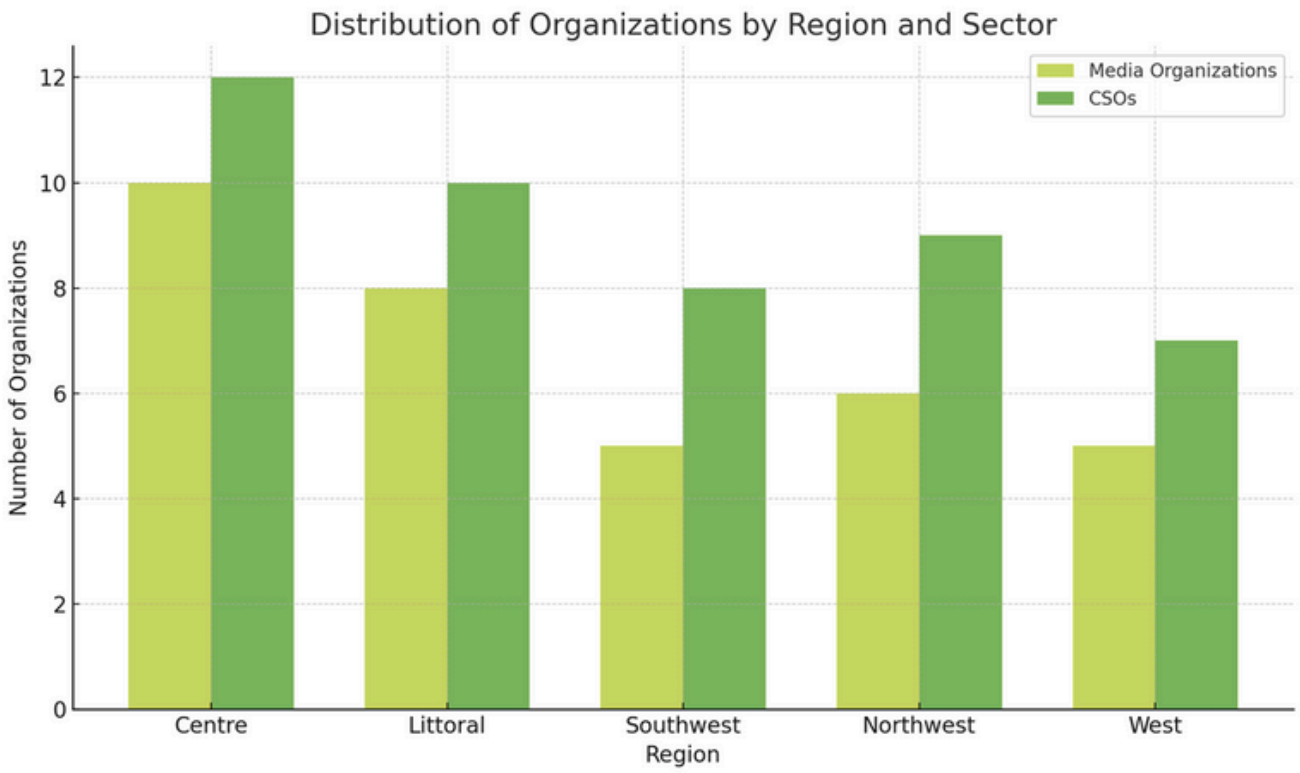
- **- Ethical considerations and informed consent**
  **- Gender sensitivity in research**
  **- Secure management of digital data and devices**

**All data were anonymized, in accordance with ethical research standards. To enhance reliability, triangulation was applied: cross-checking qualitative elements and identifying convergences or anomalies in digital behaviors and perceptions across regions and types of organizations.**

# RESPONDENTS PROFILE

**Total number of organizations:** 101
**Type of organization:** Civil society organizations: approximately 66%
**Media:** approximately 34%
**Geographic distribution:**
**English-speaking regions:** approximately 45%
**French-speaking regions:** approximately 55%
**Respondents' roles:** Coordinators, Directors, Journalists, Gender Officers, Monitoring and Evaluation Officers, among others.

**Figure 0: Distribution of organizations by region and sector Graph comparing the number of media organizations and civil society organizations (CSOs) in five regions of Cameroon (Center, Littoral, Southwest, Northwest and West).**




*Source: ADISI-Cameroun*

# MAIN CONCLUSIONS

## Digital landscape

The study shows that digital security remains an underdeveloped area in a significant number of civil society organizations and media institutions in Cameroon. Despite the increasing digitalization of operations, many organizations lack structured frameworks and investments to protect their systems.

- Only 47% of surveyed organizations report having formal digital security policies. These are often limited in scope and are not always implemented or updated regularly.

42% of organizations offer regular cybersecurity training. However, these trainings are often one-off and reserved for technical staff, excluding journalists, program managers, and administrators who frequently use digital tools.

39% of organizations conduct regular system security audits, which demonstrates a moderate level of risk assessment practices, but reveals a significant gap in institutional preparedness.

The most commonly used tools are antivirus software, basic firewalls, and periodic system updates. These measures remain fundamental but are insufficient in the face of modern cyber threats.

Adoption of advanced security protocols—end-to-end encryption, secure cloud storage, virtual private networks (VPNs), and multifactor authentication—remains limited. Many organizations cite a lack of technical capacity, funding, or awareness as reasons for this lack of adoption.

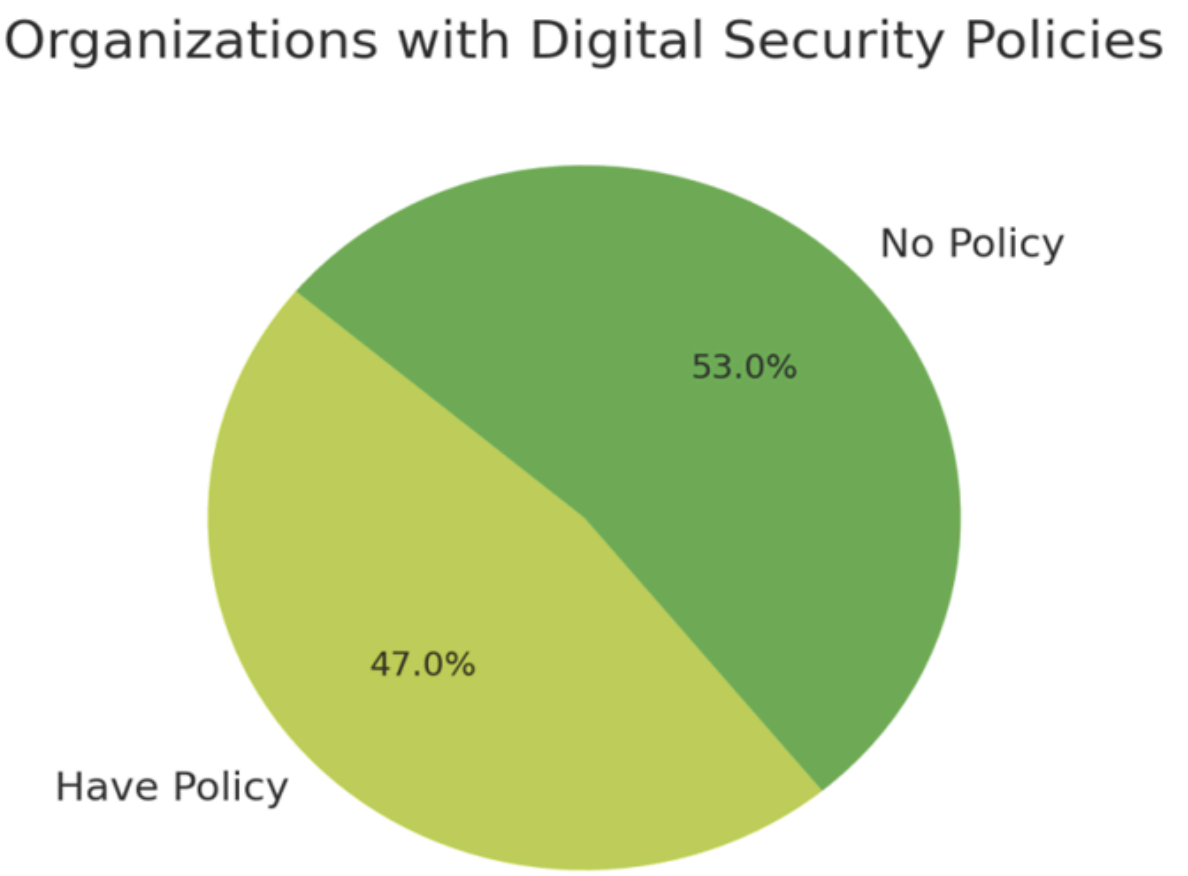
Overall, these findings illustrate a fragmented and reactive approach to digital security, which leaves many organizations vulnerable to intrusions, misinformation, and data loss, particularly in the context of increased surveillance and cyberattacks during sensitive periods such as elections.

- The lack of robust security frameworks leaves organizations vulnerable to manipulation of sensitive data, which is especially concerning during election cycles, when civil society and the media play a key role in accountability.

In such circumstances, the absence of incident response protocols, secure communication channels, or data integrity guarantees can allow malicious actors to disrupt democratic processes through disinformation, unauthorized access, or targeted attacks against institutions considered critical voices.

This systemic underinvestment in digital infrastructure poses a direct threat not only to operational continuity, but also to the integrity of civic engagement and electoral transparency in Cameroon.

***Figure 1: Graph showing the number of organizations by percentage that have or do not have a digital security policy***




*Source: ADISI-Cameroun*

# Gender dynamics

The study reveals complex and persistent gender disparities in digital security engagement, both within CSOs and the media.

Although 67% of respondents report that men and women have equal access to training, qualitative responses and further disaggregation show that this access often does not translate into equal participation in decisions or leadership positions related to digital security.

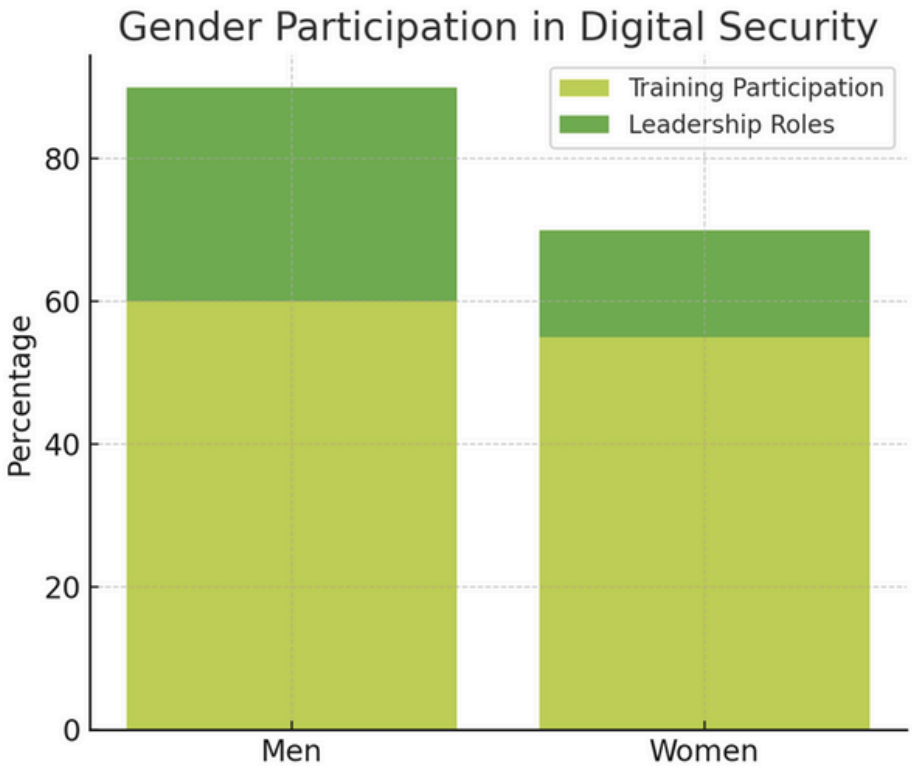
31% of organizations admit they do not actively involve women in digital security decisions. In some cases, they were not even consulted during the risk assessment or protocol development stages.

**Structural obstacles:**
**Low digital literacy among women, especially in rural organizations.**
**Organizational culture that perceives digital security as a technical (and therefore male-dominated) field.**
**Lack of representation of women in ICT functions or in incident response teams.**

**Personal and social obstacles:**
**Fear of online harassment and cyberbullying, discouraging women from engaging in technology or digital advocacy roles.**
**Limited access to secure devices or internet connection at home, especially for women with caregiving responsibilities.**
**Lack of gender-sensitive training materials and female trainers who can act as mentors or role models.**

**These findings suggest that until gender is deliberately integrated into digital security policies and practices, women will remain marginalized in this area. This has broader implications for organizational resilience, inclusivity, and human rights protection.**

***Figure 2: Gender participation in digital security Graph comparing the proportion of men and women participating in digital training versus those holding leadership positions related to cybersecurity.***




*Source: ADISI-Cameroun*

## Shortcomings of the study

The study highlighted significant capacity limitations that hinder the development and implementation of effective digital security measures within CSOs and media outlets.

**Budgetary constraints: 62% of organizations report not having a dedicated budget for digital security. In many cases, it is not considered an operational priority, and any spending remains ad hoc and reactive rather than planned and strategic. This lack of financial commitment leaves systems vulnerable to evolving cyber threats.**

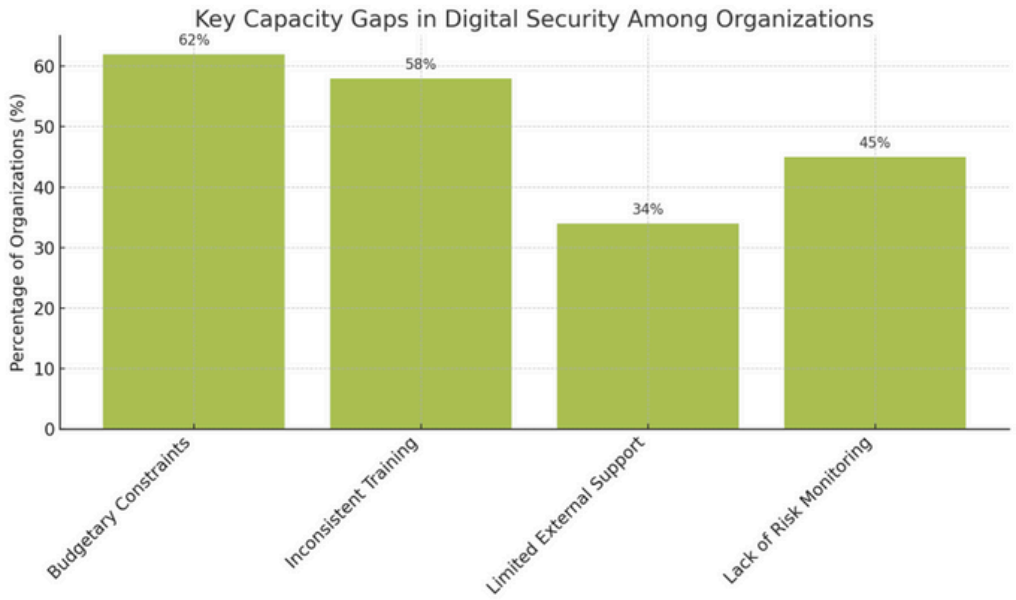
**Inconsistent training: Training efforts are sporadic and poorly integrated into organizational development plans. When organized, training primarily targets technical staff, often excluding program, administrative, or field staff—many of whom regularly handle sensitive data. Vulnerable groups, such as women and youth, are disproportionately excluded, reinforcing inequalities.**

- **Limited external support: Only a minority of organizations reliably collaborate with technical partners (cybersecurity companies, digital rights organizations, etc.). Most rely on non-specialized internal IT staff, who are not necessarily trained to deal with complex digital threats.**

**Lack of monitoring and auditing: Regular threat monitoring, digital audits, and risk assessments are rarely institutionalized. Organizations often ignore new threats or fail to document past incidents to learn from them. This lack of proactive posture reduces overall resilience.**

**These capacity gaps highlight the need for institutional reform, strategic investments and strengthened technical collaboration networks.**

***Figure 3: Key digital security capability gaps among organizations. Bar chart illustrating the percentage of organizations lacking formal policies, training programs, security audits, and advanced protection tools.***




*Source: ADISI-Cameroun*

# Election-related threats

The 2025 elections represent a critical test for the cybersecurity of media and civil society organizations (CSOs) in Cameroon. The study reveals that these actors remain dangerously unprepared for digital threats that are likely to intensify during the election period.

**Increase in disinformation and phishing threats:**
**More than 65% of respondents consider disinformation (fake news, doctored content, deepfakes), phishing emails and social engineering as their main concerns.**
**These threats are particularly virulent during election periods, as false narratives can quickly undermine public confidence or cause unrest.**

**Lack of incident response preparation and protocols:**
**Less than 35% of organizations report having protocols in place to handle politically motivated cyberattacks, such as fake news campaigns or digital harassment of activists and journalists.**
**Only a minority have conducted simulation exercises for electoral incidents (spikes in disinformation, targeted data leaks, etc.).**

**Regional and urban-rural disparities: Organizations based in Douala and Yaoundé are better prepared, thanks to access to ICT support, training and donor-funded programs.**

**On the other hand, those in the North West and South West suffer from cumulative vulnerabilities:**
**Insecurity limits the mobility and deployment of personnel.**
**Fear of surveillance and political reprisals is hampering digital engagement.**

- **Unstable internet access prevents real-time verification and digital hygiene campaigns.**

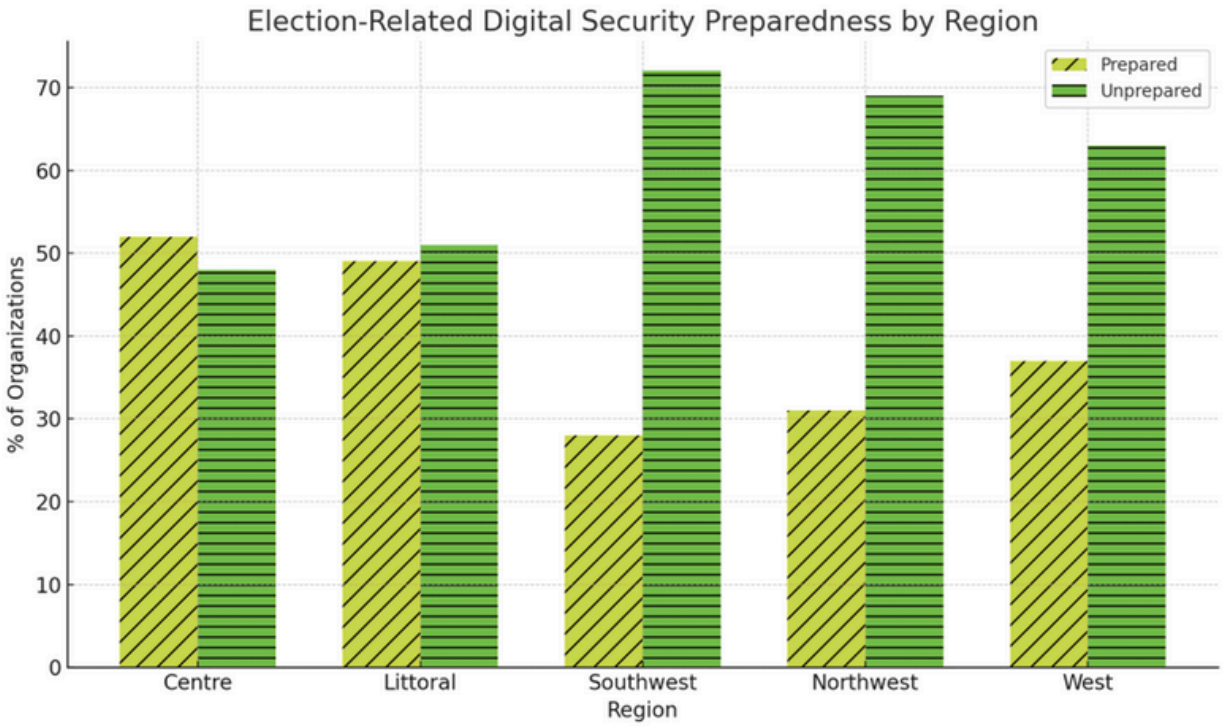
**Weak institutional collaboration:**
**Only 18% of respondents collaborate with state actors such as the National Agency for Information and Communication Technologies (ANTIC) or the National Electoral Commission (ELECAM).**
**Even fewer organizations work with fact-checking platforms or international observatories (Africa Check, Global Disinformation Index, etc.).**
**This isolation increases vulnerability to disinformation campaigns, coordinated trolling or online content removals during sensitive times.**

**Limited training and technical tools: Although some CSOs, such as Civic Watch, are active in civic education or civic tech initiatives, most lack the technical expertise to:**
**Detect manipulated media (deepfakes, etc.).**
**Establish secure voter engagement platforms.**
**Respond to distributed denial of service (DDoS) attacks targeting their sites or applications.**

**Missed Opportunities for Election Preparedness: The lack of rapid response teams, predefined escalation plans, and media monitoring systems leaves most organizations in a reactive rather than proactive position.**

**For example, Le Messager, despite its status as a leading media outlet, had not joined a collaborative fact-checking network nor developed internal strategies against electoral disinformation.**

***Figure 4: Regional comparison of preparedness for election-related digital threats.***




*Source: ADISI-Cameroun*

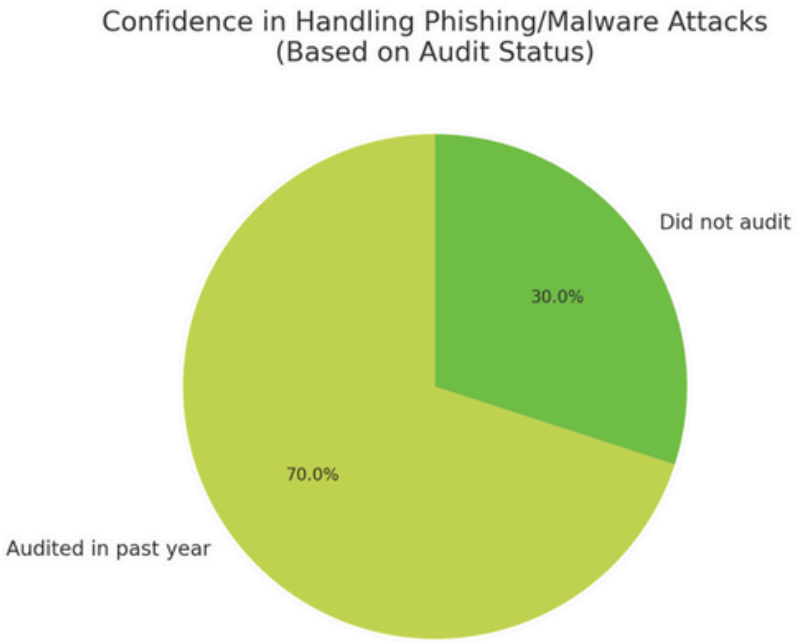
# MAIN LESSONS

The study highlights a strong correlation between institutional preparedness and exposure to cyber threats. Organizations with formalized digital security frameworks, consistent training programs, and regular audits demonstrate a significantly greater ability to detect, respond to, and prevent digital risks.

For example: More than 70% of organizations that have conducted an audit in the past year report being confident in responding to phishing or malware attacks.

Conversely, organizations without a structured framework report more system failures and disruptions related to disinformation.

***Figure 5: Confidence in handling phishing/malware attacks by audits. This graph compares the percentage of organizations reporting confidence in dealing with cyberattacks, based on whether or not they have conducted a digital security audit in the past 12 months.***



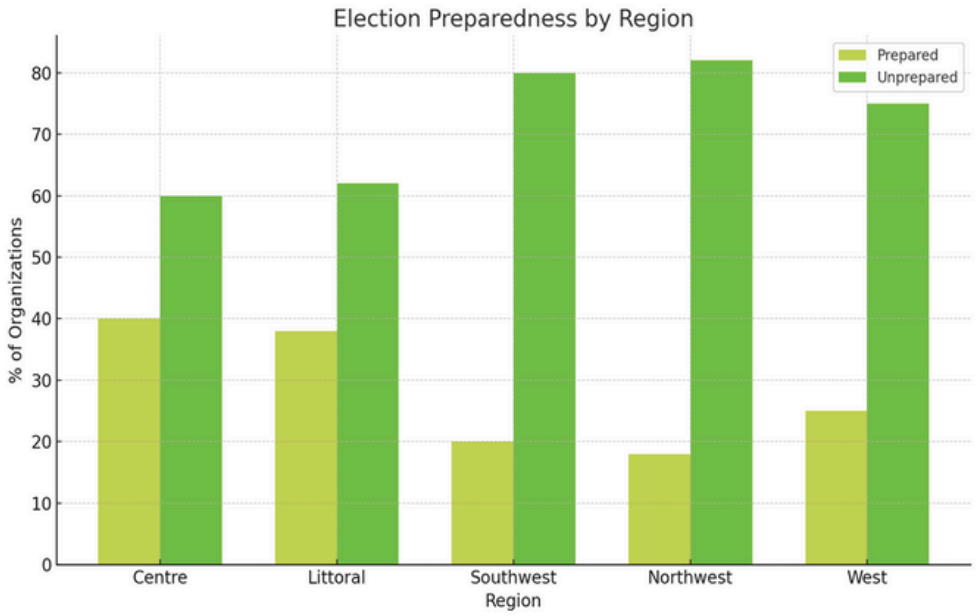

*Source: ADISI-Cameroun*

**Election-related vulnerabilities: Less than 35% of respondents feel prepared to manage digital threats during elections.**

**The returns indicate:**
**Concern about fake news and disinformation campaigns.**
**Vulnerability to social engineering attacks.**
**Weaknesses in the protection of websites and online platforms.**

**This highlights the need to:**
**Election-specific scenario planning.**
**Rapid response protocols.**
**Strengthened partnerships with digital observatories and fact-checking platforms.**

***Figure 6: Regional comparison of preparedness for digital threats related to elections.***




*Source: ADISI-Cameroun*

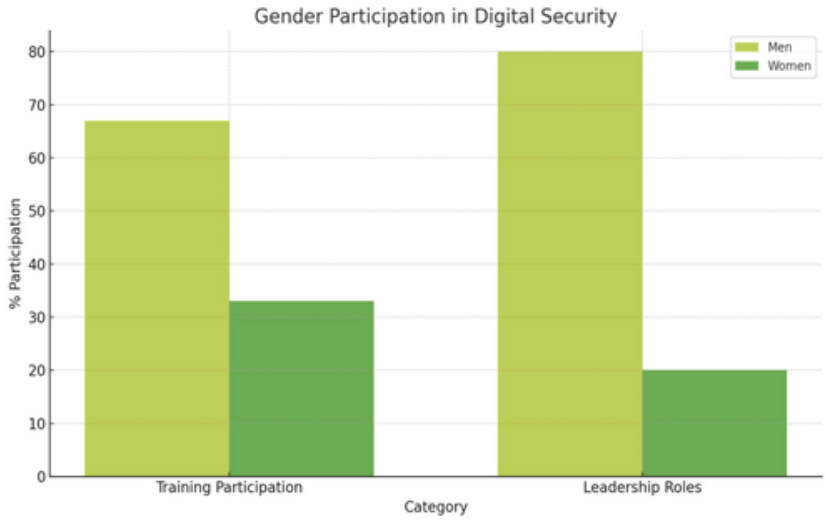
**Gender disparities in digital security: Although 67% of organizations report equal access to digital training, further analysis shows:**
**Less than 20% involve women in the design of security policies or systems.**

- **The main obstacles faced by women are:**

**Lack of mentoring in ICT functions.**
**Limited participation in decision-making bodies.**

- **Cultural and structural biases within organizations.**

***Figure 7: Women's Participation in Digital Security This graph illustrates the level of involvement of women in digital security within organizations, including in policy design, system administration and training programs.***




*Source: ADISI-Cameroun*

**Collaboration gaps: Internally, digital security is often confined to IT departments.**
**And external:**
**Less than 25% of organizations have active relationships with cybersecurity experts or government agencies.**

- **Respondents requested joint workshops, shared tools and regular status updates with their partners.**

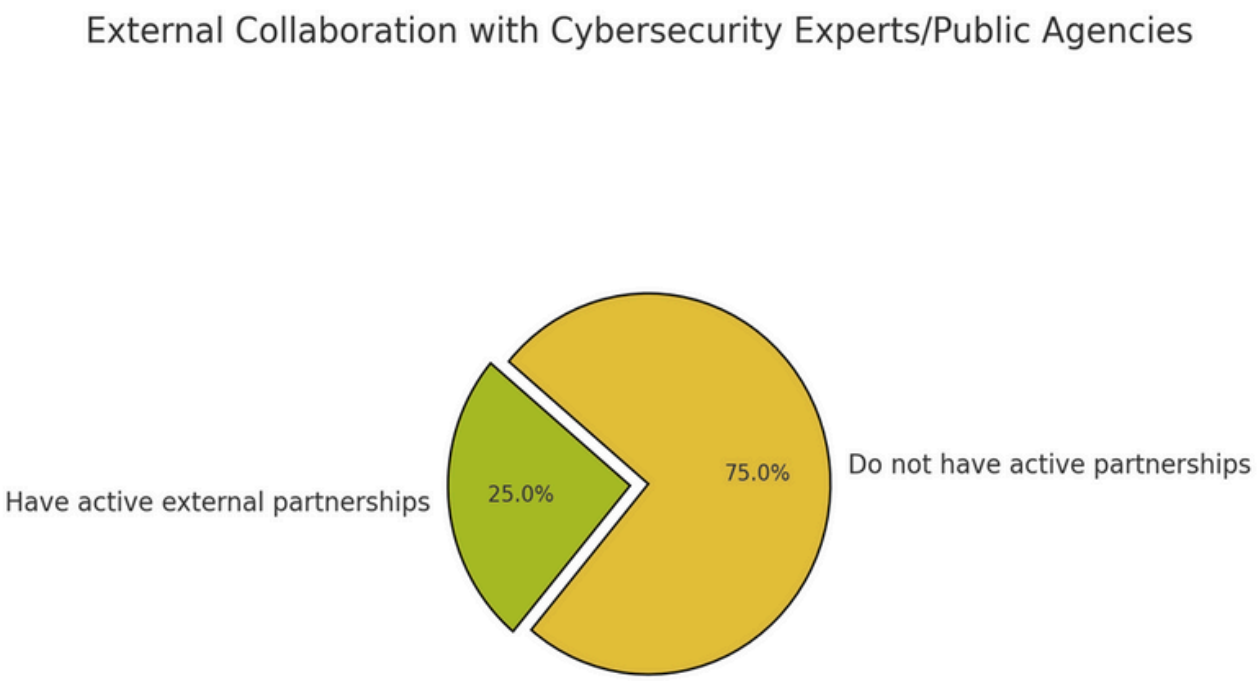
**These findings underscore the urgent need for a multi-stakeholder, gender-responsive approach to digital security. Organizations with established policies and regular training are better equipped to address cyber threats, while those without such measures remain vulnerable—especially during election periods.**

**Most respondents reported that they were unprepared to manage digital risks related to elections, citing misinformation and insufficient online protection systems. Moreover, while many organizations claim to offer equitable training opportunities, few women hold leadership positions in digital security, highlighting structural barriers to participation.**

**Collaboration therefore remains limited, both internally between departments and externally with digital experts or public authorities. Strengthening these links, promoting inclusive leadership, and institutionalizing good practices will be essential to improving the sector's resilience.**

**Democratic Implications of Digital Security Gaps: Beyond operational risks, the identified gaps—particularly in election preparation and the fight against disinformation—represent a broader threat to democratic credibility in Cameroon. When media outlets and CSOs are unable to detect and counter disinformation, citizens become more vulnerable to manipulation, undermining trust in electoral processes and hampering civic participation. In regions with limited infrastructure or heightened insecurity, these risks are even more pronounced. The absence of strong safeguards weakens the legitimacy of media and civic actors, undermining their role as watchdogs and citizen educators. Strengthening digital resilience is therefore not just a technical necessity, but a democratic imperative.**

***Figure 8: External collaboration with cybersecurity experts and public agencies This graph shows the proportion of organizations maintaining active collaborations with cybersecurity specialists, digital monitoring platforms or relevant public institutions.***




*Source: ADISI-Cameroun*

# Case studies

## Case Study 1: Media Organization – "Le Messager" (Littoral Region)

**Background: "Le Messager" is a leading French-language daily newspaper based in Douala, in the Littoral Region. Renowned for its critical investigations and wide readership, it plays a central role in shaping public discourse on governance and civic issues.**

- **Key learnings: Despite its high visibility, Le Messager does not have a formal digital security policy. Staff rely on basic tools (antivirus, passwords) without multi-factor authentication.**

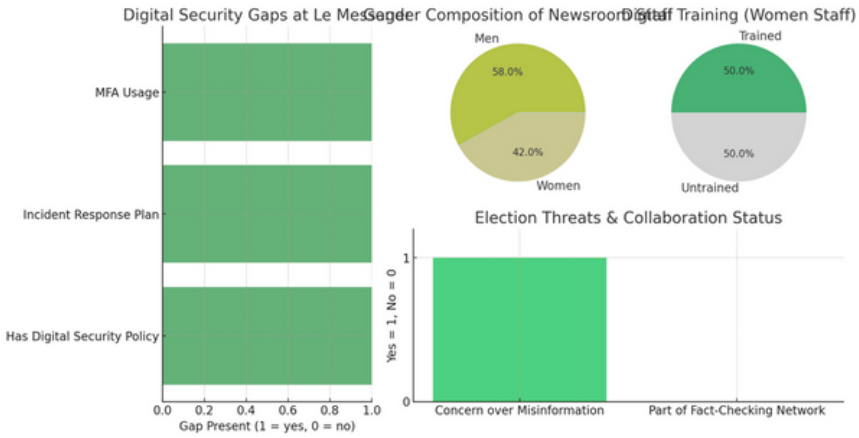
**In 2023, the newspaper suffered a cyberattack that compromised one of its email accounts and leaked sensitive documents. No digital incident response plan was in place at the time.**

In terms of gender, progress has been modest: women represent 42% of the editorial staff, and 50% of them received digital literacy training last year. However, none hold IT or cybersecurity positions.

Le Messager is concerned about upcoming electoral threats, particularly disinformation targeting journalists. However, it is not affiliated with any collaborative fact-checking or monitoring network.

**Lesson: Legacy media remain vulnerable without structured digital frameworks. There is an urgent need to invest in inclusive training and inter-agency partnerships to build resilience ahead of elections.**

***Figure 9: Case study – Le Messager (Littoral Region) This infographic presents the main lessons learned from the media organization "Le Messager", highlighting its shortcomings in digital security, the participation of women in digital training and its vulnerabilities in the run-up to elections.***




*Source: ADISI-Cameroun*

**Digital Security Preparedness and Gender Participation – Le Messager Case Study**
**This multidimensional diagram summarizes the digital security vulnerabilities and gender dynamics within "Le Messager", a leading media outlet in the Littoral Region:**
**Digital security gaps: Lack of critical infrastructure (formal security policy, multi-factor authentication, incident response plan), which increased vulnerability during the 2023 cyberattack.**
**Gender dynamics: Women represent 42% of the editorial staff and 50% of them have received digital literacy training, but none hold IT or cybersecurity positions.**
**Election preparation: despite awareness of the risks, "Le Messager" is not linked to any fact-checking or monitoring network, which exposes it to disinformation campaigns during the election period.**

**This visual illustrates how even established media outlets face systemic and structural risks without proactive and inclusive digital security strategies.**

### Case Study 2: Civil Society Organization – "Civic Watch" (North West Region)

**Background: Civic Watch is a grassroots CSO in Bamenda, working for human rights and civic education in communities affected by the North West conflict.**

- **Key lessons:**

**Proactive culture: Despite limited resources, Civic Watch uses encrypted messaging applications for its internal communications and stores sensitive data in a secure cloud.**

- **Female Leadership: The organization is 70% female-led and has made targeted efforts to train female staff in digital security;**

One of them recently completed training on digital threat monitoring with a regional partner.

**Field adaptation: Insecurity and surveillance disrupt work in the field; Civic Watch regularly rotates its teams and anonymizes field data to protect its staff.**

**Limited election preparation: As the elections approach, Civic Watch is planning an awareness campaign on digital hygiene and the fight against fake news, but lacks technical partnerships and funding to scale it up.**

**Lesson: Small CSOs in conflict zones can serve as models of resilience through innovation, community training, and flexible field practices, even without large budgets.**

***Figure 10: Case study – Civic Watch: digital resilience in a conflict zone in North West Cameroon This visual presents the proactive digital security practices of Civic Watch, a field-based CSO in Bamenda.***


*Source: ADISI-Cameroun*

# OPERATIONAL CHALLENGES DURING THE STUDY

Despite the overall success of data collection, the study encountered several major operational challenges that impacted the timing, scope, and quality of data in some cases:

**Lack of responsiveness from certain target organizations**
**Many invited media and civil society organizations did not respond to emails or phone calls.**
**In some regions—particularly the West and Northwest—this lack of response persisted even after several reminders by phone and WhatsApp.**
**Of the 90 organizations contacted, at least 15 never engaged in dialogue, limiting the diversity and representativeness of regional data.**

**Difficulties scheduling appointments and accessing teams**
**Several organizations, although interested, were unable to mobilize their staff within the timeframe due to workload constraints, travel or internal procedures.**
**Some scheduled interviews were postponed several times, sometimes at the last minute, disrupting field plans.**
**This phenomenon was particularly marked in the Littoral and Central regions, where the media have unpredictable schedules or require managerial validation to authorize interviews.**

**Communication barriers between investigators and coordinators**
**Despite using WhatsApp and phone calls, investigators in the Southwest and Northwest suffered from recurring network outages, making real-time coordination difficult.**
**Delays in sending or clarifying the questionnaire created bottlenecks in data processing.**
**The lack of a centralized daily reporting model led to uneven feedback, making it difficult to track progress.**

**Technical issues with tools**
**Using KoboToolbox in offline mode has caused compatibility issues with some versions of Android on personal devices.**
**Synchronization in areas with poor coverage sometimes required significant movement to pick up a usable network.**

Some interviews were lost or duplicated due to synchronization errors, despite prior training. Additional refresher sessions could have reduced these incidents.

**Security and access issues in conflict zones**
**In the North West (Bamenda) and some areas of the South West (Buea, Limbe), investigators felt unsafe or hampered by roadblocks and sporadic unrest.**
**Several organizations preferred anonymous or remote interviews, fearing reprisals related to their sensitive advocacy activities.**
**These conditions have extended the duration of land coverage and, in some cases, led to partial data.**

**Recommendations for future studies:**
**Early engagement: anticipate contacts well before the field phase to confirm participation and set appointments.**
**Flexible planning: Build in time margins to manage cancellations and postponements.**
**Decentralized coordination: appoint regional supervisors to ensure real-time monitoring and support.**
**Technical support: provide replacement devices and troubleshooting kits, especially in areas with unstable networks.**
**Security protocols: conduct risk assessments and train investigators on security guidelines in sensitive areas.**

# LIMITATIONS OF THE STUDY

**Geographic scope: although the study covered the Central, Littoral, North-West, South-West and West regions, some remote or particularly unstable areas could not be reached, limiting the wealth of insights for these contexts with high digital vulnerability.**

**Language barriers: Despite the questionnaires being available in English and French, some field respondents may not have fully understood the technical terms, which may have affected the accuracy of some responses.**

**Resource constraints: The project took place over six months on a limited budget, limiting the number of follow-up qualitative interviews and validation meetings. Several researchers reported difficulties scheduling second interviews, particularly in the Northwest and Southwest.**

- **Self-report bias: Responses may have been skewed upward, with organizations presenting their security and gender inclusion practices in a more favorable light. For example, while 67% report equal access to training, only 19.5% actually have women in cybersecurity roles.**

Coordination issues: Communication delays between the project team and some surveyors resulted in irregular data flows. Some data collectors reported difficulties reaching organization managers or scheduling appointments within the timeframe.

These limitations were mitigated through data triangulation, close monitoring of field activities, and cross-checking via KoboToolbox's follow-up functions.

# RECOMMENDATIONS

**Institutionalize appropriate digital security policies**
**Develop and maintain tailored policies, incorporating protocols against phishing and data leaks, as illustrated by Civic Watch in conflict zones.**

**Strengthening inclusive training programs**
**Integrate regular and mandatory sessions for all profiles (IT, program, administration, field), with a focus on the specific needs of women and young people. Implement mentoring programs to promote women's access to technical and decision-making roles.**

**Create cross-functional digital security teams**

- **Establish security committees including IT, communications, program and administration, to distribute responsibility and spread the cybersecurity culture at all levels.**

**Improving election preparedness**
**Establish rapid response protocols, media monitoring systems to detect disinformation and designate points of contact to coordinate the response during election periods.**

**Promoting gender-responsive digital leadership**
**Include parity objectives in internal policies, define career paths for women in cybersecurity, and develop training content adapted to gender sensitivities.**

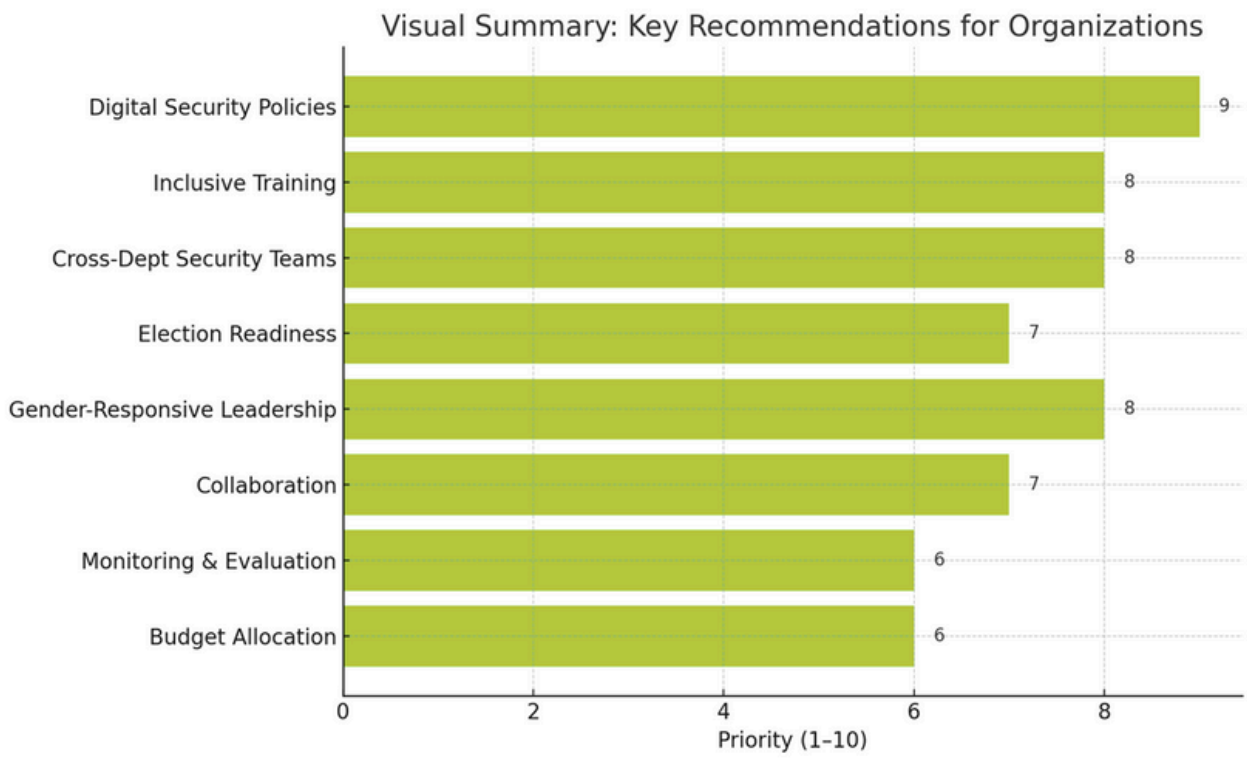
**Strengthen internal and external collaboration**
**Build partnerships with other CSOs, universities, and public and private actors specializing in cybersecurity. Exchange best practices and establish common intervention protocols (MoUs).**

**Implement practical monitoring and evaluation tools**
**Adopt simple dashboards (incident trackers, self-assessment checklists, quarterly training reports) to capitalize on incidents and adjust strategies.**

**Allocate dedicated budgets to digital security**
**Advocate for 5–10% of the IT or operational budget to be dedicated to cybersecurity (secure hosting, antivirus, backups, training). Educate donors and boards of directors on the importance of these budget lines.**

**These recommendations, rooted in the realities on the ground, aim to be pragmatic, scalable, and adapted to each context. Organizations are encouraged to start with low-cost actions and scale up as partnerships and resources become available.**

**Figure 11: Visual Summary – Key Recommendations for Organizations This infographic visually and actionably brings together key tips for strengthening digital security and promoting gender equity: policy development, inclusive training, collaborative frameworks, gender-sensitive leadership, and electoral preparedness.**




*Source: ADISI-Cameroun*

# CONSIDERATIONS FOR IMPLEMENTING THE RECOMMENDATIONS

**Phased implementation: The recommendations should be rolled out in structured phases. Organizations will begin with a thorough assessment of their current practices, then develop policies, train staff, and gradually expand digital protocols.**

**Financial Partnerships: To ensure sustainability, organizations must build alliances with donors, private actors, and international agencies to co-finance infrastructure improvements, secure software acquisition, and long-term capacity-building programs.**

**Regional champions: Identifying and training local representatives—particularly people rooted in their communities—will help tailor interventions to the context and facilitate the sharing of experiences, monitoring of implementation, and liaison with national stakeholders.**

**Monitoring tools: Implementing simple and effective tools (incident logs, audit templates, training logs) will help track progress, record lessons learned and continuously adjust strategies, thus strengthening institutional learning and accountability.**

**Policy alignment: Aligning digital security practices with national digital transformation, cybersecurity, and gender equality strategies ensures consistency, facilitates compliance, and opens opportunities for collaboration and public funding.**

# CONCLUSION

The objective of this study was to analyze the intersection between digital security and gender dynamics within the media and civil society organizations (CSOs) in Cameroon, in the run-up to the 2025 elections. Using a mixed methodology combining quantitative and qualitative data, data was collected in five major regions (Centre, Littoral, North-West, South-West, West), revealing challenges, good practices and structuring innovations.

The results show a clear disparity in digital readiness across regions and organizational types. Some actors, such as Civic Watch in the Northwest, demonstrate ingenuity despite limited resources, while others—including influential media outlets—remain vulnerable due to a lack of appropriate frameworks, training, or awareness. Gender equity in digital leadership remains a challenge, with women remaining underrepresented in decision-making positions despite high participation in training.

- Election threats (disinformation, phishing) appear to be major concerns, but only a few organizations have the protocols, partnerships and infrastructure needed to address them. The regional contrasts are striking: large cities benefit from better technical support, while conflict zones are lagging behind in terms of structure.

These findings call for action:
Institutionalize digital security policies and audits,
Deploy inclusive and feminist training,
Strengthen collaboration between CSOs, media, experts and authorities,
Developing digital literacy to counter disinformation and prepare for elections.

Despite the limitations identified (geographical scope, logistical constraints), this research provides a detailed overview and proposes a strategic roadmap to strengthen Cameroon's civic and media resilience in the digital age.

# Contacts


## ADISI-Cameroun

Douala-Cameroon
5e étage Immeuble Aziccul
Yaoundé-Cameroon Simbock, 4e étage
Complexe Tcha-Mo SARL
adisi@adisicameroun.org
243 526 139
www.adisicameroun.org [1]
www.datacameroon.com [2]

ADISI - CAMEROUN

ifex

# STUDY REPORT ON THE STATE OF DIGITAL SECURITY AND GENDER DYNAMICS IN THE MEDIA AND CIVIL SOCIETY ORGANIZATIONS IN CAMEROON

2025