ADISI - CAMEROUN

ifex

RAPPORT D'ÉTUDE SUR L'ÉTAT DE LA SÉCURITÉ NUMÉRIQUE ET LES DYNAMIQUE DE GENRE DANS LES MÉDIAS ET ORGANISATIONS DE LA SOCIÉTÉ CIVILE AU CAMEROUN

2025

RAPPORT D'ÉTUDE SUR L'ÉTAT DE LA SÉCURITÉ NUMÉRIQUE ET LES DYNAMIQUE DE GENRE DANS LES MÉDIAS ET ORGANISATIONS DE LA SOCIÉTÉ CIVILE AU CAMEROUN

TABLE DES MATIÈRES

Résumé exécutif	p.01
Introduction	p.03
Objectifs	p.04
Méthodologie	p.05
Profil des répondants	p.07
Principaux résultats	p.08
Principaux enseignements	p.15
Études de cas	p.19
Recommandations	p.22
Considérations de mise en œuvre des recommandations	p.24
Conclusion	p.26
Annexes	p.28
	p.29

Résumé exécutif

Cette étude, commanditée par ADISI-Cameroun, évalue l'état de la sécurité numérique et ses implications genrées au sein des médias et des organisations de la société civile (OSC) au Cameroun. Elle vise à offrir une compréhension fine de la préparation institutionnelle, des cadres politiques et des dispositifs de protection concrets structurant l'univers numérique à l'approche des élections de 2025, avec un accent marqué sur l'inclusion des femmes.

L'analyse repose sur les données de 101 organisations réparties dans cinq régions, couvrant tant les zones anglophones (45 %) que francophones (55 %). La collecte s'est faite à l'aide de questionnaires structurés, administrés en présentiel et à distance par des enquêteurs formés, via KoboToolbox, afin de garantir fiabilité, anonymat et adaptation contextuelle. Ces questionnaires ont ciblé un large éventail de profils (directeurs, personnels informatiques, journalistes, responsables genre, etc.), reflétant des expériences variées dans les milieux urbains, périurbains et affectés par les conflits.

Principales vulnérabilités identifiées :

- 53 % des organisations n'ont pas de politiques formelles de sécurité numérique, et seules 42 % proposent des formations régulières en cybersécurité, souvent ad hoc et réservées au personnel technique.
- 39 % seulement réalisent des audits de sécurité numérique, laissant nombre d'organisations mal préparées face aux cyber menaces croissantes (hameçonnage, rançongiciels, attaques à caractère politique).
- Moins de 35 % se sentent prêtes à faire face aux menaces numériques liées aux élections, malgré la montée des risques de désinformation durant les cycles électoraux.
- Si 67 % déclarent offrir un accès égal aux formations numériques, moins de 20 % des postes de décision en sécurité numérique sont occupés par des femmes, traduisant un écart significatif de participation selon le genre.

L’étude met également en lumière des défis de capacité : 62 % des organisations ne disposent d’aucun budget dédié à la sécurité numérique, et moins de 25 % collaborent activement avec des experts en cybersécurité ou des institutions publiques compétentes. Les régions du Nord-Ouest et du Sud-Ouest, particulièrement affectées par des conflits, souffrent en outre d’un manque d’outils de communication sécurisés et de risques accrus de surveillance.

Le rapport se conclut par des recommandations opérationnelles adaptées au contexte : institutionnaliser des politiques de sécurité numérique, proposer des formations sensibles au genre et aux fonctions, encourager la collaboration multipartisme et intégrer des évaluations de risque numérique dans les processus internes.

Au final, cette recherche fondée sur des données offre une feuille de route stratégique pour bâtir un écosystème civique et médiatique au Cameroun plus sûr, inclusif et résilient, où les droits numériques et la sécurité sont garantis pour tous.

INTRODUCTION

ADISI-Cameroun, une association à but non lucratif dédiée à la transparence, à la participation citoyenne et aux droits numériques au Cameroun, a lancé cette étude en partenariat avec IFEX dans le cadre de sa mission globale visant à renforcer la gouvernance et la résilience démocratique par une transformation numérique inclusive. Consciente du rôle central des acteurs des médias et de la société civile dans la responsabilisation et le dialogue public, l'étude a été conçue pour évaluer de manière critique l'intersection entre la sécurité numérique et les dynamiques de genre dans ces secteurs clés.

Le Cameroun connaît une évolution numérique majeure : la pénétration d'Internet est passée d'environ 6 % en 2010 à plus de 35 % en 2023 [1](Internet World Stats, 2023), et le nombre d'abonnements mobiles dépasse désormais 22 millions (GSMA, 2023). Cette croissance a favorisé l'engagement civique, le pluralisme médiatique et le plaidoyer social. Elle a toutefois entraîné une série de menaces numériques : en 2022 seulement, plus de 3 800 cas de cybercriminalité ont été recensés [2](Minpostel, 2023), notamment des attaques par rançongiciel, des tentatives de phishing, des campagnes de désinformation et des piratages à motivation politique.

Ces menaces ne sont pas réparties de manière homogène : les zones urbaines comme Yaoundé et Douala bénéficient d'infrastructures et de soutiens techniques plus solides, tandis que les organisations des régions touchées par les conflits — notamment le Nord-Ouest et le Sud-Ouest — subissent des vulnérabilités accrues (insécurité, surveillance, faible connectivité).

À ces défis s'ajoutent des inégalités systémiques entre les genres. Si la part des femmes dans les organisations médiatiques et de la société civile est en hausse, leur implication dans la gouvernance des TIC et l'élaboration des politiques de sécurité numérique reste faible. Selon [3]ONU Femmes, seuls 17 % des postes décisionnels liés aux TIC en Afrique subsaharienne sont occupés par des femmes (UN Women, 2022). L'étude confirme ce fossé : moins de 20 % des répondants impliqués dans la sécurité numérique des organisations s'identifient comme femmes.

1) Internet World Stats. (2023). Rapport sur l'utilisation d'Internet et les télécommunications au Cameroun. Disponible sur : https://www.internetworldstats.com
2) Ministère des Postes et Télécommunications (Minpostel), Cameroun. (2023). Rapports d'incidents de cybersécurité.
3) ONU Femmes. (2022). Genre et TIC en Afrique subsaharienne. Disponible sur : https://www.unwomen.org

OBJECTIFS

ÉVALUER LA PRÉPARATION INSTITUTIONNELLE

- Vérifier l'existence de politiques formelles de sécurité numérique, d'audits et de personnel formé.
- Mesurer la capacité de réponse aux menaces telles que le phishing, les maliciels et les brèches de données.

ANALYSER LES DYNAMIQUES DE GENRE DANS L'ENGAGEMENT NUMÉRIQUE

- Étudier la participation des femmes à l'accès, à la formation et aux prises de décision en matière de numérique.
- Identifier les barrières structurelles ou culturelles à un leadership inclusif.

PASSER EN REVUE LES PRATIQUES ACTUELLES DE SÉCURITÉ NUMÉRIQUE

- Examiner les politiques, formations et protocoles en place.
- Évaluer leur portée, leur fréquence et leur efficacité sur le terrain.

IDENTIFIER LES OBSTACLES CLÉS

- Mettre en lumière les contraintes budgétaires, les faiblesses d'infrastructure, le faible niveau de littératie numérique et l'absence de soutien externe.
- Comprendre les défis spécifiques selon le genre et les régions.

ÉLABORER DES RECOMMANDATIONS OPÉRATIONNELLES

- Proposer des actions concrètes et basées sur les données, adaptées aux réalités organisationnelles.
- Encourager la résilience numérique, l'équité de genre et la collaboration multipartite.

MÉTHODOLOGIE

Les données de cette étude ont été recueillies selon une approche mixte, intégrant des éléments quantitatifs et qualitatifs pour offrir une compréhension riche et contextualisée de la sécurité numérique et des dynamiques de genre.

COUVERTURE RÉGIONALE

Des questionnaires structurés ont été administrés dans cinq grandes régions : Centre, Littoral, Sud-Ouest, Nord-Ouest et Ouest. Cette répartition géographique a été conçue pour refléter la diversité linguistique, régionale et infrastructurale du Cameroun.

STRATÉGIE D'ÉCHANTIL-LONAGE

L'échantillon a été volontairement sélectionné pour assurer une représentation des zones anglophones et francophones, ainsi que des organisations urbaines et périurbaines. Un équilibre a été recherché entre médias et OSC, en tenant compte de la taille, du périmètre d'action et de l'exposition numérique de chaque entité.

PROFIL DES RÉPONDANTS

Les participants comprenaient des responsables d'organisation (coordinateurs, directeurs), du personnel technique (informaticiens), des journalistes, des chargés de suivi-évaluation et des responsables genre. La parité a été priorisée dans le choix des répondants pour garantir une vision inclusive des pratiques numériques.

En complément des enquêtes structurées, l'étude a mobilisé les outils et processus suivants :

- **KoboToolbox** pour l'administration des questionnaires, en modes en ligne et hors-ligne selon la disponibilité d'Internet dans chaque région.
- Un questionnaire combinant des questions à choix multiples, des échelles de Likert et des questions ouvertes pour recueillir des données mesurables et descriptives.
- **Formation des enquêteurs** sur :
  - Les considérations éthiques et le consentement éclairé
  - La sensibilité au genre dans la recherche
  - La gestion sécurisée des données numériques et des appareils

Toutes les données ont été anonymisées, en conformité avec les standards éthiques de la recherche. Pour renforcer la fiabilité, la triangulation a été appliquée : recoupement des éléments qualitatifs et identification des convergences ou anomalies dans les comportements et perceptions numériques selon les régions et types d'organisations.

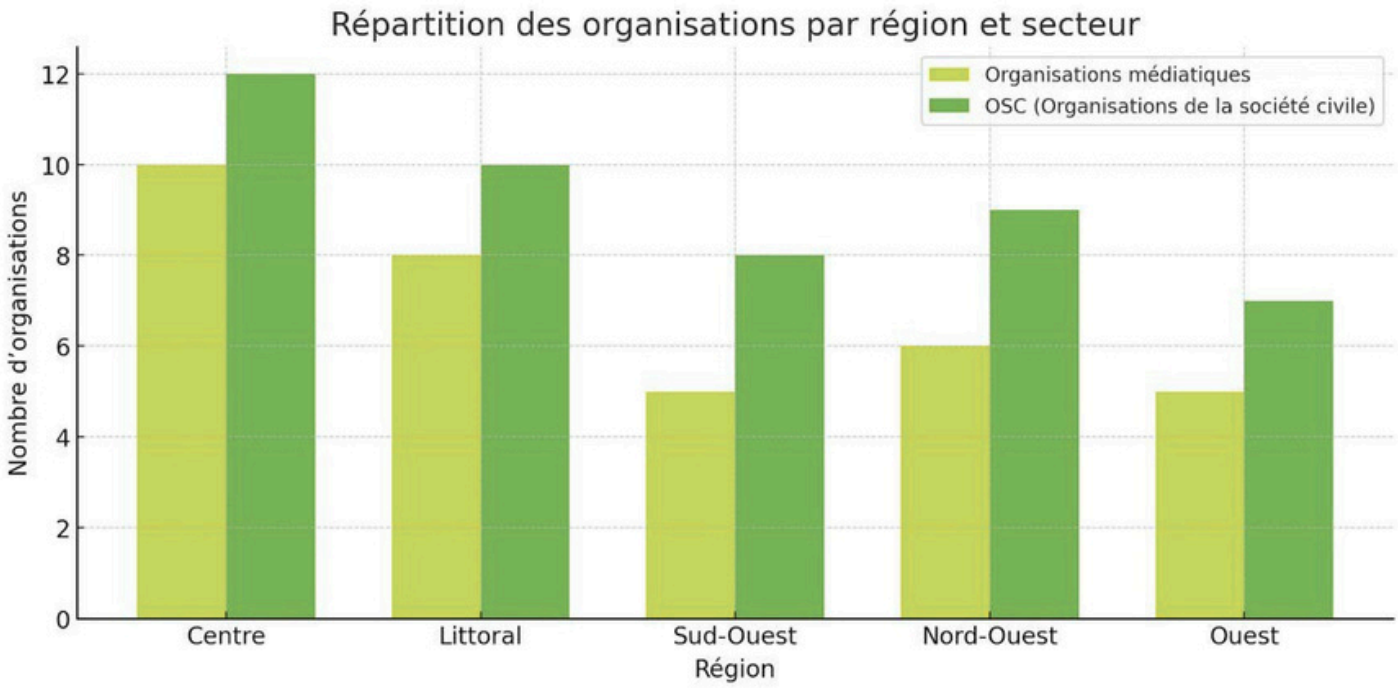
PROFIL DES RÉPONDANTS

Nombre total d'organisations : 101
Type d'organisation : Organisations de la société civile : environ 66 %
Médias : environ 34 %
Répartition géographique :

- Régions anglophones : environ 45 %
- Régions francophones : environ 55 %

Fonctions des répondants : Coordinators, Directeurs, Journalistes, Responsables genre, Chargés de suivi-évaluation, entre autres.

Figure 0 : Répartition des organisations par région et par secteur
Graphique comparant le nombre d'organisations médiatiques et d'organisations de la société civile (OSC) dans cinq régions du Cameroun (Centre, Littoral, Sud-Ouest, Nord-Ouest et Ouest).



Source : ADISI-Cameroun

PRINCIPALES CONCLUSIONS

Paysage numérique

L'étude montre que la sécurité numérique reste un domaine sous-développé dans un nombre significatif d'organisations de la société civile et d'institutions médiatiques au Cameroun. Malgré la numérisation croissante des opérations, de nombreuses organisations manquent de cadres structurés et d'investissements pour protéger leurs systèmes.

Seulement 47 % des organisations interrogées déclarent disposer de politiques formelles de sécurité numérique. Celles-ci sont souvent limitées dans leur périmètre et ne sont pas toujours mises en œuvre ou actualisées régulièrement.

42 % des organisations proposent des formations régulières à la cybersécurité. Toutefois, ces formations sont souvent ponctuelles et réservées au personnel technique, excluant journalistes, chargés de programme et administrateurs qui utilisent fréquemment des outils numériques.

39 % des organisations réalisent des audits réguliers de la sécurité des systèmes, ce qui témoigne d'un niveau modéré de pratiques d'évaluation des risques, mais révèle un écart important dans la préparation institutionnelle.

Les outils les plus utilisés sont les antivirus, les pare-feu basiques et les mises à jour périodiques des systèmes. Ces mesures restent fondamentales mais insuffisantes face aux menaces cybernétiques modernes.

L'adoption de protocoles de sécurité avancés — chiffrement de bout en bout, stockage cloud sécurisé, réseaux privés virtuels (VPN) et authentification multifactorielle — reste limitée. De nombreuses organisations invoquent un manque de capacités techniques, de financements ou de sensibilisation pour expliquer cette non-adoption.

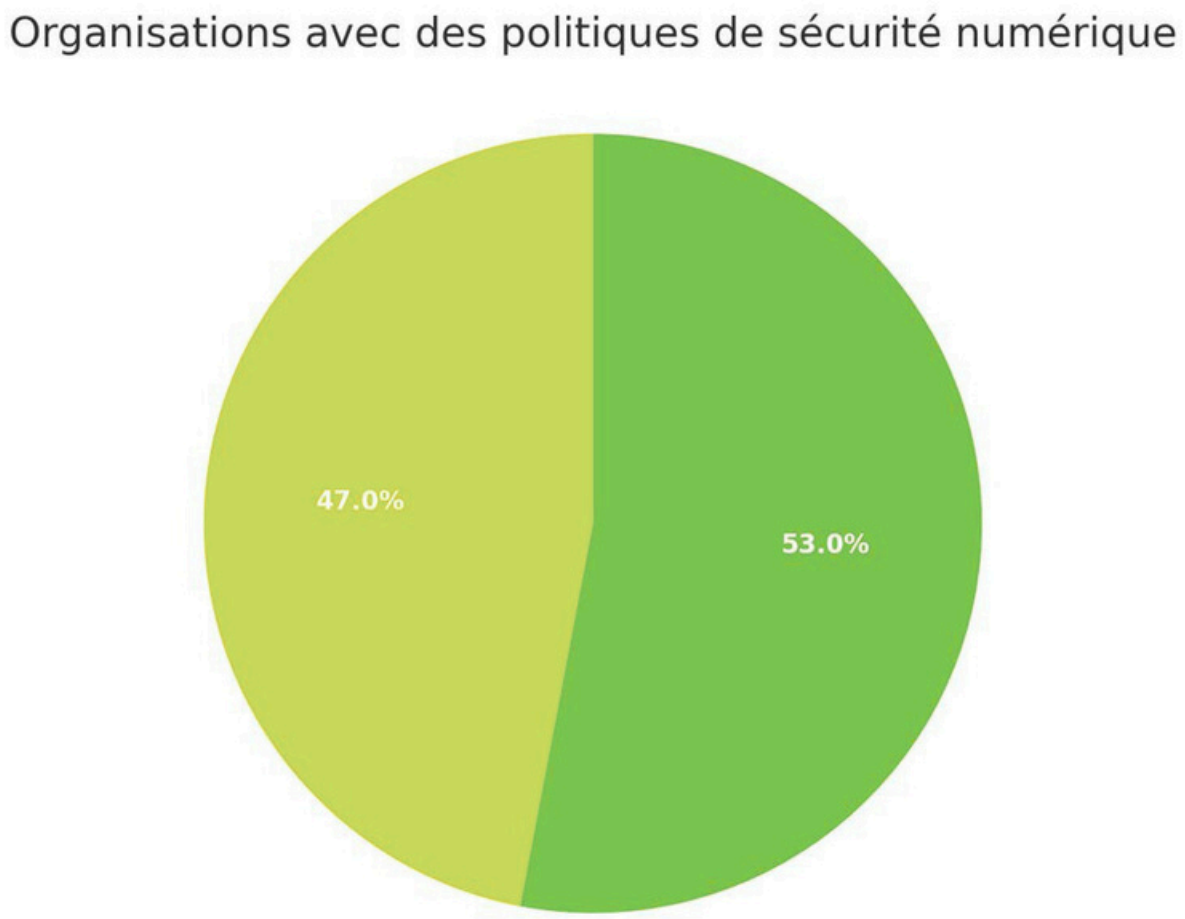
Dans l'ensemble, ces résultats illustrent une approche fragmentée et réactive de la sécurité numérique, qui expose nombre d'organisations à des intrusions, à la désinformation et à la perte de données, en particulier dans un contexte de surveillance accrue et de cyberattaques lors de périodes sensibles comme les élections.

L'absence de cadres de sécurité robustes rend les organisations vulnérables à la manipulation de données sensibles, d'autant plus préoccupant pendant les cycles électoraux, lorsque la société civile et les médias jouent un rôle clé dans la reddition de comptes.

En de telles circonstances, l'absence de protocoles de réponse aux incidents, de canaux de communication sécurisés ou de garanties d'intégrité des données peut permettre à des acteurs malveillants de perturber les processus démocratiques par la désinformation, l'accès non autorisé ou des attaques ciblées contre des institutions considérées comme des voix critiques.

Ce sous-investissement systémique dans l'infrastructure numérique constitue une menace directe non seulement pour la continuité opérationnelle, mais aussi pour l'intégrité de l'engagement civique et la transparence électorale au Cameroun.

Figure 1 : Graphique illustrant le nombre d'organisations par pourcentage qui disposent ou pas de politique de sécurité numérique



Source : ADISI-Cameroun

Dynamiques de genre

L'étude révèle des disparités de genre complexes et persistantes dans l'engagement en matière de sécurité numérique, tant au sein des OSC que des médias.

Bien que 67 % des répondants déclarent que les hommes et les femmes ont un accès égal aux formations, les réponses qualitatives et une désagrégation plus fine montrent que cet accès ne se traduit souvent pas par une participation équivalente aux décisions ou aux postes de leadership liés à la sécurité numérique.

31 % des organisations reconnaissent ne pas impliquer activement les femmes dans les décisions de sécurité numérique. Dans certains cas, elles n'ont même pas été consultées lors des étapes d'évaluation des risques ou d'élaboration des protocoles.

Obstacles structurels :

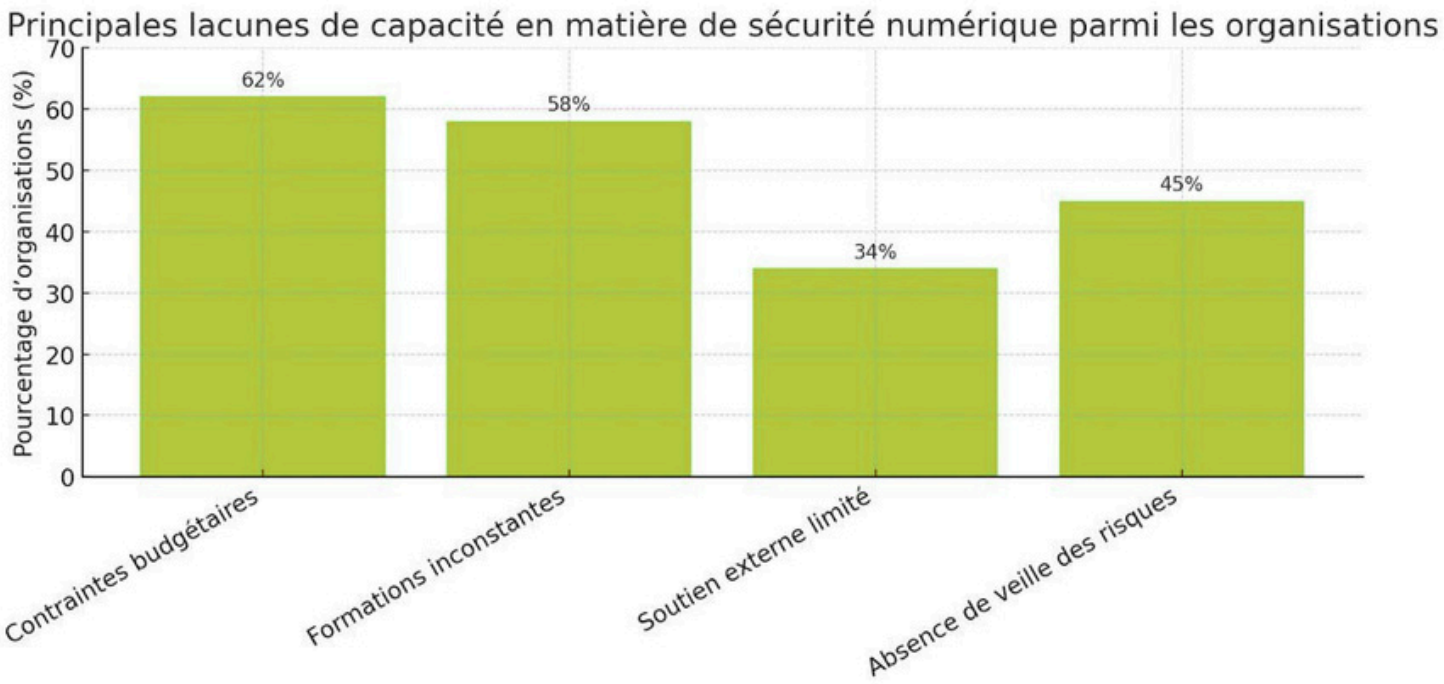
- Faible littératie numérique chez les femmes, en particulier dans les organisations rurales.
- Culture organisationnelle qui perçoit la sécurité numérique comme un domaine technique (donc dominé par les hommes).
- Manque de représentation des femmes dans les fonctions TIC ou dans les équipes de réponse aux incidents.

Obstacles personnels et sociaux :

- Peur du harcèlement en ligne et du cyberharcèlement, décourageant les femmes de s'engager dans des rôles technologiques ou de plaidoyer numérique.
- Accès limité à des appareils sécurisés ou à une connexion Internet à domicile, notamment pour les femmes assumant des responsabilités de soin.
- Manque de supports de formation sensibles au genre et de formatrices pouvant jouer un rôle de mentor ou de modèle.

Ces résultats suggèrent que tant que le genre ne sera pas délibérément intégré dans les politiques et pratiques de sécurité numérique, les femmes resteront marginalisées dans ce domaine. Cela a des répercussions plus larges sur la résilience organisationnelle, l'inclusivité et la protection des droits humains.

Figure 2 : Participation des genres à la sécurité numérique
Graphique comparant la proportion d'hommes et de femmes participant aux formations numériques versus ceux occupant des postes de leadership liés à la cybersécurité.



Source : ADISI-Cameroun

Lacunes de l'étude

L'étude a mis en évidence d'importantes limites de capacité qui entravent le développement et la mise en œuvre de mesures efficaces de sécurité numérique au sein des OSC et des médias.

Contraintes budgétaires : 62 % des organisations déclarent ne pas disposer d'un budget dédié à la sécurité numérique. Dans de nombreux cas, celle-ci n'est pas considérée comme une priorité opérationnelle, et toute dépense reste ponctuelle et réactive plutôt que planifiée et stratégique. Ce manque d'engagement financier rend les systèmes vulnérables aux cyber menaces évolutives.

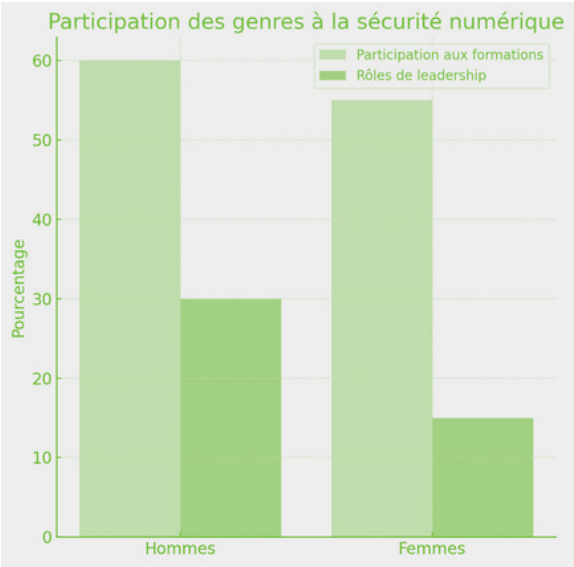
Formations inconstantes : Les efforts de formation sont sporadiques et mal intégrés aux plans de développement organisationnel. Lorsqu'elles sont organisées, les formations ciblent principalement le personnel technique, excluant souvent le personnel programme, administratif ou de terrain—nombre de ces acteurs manipulant régulièrement des données sensibles. Les groupes vulnérables, tels que les femmes et les jeunes, sont disproportionnellement mis à l'écart, renforçant ainsi les inégalités.

Soutien externe limité : Seule une minorité d'organisations collabore de manière fiable avec des partenaires techniques (entreprises de cybersécurité, organisations de défense des droits numériques, etc.). La plupart s'appuient sur un personnel informatique interne non spécialisé, qui n'est pas nécessairement formé pour faire face à des menaces numériques complexes.

Absence de veille et d'audit : La surveillance régulière des menaces, les audits numériques et les évaluations de risques ne sont que rarement institutionnalisés. Les organisations ignorent souvent les nouvelles menaces ou ne documentent pas les incidents passés pour en tirer des enseignements. Cette absence de posture proactive réduit la résilience globale.

Ces lacunes de capacité soulignent le besoin d'une réforme institutionnelle, d'investissements stratégiques et de réseaux de collaboration technique renforcés.

Figure 3: Lacunes clés de capacité en matière de sécurité numérique parmi les organisations. Graphique en barres illustrant le pourcentage d'organisations dépourvues de politiques formelles, de programmes de formation, d'audits de sécurité et d'outils de protection avancés.



Source : ADISI-Cameroun

Menaces liées aux élections

Les élections de 2025 constituent un véritable banc d'essai pour la cybersécurité des médias et des organisations de la société civile (OSC) au Cameroun. L'étude révèle que ces acteurs restent dangereusement peu préparés face aux menaces numériques susceptibles de s'intensifier pendant la période électorale.

Hausse des menaces de désinformation et de phishing :

- Plus de 65 % des répondants considèrent la désinformation (fake news, contenus trafiqués, deepfakes), les courriels de phishing et l'ingénierie sociale comme leurs principales inquiétudes.
- Ces menaces sont particulièrement virulentes en période électorale, car de fausses narrations peuvent rapidement saper la confiance du public ou provoquer des troubles.

Absence de préparation et de protocoles de réponse aux incidents :

- Moins de 35 % des organisations déclarent disposer de protocoles pour gérer des cyberattaques à motivation politique, telles que les campagnes de fake news ou le harcèlement numérique d'activistes et de journalistes.
- Seule une minorité a effectué des exercices de simulation pour des incidents électoraux (pics de désinformation, fuites de données ciblées, etc.).

Disparités régionales et urbain-rural : Les organisations basées à Douala et Yaoundé sont mieux préparées, grâce à l'accès au support TIC, à des formations et à des programmes financés par des donateurs.

En revanche, celles du Nord-Ouest et du Sud-Ouest subissent des vulnérabilités cumulées :

- L'insécurité limite la mobilité et la déploiement du personnel.
- La crainte de la surveillance et des représailles politiques freine l'engagement numérique.
- L'accès instable à Internet empêche la vérification en temps réel et les campagnes d'hygiène numérique.

Faible collaboration institutionnelle :

- Seuls 18 % des répondants collaborent avec des acteurs étatiques tels que l'Agence nationale des technologies de l'information et de la communication (ANTIC) ou la Commission électorale nationale (ELECAM).
- Encore moins d'organisations travaillent avec des plateformes de fact-checking ou des observatoires internationaux (Africa Check, Global Disinformation Index, etc.).
- Cette isolation accroît la vulnérabilité aux campagnes de désinformation, aux trollings coordonnés ou aux suppressions de contenu en ligne en période sensible.

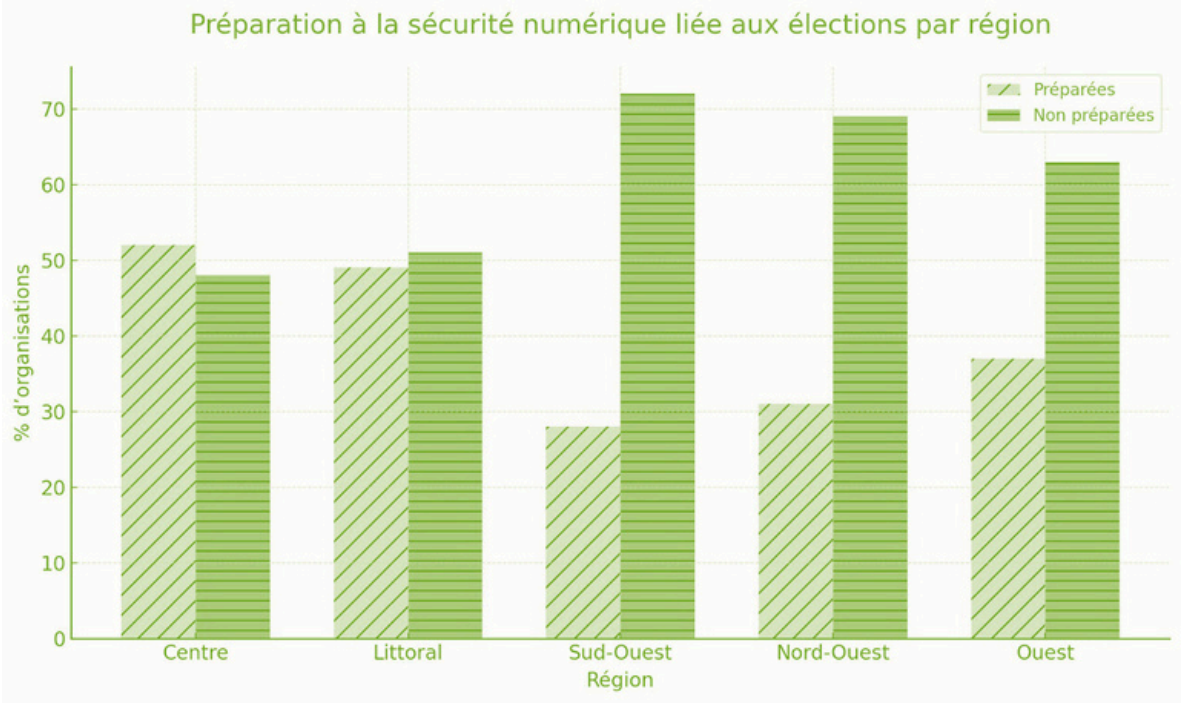
Formation et outils techniques limités : Bien que certaines OSC, comme Civic Watch, soient actives en éducation civique ou en initiatives de civic tech, la plupart manquent d'expertise technique pour :

- Détecter les médias manipulés (deepfakes, etc.).
- Mettre en place des plateformes d'engagement sécurisé des électeurs.
- Réagir aux attaques par déni de service distribué (DDoS) visant leurs sites ou applications.

Opportunités manquées pour la préparation électorale : L'absence d'équipes d'intervention rapide, de plans d'escalade prédéfinis et de systèmes de veille médiatique laisse la plupart des organisations en position réactive plutôt que proactive.

Par exemple, Le Messager, malgré son statut de média de référence, n'avait pas adhéré à un réseau de fact-checking collaboratif ni développé de stratégies internes contre la désinformation électorale.

Figure 4 : Comparaison régionale de la préparation aux menaces numériques liées aux élections.



Source : ADISI-Cameroun

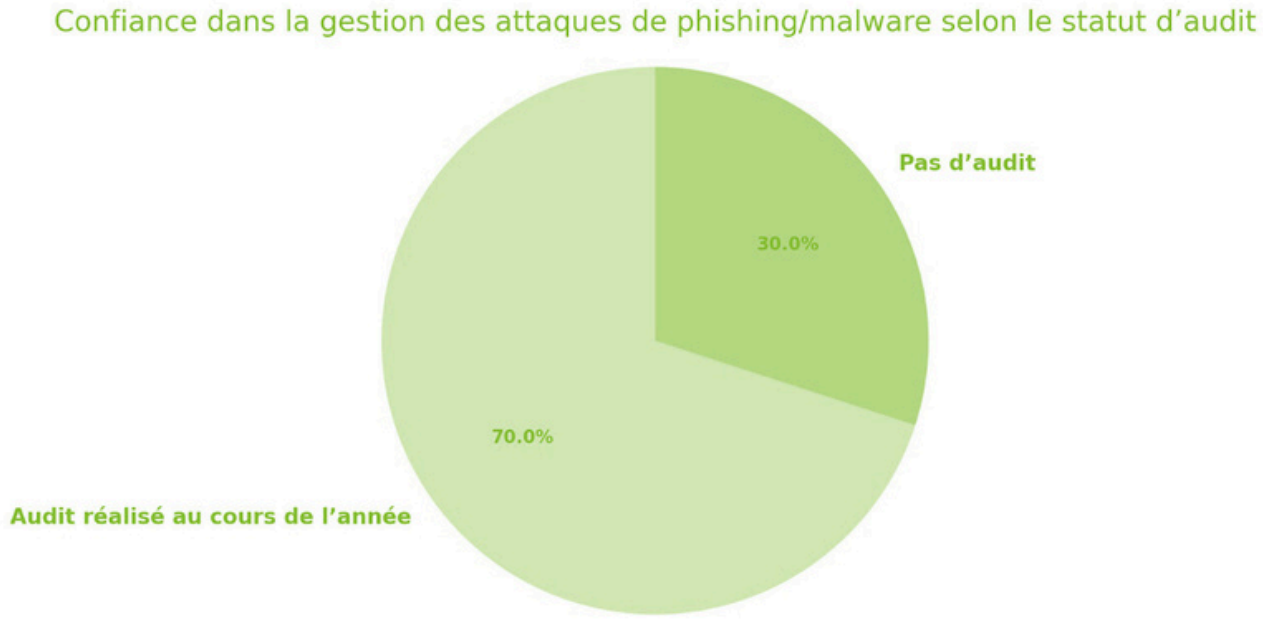
PRINCIPAUX ENSEIGNEMENTS

L'étude met en évidence une forte corrélation entre la préparation institutionnelle et l'exposition aux cybermenaces. Les organisations disposant de cadres formalisés de sécurité numérique, de programmes de formation cohérents et d'audits réguliers font preuve d'une capacité nettement supérieure à détecter, répondre et prévenir les risques numériques.

Par exemple : Plus de 70 % des organisations ayant réalisé un audit au cours de l'année écoulée déclarent être confiantes pour répondre à des attaques de phishing ou de logiciels malveillants.

À l'inverse, les organisations sans cadre structuré signalent davantage de failles système et de perturbations liées à la désinformation.

Figure 5 : Confiance dans la gestion des attaques de phishing/malware selon la réalisation d'audits. Ce graphique compare le pourcentage d'organisations se déclarant confiantes pour faire face aux cyberattaques, selon qu'elles ont ou non réalisé un audit de sécurité numérique au cours des douze derniers mois.



Source : ADISI-Cameroun

Vulnérabilités liées aux élections : Moins de 35 % des répondants se sentent prêts à gérer les menaces numériques lors des élections.

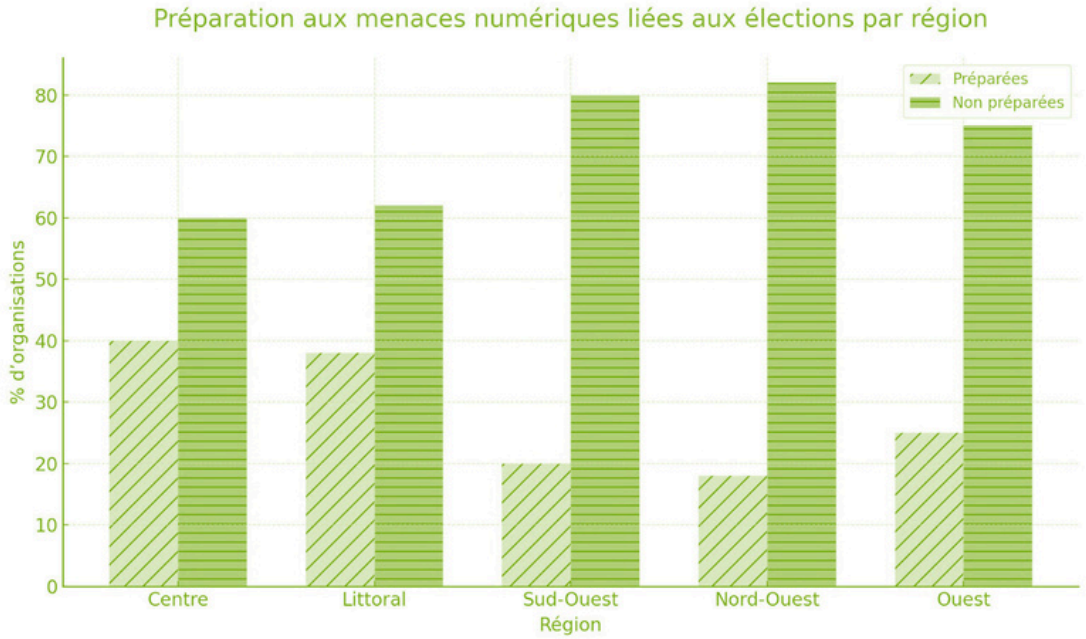
Les retours indiquent :

- Inquiétude face aux fake news et aux campagnes de désinformation.
- Vulnérabilité aux attaques d'ingénierie sociale.
- Faiblesses dans la protection des sites web et des plateformes en ligne.

Cela souligne la nécessité de :

- Une planification de scénarios spécifique aux élections.
- Protocoles de réponse rapide.
- Partenariats renforcés avec les observatoires numériques et les plateformes de fact-checking.

Figure 6 : Comparaison régionale de la préparation aux menaces numériques liées aux élections.



Source : ADISI-Cameroun

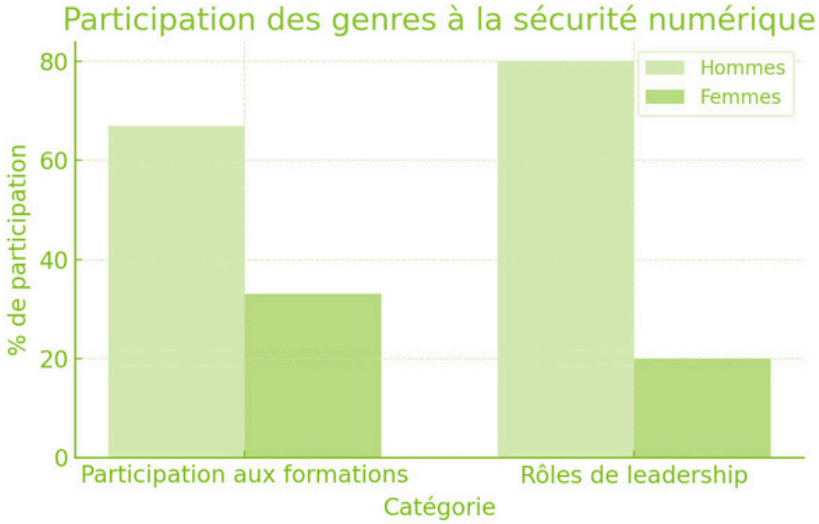
Disparités de genre dans la sécurité numérique : Bien que 67 % des organisations déclarent un accès égal aux formations numériques, une analyse plus poussée montre :

- Moins de 20 % impliquent des femmes dans la conception des politiques ou des systèmes de sécurité.

Les principaux obstacles rencontrés par les femmes sont :

- Manque de mentorat dans les fonctions TIC.
- Participation limitée aux instances décisionnelles.
- Biais culturels et structurels au sein des organisations.

Figure 7 : Participation des femmes à la sécurité numérique
Ce graphique illustre le niveau d'implication des femmes dans la sécurité numérique au sein des organisations, notamment dans la conception des politiques, l'administration des systèmes et les programmes de formation.



Source : ADISI-Cameroun

Lacunes de collaboration : En interne, la sécurité numérique est souvent confinée aux services informatiques.
En externe :

- Moins de 25 % des organisations entretiennent des liens actifs avec des experts en cybersécurité ou des agences publiques.
- Les répondants ont demandé des ateliers conjoints, des outils partagés et des points de situation réguliers avec leurs partenaires.

Ces résultats soulignent l'urgence d'adopter une approche multipartite et sensible au genre en matière de sécurité numérique. Les organisations qui disposent de politiques établies et de formations régulières sont mieux armées pour faire face aux cybermenaces, tandis que celles qui n'ont pas mis en place de telles mesures restent vulnérables—en particulier lors des périodes électorales.

La plupart des répondants ont signalé qu'ils n'étaient pas prêts à gérer les risques numériques liés aux élections, invoquant la désinformation et des systèmes de protection en ligne insuffisants. De plus, même si de nombreuses organisations prétendent offrir des opportunités de formation équitables, peu de femmes occupent des postes de direction en sécurité numérique, ce qui met en évidence des obstacles structurels à la participation.

La collaboration demeure donc limitée, tant en interne entre les départements qu'en externe avec les experts numériques ou les autorités publiques. Renforcer ces liens, promouvoir un leadership inclusif et institutionnaliser les bonnes pratiques seront essentiels pour améliorer la résilience du secteur.

Implications démocratiques des failles de la sécurité numérique : Au-delà des risques opérationnels, les lacunes identifiées—en particulier dans la préparation aux élections et la lutte contre la désinformation—représentent une menace plus vaste pour la crédibilité démocratique au Cameroun. Lorsque les médias et les OSC ne sont pas en mesure de détecter et de contrer la désinformation, les citoyens deviennent plus vulnérables à la manipulation, ce qui mine la confiance dans les processus électoraux et freine la participation civique. Dans les régions où l'infrastructure est limitée ou l'insécurité accrue, ces risques sont encore plus marqués. L'absence de garanties solides affaiblit la légitimité des acteurs médiatiques et civiques, sapant leur rôle de vigie et d'éducateur citoyen. Renforcer la résilience numérique n'est donc pas seulement une nécessité technique, mais un impératif démocratique.

Figure 8 : Collaboration externe avec des experts en cybersécurité et des agences publiques

Ce graphique montre la proportion d'organisations entretenant des collaborations actives avec des spécialistes de la cybersécurité, des plateformes de veille numérique ou des institutions publiques compétentes.

Source : ADISI-Cameroun

Études de cas

Étude de cas 1 : Organisation médiatique – « Le Messager » (Région du Littoral)

Contexte : « Le Messager » est un quotidien francophone de premier plan basé à Douala, dans la Région du Littoral. Réputé pour ses enquêtes critiques et sa large audience, il joue un rôle central dans le façonnement du discours public sur la gouvernance et les enjeux civiques.

Enseignements clés : Malgré sa forte visibilité, Le Messager ne dispose pas de politique formelle de sécurité numérique. Le personnel se contente d'outils basiques (antivirus, mots de passe) sans authentification multifactorielle.

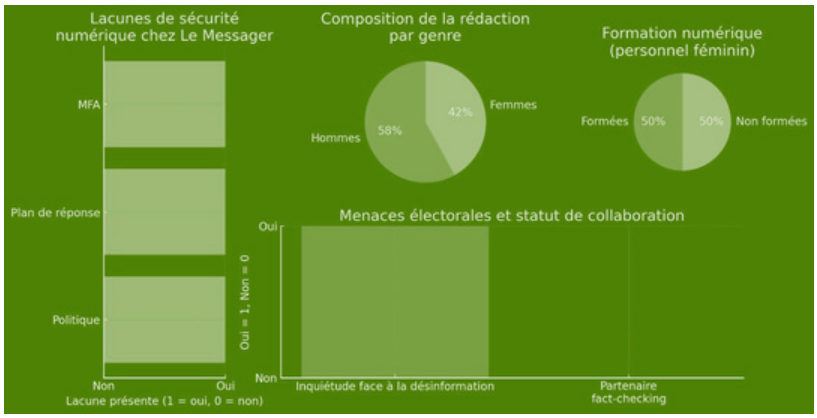
En 2023, le journal a subi une cyberattaque ayant compromis l'un de ses comptes de messagerie et divulgué des documents sensibles. Aucun plan de réponse aux incidents numériques n'était en place à l'époque.

Sur le plan du genre, les progrès sont modestes : les femmes représentent 42 % des effectifs de la rédaction, et 50 % d'entre elles ont suivi une formation en littératie numérique l'an dernier. Cependant, aucune n'occupe de poste IT ou cybersécurité.

Le Messager s'inquiète des menaces électorales à venir, notamment la désinformation visant les journalistes. Pourtant, il n'est affilié à aucun réseau collaboratif de fact-checking ou de veille.

Leçon : Les médias historiques demeurent vulnérables sans cadres numériques structurés. Il est urgent d'investir dans des formations inclusives et des partenariats inter-organisations pour renforcer la résilience avant les élections.

Figure 9 : Étude de cas – Le Messager (Région du Littoral)
Cette infographie présente les principaux enseignements tirés de l'organisation médiatique « Le Messager », en soulignant ses manques en matière de sécurité numérique, la participation des femmes aux formations numériques et ses vulnérabilités à l'approche des élections.



Source : ADISI-Cameroun

Préparation à la sécurité numérique et participation de genre – Étude de cas de Le Messager

Ce schéma multidimensionnel résume les vulnérabilités en matière de sécurité numérique et les dynamiques de genre au sein de « Le Messager », média de référence dans la Région du Littoral :

- **Lacunes de sécurité numérique :** absence d'infrastructure essentielle (politique de sécurité formelle, authentification multifactorielle, plan de réponse aux incidents), ce qui a creusé la vulnérabilité lors de la cyberattaque de 2023.
- **Dynamiques de genre :** les femmes représentent 42 % de la rédaction et 50 % d'entre elles ont suivi une formation en littératie numérique, mais aucune n'occupe de poste IT ou cybersécurité.
- **Préparation électorale :** malgré une prise de conscience des risques, « Le Messager » n'est lié à aucun réseau de fact-checking ou de veille, ce qui l'expose aux campagnes de désinformation durant la période électorale.

Ce visuel illustre comment même les médias établis courent des risques systémiques et structurels sans stratégies proactives et inclusives de sécurité numérique.

Étude de cas 2 : Organisation de la société civile – « Civic Watch » (Région du Nord-Ouest)

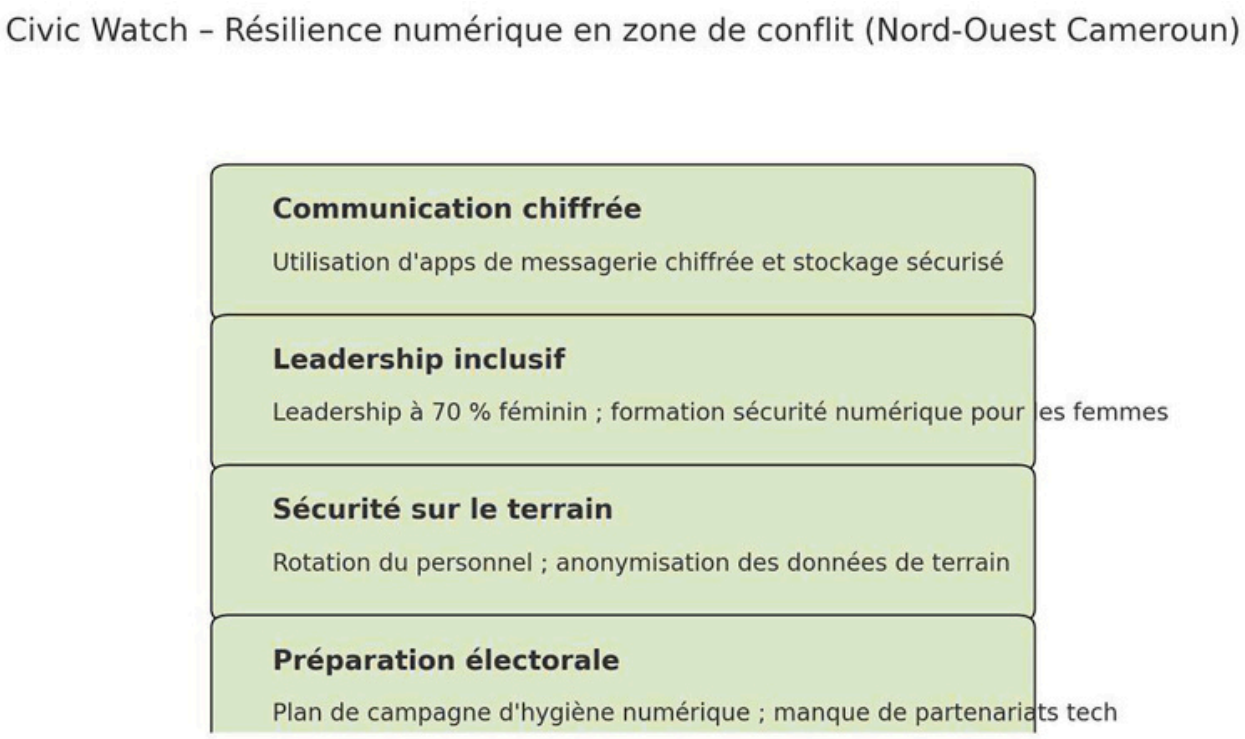
Contexte : « Civic Watch » est une OSC de base à Bamenda, œuvrant pour les droits humains et l'éducation civique dans les communautés affectées par le conflit du Nord-Ouest.

Enseignements clés :

- **Culture proactive :** malgré des ressources limitées, Civic Watch utilise des applications de messagerie chiffrée pour ses communications internes et stocke les données sensibles dans un cloud sécurisé.
- **Leadership féminin :** l'organisation est dirigée à 70 % par des femmes et a déployé des efforts ciblés pour former le personnel féminin à la sécurité numérique ; l'une d'elles a récemment suivi une formation sur la veille des menaces numériques auprès d'un partenaire régional.
- **Adaptation terrain :** sur le terrain, l'insécurité et la surveillance perturbent le travail ; Civic Watch fait régulièrement tourner ses équipes et anonymise les données de terrain pour protéger son personnel.
- **Préparation électorale limitée** : à l'approche des élections, Civic Watch prévoit une campagne de sensibilisation à l'hygiène numérique et à la lutte contre les fake news, mais manque de partenariats techniques et de financements pour la généraliser.

Leçon : Les petites OSC en zones de conflit peuvent servir de modèles de résilience grâce à l'innovation, à la formation communautaire et à des pratiques terrain flexibles, même sans gros budgets.

Figure 10 : Étude de cas – Civic Watch : résilience numérique en zone de conflit dans le Nord-Ouest du Cameroun
Ce visuel présente les pratiques proactives de sécurité numérique de Civic Watch, OSC de terrain à Bamenda.



Source : ADISI-Cameroun

DÉFIS OPÉRATIONNELS LORS DE L'ÉTUDE

Malgré le succès global de la collecte de données, l'étude a rencontré plusieurs difficultés opérationnelles majeures qui ont eu des répercussions sur le calendrier, la portée et la qualité des données dans certains cas :

Manque de réactivité de certaines organisations cibles

- De nombreuses organisations médiatiques et de la société civile invitées n'ont pas répondu aux emails ni aux appels téléphoniques.
- Dans certaines régions—notamment l'Ouest et le Nord-Ouest—cette absence de réponse a persisté même après plusieurs relances par téléphone et WhatsApp.
- Sur 90 organisations contactées, au moins 15 n'ont jamais engagé le dialogue, limitant la diversité et la représentativité des données régionales.

Difficultés de planification des rendez-vous et d'accès aux équipes

- Plusieurs organisations, bien qu'intéressées, n'ont pas pu mobiliser leur personnel dans les délais en raison de contraintes de charge de travail, de déplacements ou de procédures internes.
- Certains entretiens programmés ont été reportés à plusieurs reprises, parfois à la dernière minute, perturbant les plans de terrain.
- Ce phénomène était particulièrement marqué dans les régions du Littoral et du Centre, où les médias ont des horaires imprévisibles ou exigent une validation managériale pour autoriser les interviews.

Barrières de communication entre enquêteurs et coordinateurs

- Malgré l'usage de WhatsApp et des appels téléphoniques, les enquêteurs dans le Sud-Ouest et le Nord-Ouest ont souffert de coupures réseau récurrentes, rendant la coordination en temps réel difficile.
- Des retards d'envoi ou de clarification du questionnaire ont généré des goulots d'étranglement dans le traitement des données.
- L'absence d'un modèle de rapport quotidien centralisé a conduit à des remontées inégales, compliquant le suivi de l'avancement.

Problèmes techniques liés aux outils

- L'utilisation de KoboToolbox en mode hors-ligne a posé des problèmes de compatibilité avec certaines versions d'Android sur les appareils personnels.
- La synchronisation en zones à faible couverture nécessitait parfois des déplacements importants pour capter un réseau exploitable.

- Certaines interviews ont été perdues ou dupliquées en raison d'erreurs de synchronisation, malgré une formation préalable. Des sessions de rappel supplémentaires auraient pu limiter ces incidents.

Enjeux de sécurité et d'accès en zones de conflit

- Dans le Nord-Ouest (Bamenda) et certains secteurs du Sud-Ouest (Buea, Limbé), les enquêteurs se sont sentis en insécurité ou entravés par des barrages et des troubles sporadiques.
- Plusieurs organisations ont préféré des entretiens anonymes ou à distance, craignant des représailles liées à leurs activités de plaidoyer sensible.
- Ces conditions ont rallongé la durée de couverture des terrains et, dans certains cas, conduit à des données partielles.

Recommandations pour les études futures :

- **Engagement précoce :** anticiper les contacts bien avant la phase de terrain pour confirmer la participation et fixer les rendez-vous.
- **Planification flexible :** intégrer des marges de temps pour gérer annulations et reports.
- **Coordination décentralisée :** nommer des superviseurs régionaux pour assurer le suivi et le support en temps réel.
- **Appui technique :** fournir des appareils de rechange et des kits de dépannage, surtout en zones à réseau instable.
- **Protocoles de sécurité :** réaliser des évaluations de risques et former les enquêteurs aux consignes de sécurité en zone sensible.

LIMITES DE L'ÉTUDE

- **Étendue géographique :** bien que l'étude ait couvert les régions du Centre, du Littoral, du Nord-Ouest, du Sud-Ouest et de l'Ouest, certaines zones reculées ou particulièrement instables n'ont pu être atteintes, limitant la richesse des insights pour ces contextes à haute vulnérabilité numérique.
- **Barrières linguistiques :** malgré la mise à disposition des questionnaires en anglais et en français, certains répondants de terrain ont pu ne pas comprendre pleinement les termes techniques, ce qui pourrait avoir altéré la précision de certaines réponses.
- **Contraintes de ressources :** le projet s'est déroulé sur six mois avec un budget restreint, limitant le nombre d'entretiens qualitatifs de suivi et de réunions de validation. Plusieurs enquêteurs ont signalé des difficultés à programmer des secondes interviews, en particulier dans le Nord-Ouest et le Sud-Ouest.
- **Biais d'auto-évaluation :** des réponses peuvent avoir été biaisées à la hausse, les organisations présentant leurs pratiques de sécurité et d'inclusion de genre sous un jour plus favorable. Par exemple, si 67 % affirment un accès égal à la formation, seules 19,5 % ont effectivement des femmes dans des rôles cybersécurité.
- Problèmes de coordination : des délais de communication entre l'équipe projet et certains enquêteurs ont généré des flux de données irréguliers. Quelques collecteurs ont mentionné des difficultés à joindre les responsables d'organisation ou à fixer des rendez-vous dans les délais.

Ces limites ont été atténuées par la triangulation des données, un suivi rapproché des activités de terrain et des vérifications croisées via les fonctions de relance de KoboToolbox.

RECOMMANDATIONS

Institutionnaliser des politiques de sécurité numérique adaptées
Élaborer et maintenir à jour des politiques sur mesure, intégrant des protocoles contre le phishing et les fuites de données, comme l'a illustré Civic Watch en zone de conflit.

Renforcer les programmes de formation inclusifs
Intégrer des sessions régulières et obligatoires pour tous les profils (IT, programme, administration, terrain), avec un focus sur les besoins spécifiques des femmes et des jeunes. Mettre en place des programmes de mentorat pour favoriser l'accès des femmes aux rôles techniques et décisionnels.

Créer des équipes transversales de sécurité numérique
Constituer des comités de sécurité comprenant IT, communication, programme et administration, pour répartir la responsabilité et diffuser la culture de cybersécurité à tous les niveaux.

Améliorer la préparation aux élections
Mettre en place des protocoles d'intervention rapide, des systèmes de veille médiatique pour détecter la désinformation et désigner des référents chargés de coordonner la réponse en période électorale.

Promouvoir un leadership numérique sensible au genre
Inscrire des objectifs de parité dans les politiques internes, définir des trajectoires de carrière pour les femmes en cybersécurité, et développer des contenus de formation adaptés aux sensibilités de genre.

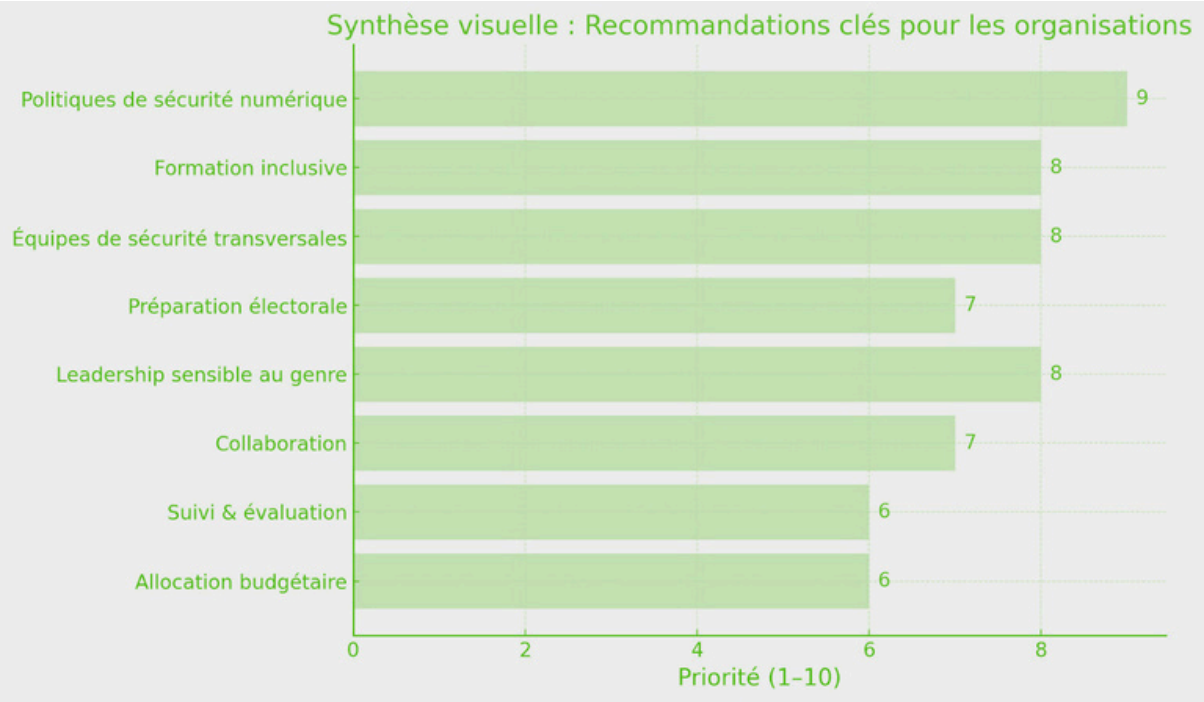
Renforcer la collaboration interne et externe
Tisser des partenariats avec d'autres OSC, des universités et des acteurs publics ou privés spécialisés en cybersécurité. Échanger des bonnes pratiques et établir des protocoles d'intervention communs (MoU).

Mettre en place des outils pratiques de suivi & évaluation
Adopter des tableaux de bord simples (traqueurs d'incidents, check-lists d'auto-évaluation, bilans trimestriels de formation) pour capitaliser sur les incidents et ajuster les stratégies.

Allouer des budgets dédiés à la sécurité numérique
Plaider pour que 5–10 % du budget IT ou opérationnel soit consacré à la cybersécurité (hébergement sécurisé, antivirus, sauvegardes, formations). Sensibiliser donateurs et conseils d'administration à l'importance de ces lignes budgétaires.

Ces recommandations, ancrées dans les réalités du terrain, visent à être pragmatiques, évolutives et adaptées à chaque contexte. Les organisations sont encouragées à démarrer par des actions à faible coût et à monter en puissance au fil des partenariats et des ressources disponibles.

Figure 11 : Synthèse visuelle – Principales recommandations pour les organisations
Cet infographique regroupe de manière visuelle et actionnable les conseils clés pour renforcer la sécurité numérique et promouvoir l'équité de genre : élaboration de politiques, formation inclusive, cadres collaboratifs, leadership sensibilisé au genre et préparation électorale.



Source : ADISI-Cameroun

CONSIDÉRATIONS DE MISE EN ŒUVRE DES RECOMMANDATIONS

Mise en œuvre progressive : Les recommandations doivent être déployées par phases structurées. Les organisations commenceront par un diagnostic approfondi de leurs pratiques actuelles, puis élaboreront des politiques, formeront le personnel et étendront progressivement les protocoles numériques.

Partenariats financiers : Pour assurer la pérennité, les organisations doivent nouer des alliances avec donateurs, acteurs privés et agences internationales afin de cofinancer les améliorations d'infrastructures, l'acquisition de logiciels sécurisés et les programmes de renforcement de capacités à long terme.

Champions régionaux : Identifier et former des référents locaux — particulièrement des personnes ancrées dans leurs communautés — permettra d'adapter les interventions au contexte et de faciliter le partage d'expériences, le suivi de la mise en œuvre et la liaison avec les parties prenantes nationales.

Outils de suivi : Mettre en place des instruments simples et efficaces (journal d'incidents, modèles d'audit, registres de formation) aidera à suivre les progrès, consigner les enseignements et ajuster les stratégies en continu, renforçant ainsi l'apprentissage institutionnel et la reddition de comptes.

Alignement des politiques : Harmoniser les pratiques de sécurité numérique avec les stratégies nationales de transformation digitale, de cybersécurité et d'égalité des genres garantit la cohérence, facilite la conformité et ouvre des opportunités de collaboration et de financements publics.

CONCLUSION

Cette étude avait pour objectif d'analyser l'intersection entre la sécurité numérique et les dynamiques de genre au sein des médias et des organisations de la société civile (OSC) au Cameroun, à l'approche des élections de 2025. Grâce à une méthodologie mixte alliant quantitatif et qualitatif, des données ont été recueillies dans cinq grandes régions (Centre, Littoral, Nord-Ouest, Sud-Ouest, Ouest), révélant défis, bonnes pratiques et innovations structurantes.

Les résultats montrent une disparité nette de préparation numérique selon les régions et les types d'organisations. Certains acteurs, comme Civic Watch dans le Nord-Ouest, font preuve d'ingéniosité malgré des ressources limitées, tandis que d'autres — y compris des médias influents — restent vulnérables faute de cadres, formations ou sensibilisation adaptés. L'équité de genre en leadership numérique demeure un enjeu, les femmes restant sous-représentées dans les postes décisionnels malgré une forte participation aux formations.

Les menaces électorales (désinformation, phishing) apparaissent comme des préoccupations majeures, mais seules quelques organisations disposent des protocoles, partenariats et infrastructures nécessaires pour y faire face. Les contrastes régionaux sont saisissants : les grandes villes bénéficient d'un meilleur soutien technique, alors que les zones de conflit accusent un retard structurant.

Ces constats appellent à l'action :

- Institutionnaliser des politiques et audits de sécurité numérique,
- Déployer des formations inclusives et féministes,
- Renforcer la collaboration entre OSC, médias, experts et autorités,
- Développer la littératie numérique pour contrer la désinformation et préparer les élections.

Malgré les limites identifiées (portée géographique, contraintes logistiques), cette recherche dresse un panorama détaillé et propose une feuille de route stratégique pour renforcer la résilience civique et médiatique du Cameroun à l'ère numérique.

Contacts

ADISI-Cameroun

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

ADISI - CAMEROUN

RAPPORT D'ÉTUDE SUR L'ÉTAT DE LA SÉCURITÉ NUMÉRIQUE ET LES DYNAMIQUE DE GENRE DANS LES MÉDIAS ET ORGANISATIONS DE LA SOCIÉTÉ CIVILE AU CAMEROUN

2025