REPUBLIQUE DU CAMEROUN
Paix – Travail – Patrie

UNIVERSITE DE YAOUNDE I

ECOLE NATIONALE SUPERIEURE POLYTECHNIQUE DE YAOUNDE

DEPARTEMENT DE GENIE INFORMATIQUE

REPUBLIC OF CAMEROON
Peace – Work – Fatherland

UNIVERSITY OF YAOUNDE I

NATIONAL ADVANCED SCHOOL OF ENGINEERING OF YAOUNDE

DEPARTMENT OF COMPUTER SCIENCE

Résumé des exposés

Participant

Matricule : 22P035

Spécialité : Cybersécurité et Investigation Numérique

Noms : MBETSI DJOFANG AIME LINDSEY

Niveau : 4

Superviseur

M. MINKA MI NGUIDJOI Thierry Emmanuel

Année Scolaire : 2025–2026

Table des matières

Introduction

L'univers numérique, en pleine expansion, transforme en profondeur les sociétés modernes, mais s'accompagne de défis sécuritaires et juridiques sans précédent. Les exposés rassemblés ici explorent plusieurs facettes de cette transformation, en se concentrant sur les outils, les risques et les méthodes qui façonnent l'investigation numérique et la cybersécurité aujourd'hui. Qu'il s'agisse de garantir l'authenticité des preuves grâce à des mécanismes cryptographiques avancés comme la non-répudiation, de comprendre la facilité déconcertante avec laquelle on peut falsifier des conversations ou des voix via des deepfakes, ou d'évaluer l'impact des cyberattaques majeures en Afrique, tous ces travaux soulignent une réalité commune : le numérique est à la fois un levier de progrès et un terrain de vulnérabilités critiques. Ils montrent également comment des technologies comme la reconnaissance faciale ou l'IA générative ouvrent de nouveaux horizons opérationnels, tout en exigeant une réflexion urgente sur leur encadrement éthique et juridique. Dans un contexte où la preuve numérique devient centrale pour la justice et où la menace cybernétique ne cesse de croître, ces contributions dressent un état des lieux complet des avancées, des risques et des réponses nécessaires pour naviguer dans cet écosystème complexe.

1 PROTOCOLE ZK-NR : RL et positionnement dans l'investigation numérique moderne

La non-répudiation numérique est présentée comme un enjeu central de la sécurité et de la justice à l'ère du numérique. Dans un monde où la cryptographie ne sert plus seulement à protéger la confidentialité, il devient essentiel de garantir l'authenticité, l'intégrité et surtout l'opposabilité juridique des données. La non-répudiation vise à prouver qu'une action – comme l'envoi d'un message ou la signature d'un document – a bien été réalisée par une personne donnée, qui ne peut ensuite la nier. Pour y parvenir, on s'appuie sur des outils tels que les signatures numériques, les certificats électroniques délivrés par des autorités de certification, les horodatages numériques assurant la traçabilité temporelle et les fonctions de hachage garantissant l'intégrité. Cependant, ces mécanismes classiques atteignent leurs limites face aux nouvelles exigences légales et aux menaces futures, notamment celles issues de l'informatique quantique. C'est dans ce contexte qu'apparaît l'approche **ZK-NR (Zero-Knowledge Non-Repudiation)**, une architecture combinant des primitives cryptographiques post-quantiques permettant de produire des preuves vérifiables sans révéler les données sensibles. Elle s'appuie sur le principe des preuves à divulgation nulle de connaissance et introduit un équilibre entre trois exigences souvent contradictoires : la confidentialité, la fiabilité et l'opposabilité juridique, connues sous le nom de trilemme CRO. Pour surmonter ce défi, plusieurs primitives appelées **CASH** (CEE, AOW, SH) sont proposées : chacune vise respectivement à renforcer la confidentialité, la fiabilité et l'opposabilité. Ces outils permettent d'assurer la validité des preuves numériques, leur traçabilité et leur recevabilité devant les tribunaux tout en protégeant les données confidentielles. Dans le domaine de l'investigation numérique, cette approche s'avère décisive : elle permet de certifier les preuves sans compromettre les enquêtes, de préserver la chaîne de possession et de rendre les analyses opposables en justice. Les exemples de cyberfraude, d'escroquerie ou de trafic télécoms illustrent bien les enjeux concrets de ces mécanismes dans les enquêtes modernes.

En conclusion, la cryptographie devient aujourd'hui un instrument de vérité et de droit : elle ne se limite plus à chiffrer, mais à prouver, certifier et garantir la confiance numérique dans un environnement technologique en mutation rapide.

2 Simulation d'une serie de messages sur WhatsApp entre un homme et sa maitresse

Dans le cadre d'un exercice d'investigation numérique, des échanges compromettants ont été simulés entre un enseignant et une étudiante afin d'illustrer la facilité de fabrication de preuves visuelles. Les éléments remis comprenaient sept captures d'écran et deux photos ; la méthodologie a combiné l'usage de Chatsmock (génération de conversations réalistes : participants, dates, heures, statuts) et des retouches sous Adobe Photoshop (alignements, bulles, insertion d'images) pour augmenter le réalisme et rendre les captures quasi indiscernables au premier regard. Le rapport décrit les limites de Chatsmock (incohérences graphiques avec les dernières versions de l'application, fonctionnalités manquantes comme les notes vocales, dépendance au format image) et compare cet outil à d'autres solutions (FakeChat, WhatsFake, editors avancés et outils forensiques détournés), notant que Photoshop offre une personnalisation plus poussée mais exige des compétences techniques. Il a surtout été montré l'impact de ces outils sur l'investigation : les captures d'écran seules ne sont plus fiables comme preuves, la détection exige des analyses forensiques poussées (métadonnées, horodatages, signatures, récupération des données brutes depuis les appareils ou serveurs) et il existe un risque réel de manipulation judiciaire ou disciplinaire. Pour répondre à ces menaces, le rapport recommande la vérification technique des preuves (métadonnées, origine, horodatage), la préférence pour la collecte des données brutes, l'utilisation d'outils spécialisés de détection de falsification, la formation des acteurs judiciaires et un renforcement du cadre légal encadrant l'acceptation des preuves numériques.

En conclusion, l'exercice démontre qu'il est aujourd'hui simple de créer des preuves numériques trompeuses ; face à cette facilité de falsification, l'investigation numérique doit s'appuyer sur des tech-

niques de vérification rigoureuses et une sensibilisation accrue des experts et des décideurs pour préserver l'intégrité et la recevabilité des preuves.

3 Deepfake Vocal

L'exposé examine le phénomène des deepfakes vocaux — des enregistrements synthétiques créés par l'IA qui imitent une voix humaine à partir d'échantillons — en expliquant leur fonctionnement, leur évolution, leurs usages et les risques concrets pour l'investigation numérique. Il rappelle que la synthèse vocale a progressé depuis les vocoders des années 1960 jusqu'aux percées récentes (WaveNet, Tacotron, outils open-source) qui rendent possible le clonage vocal à partir de quelques secondes d'audio ; cette démocratisation a facilité des usages utiles (accessibilité, doublage, assistants vocaux) mais aussi des détournements (escroqueries, usurpation d'identité, manipulation de l'opinion, falsification de preuves).

Sur le plan technique, l'exposé décrit comment fonctionnent les modèles de clonage (entraînement sur bases de voix, génération via « voice clone » puis insertion de texte via « text-to-speech ») et illustre le procédé avec l'étude de cas MINIMAX audio : capture d'échantillons, création d'un profil vocal, génération de phrases inédites et post-traitement (isolation de voix, réduction de bruit). Les auteurs montrent que le rendu est souvent indiscernable à l'oreille humaine et citent des exemples réels d'escroqueries financières où des voix clonées ont permis des transferts frauduleux, ainsi que des études démontrant la facilité de tromper des systèmes automatiques.

Pour l'investigation numérique, les enjeux sont importants : les deepfakes remettent en cause la confidentialité, la fiabilité et l'opposabilité des preuves (le « trilemme CRO »). Détecter une manipulation exige désormais des analyses forensiques avancées (empreintes acoustiques, artefacts de synthèse, métadonnées, provenance des fichiers) et la capacité à expliquer techniquement ces analyses devant un tribunal. L'exposé insiste aussi sur les dimensions éthiques et sociales (consentement, réputation, risques psychologiques).

Enfin, les contre-mesures proposées combinent technologie, organisation et droit : développement d'outils de détection IA, watermarking/traçabilité des contenus générés, renforcement des mécanismes d'authentification (multi-facteur, biométrie dynamique), formation des acteurs judiciaires et adoption de cadres légaux et chartes éthiques pour l'IA. Les auteurs concluent que, si le deepfake vocal ouvre des possibilités positives, il exige une réponse coordonnée (technique, juridique et éducative) pour préserver la confiance et l'intégrité des preuves numériques.

4 A l'aide d'une IA, réaliser une vidéo dans laquelle le chef de groupe dispense le premier chapitre du cour : Deepfake

L'émergence de l'intelligence artificielle générative a profondément transformé les méthodes de création de contenus numériques en offrant de nouvelles possibilités dans des domaines variés tels que la communication, la pédagogie, le divertissement et la recherche. Ce travail se concentre sur la réalisation d'une vidéo pédagogique sous forme de deepfake, combinant les capacités du modèle GPT-5 pour la rédaction du script et de la plateforme HeyGen AI pour la génération vidéo. Le deepfake est défini comme un enregistrement vidéo ou audio réalisé ou modifié grâce à l'IA, produisant des contenus faux rendus très crédibles par l'intelligence artificielle. Cette technologie repose sur les réseaux antagonistes génératifs (GAN), où deux algorithmes s'entraînent mutuellement à produire et identifier les faux.

Cependant, les deepfakes présentent aussi des inconvénients, notamment la propagation rapide de fausses informations via les réseaux sociaux. Plusieurs initiatives, comme un projet de désidentification développé par Facebook FAIR ou les cadres législatifs de la CNIL, visent à limiter les abus tout en protégeant la vie privée et le droit à l'image, essentiels face aux enjeux stratégiques et politiques qui se posent. HeyGen AI, créée en 2022, est une IA spécialisée dans la génération rapide de vidéos réalistes à partir de simples instructions textuelles, accessible sans compétences techniques poussées, utilisée notamment pour la création de contenus, le journalisme, la communication d'entreprise ainsi

que l'enseignement. GPT-5, sorti en août 2025, est un modèle d'OpenAI combinant rapidité et raisonnement approfondi, capable de générer non seulement du texte mais aussi du code, des images et des applications complètes, avec une capacité étendue à gérer de longs échanges cohérents.

La réalisation vidéo consistait à créer une vidéo dans laquelle le chef de groupe présente le premier chapitre du cours. GPT-5 a permis la génération précise du script, tandis que HeyGen a créé un avatar vidéo réaliste à partir de ce script, agrémenté de voix synthétiques avancées, clonage vocal, traduction multilingue et processus automatisé de création. Ce projet illustre la complémentarité entre traitement du langage naturel et synthèse d'images pour produire des contenus immersifs. En conclusion, ce travail démontre le potentiel significatif de l'IA générative pour créer des contenus audiovisuels innovants, tout en soulignant la nécessité de prendre en compte les limites techniques, les risques d'abus et les enjeux éthiques liés à l'utilisation de telles technologies, ouvrant ainsi la voie à une réflexion approfondie sur leur intégration responsable dans la société.

5 Les trois meilleurs logiciels de rédaction de mémoire

L'exposé porte sur les outils logiciels essentiels pour la rédaction efficace d'un mémoire académique, un travail d'envergure aux multiples exigences, allant de la structuration du contenu à la gestion rigoureuse des références bibliographiques. Face à la complexité et aux nombreuses contraintes liées à la rédaction de documents longs et formels, le choix des outils devient un facteur déterminant pour la réussite de l'étudiant. Trois types d'outils sont analysés en détail : Overleaf, Microsoft Word et Zotero. Overleaf est présenté comme une plateforme LaTeX collaborative qui a révolutionné la rédaction scientifique en rendant accessible la puissance de LaTeX sans installation complexe. Elle se distingue par son approche orientée vers la qualité typographique et la gestion avancée des références, idéale pour les disciplines scientifiques qui exigent précision et rigueur. Cependant, Overleaf présente une courbe d'apprentissage assez raide, et certaines difficultés en édition hors ligne, ce qui peut représenter un frein pour certains utilisateurs.

Microsoft Word reste l'outil universel le plus répandu grâce à sa large diffusion, sa compatibilité avec la plupart des institutions et son interface familière qui facilite la prise en main immédiate. Word offre des fonctionnalités avancées pour le référencement, la gestion des styles et la collaboration, notamment via le suivi des modifications et les commentaires. Néanmoins, il présente des limites dans la gestion bibliographique native et peut être instable sur des documents très volumineux ou complexes, ce qui peut nuire à l'efficacité dans le cadre de travaux académiques exigeants.

Zotero, quant à lui, est un gestionnaire de références bibliographiques open-source, spécialement conçu pour la recherche académique. Il facilite la centralisation, l'organisation et l'exploitation des sources, avec des fonctionnalités avancées telles que la capture automatique des métadonnées, l'intégration transparente avec des outils de rédaction comme Word ou Overleaf, et la gestion de milliers de styles de citation. Zotero se démarque par son écosystème extensible, sa gratuité et sa capacité à s'adapter aux différents workflows académiques.

L'exposé met également en évidence les combinaisons gagnantes entre ces outils pour optimiser le processus de rédaction. L'association Word-Zotero est plus accessible et convient aux étudiants débutants ou ceux qui préfèrent un environnement familier. La combinaison Overleaf-Zotero représente le choix d'excellence pour les disciplines scientifiques, conjuguant qualité typographique et rigueur bibliographique. Pour les travaux collaboratifs, l'option Overleaf avec Zotero Groups permet un travail synchronisé en temps réel, particulièrement adaptée aux thèses et projets d'équipe.

Un tableau comparatif des fonctionnalités met en lumière les forces et faiblesses relatives de ces solutions, soulignant que la réussite de la rédaction dépend plus de la complémentarité des outils que d'un choix exclusif. La conclusion insiste enfin sur le fait que, malgré toute la sophistication des outils logiciels, la qualité du contenu et la profondeur de la réflexion restent primordiales. La maîtrise technique doit toujours s'accompagner d'un travail intellectuel sérieux pour assurer le succès académique.

Ce résumé reflète ainsi la richesse et la cohérence de l'exposé, fournissant une vision complète des enjeux, des outils et des stratégies optimales pour la rédaction d'un mémoire selon les différents profils

et besoins des étudiants.

6 Les algorithmes de reconnaissance faciale

Cet exposé traite de la reconnaissance faciale, une technologie biométrique d'intelligence artificielle qui permet d'identifier ou de vérifier l'identité d'une personne à partir de ses traits faciaux. Cette technique repose sur des algorithmes capables de détecter, analyser et comparer des caractéristiques faciales uniques, telles que la distance entre les yeux, la forme du nez, les contours de la mâchoire ou des lèvres. Très utilisée dans des domaines variés comme la sécurité, la vidéosurveillance, le contrôle d'accès ou encore le déverrouillage de smartphones, la reconnaissance faciale soulève néanmoins d'importants enjeux éthiques et juridiques, notamment en matière de protection des données personnelles et de respect de la vie privée.

Un système biométrique de reconnaissance faciale fonctionne en plusieurs étapes : l'enrôlement (où le visage est capturé, prétraité et enregistré), l'identification (qui consiste à retrouver une identité sans qu'elle soit explicitement donnée), et la vérification (comparaison de l'image faciale avec un profil pour valider une identité). L'architecture de ces systèmes comprend quatre modules clés : la capture des données, l'extraction des caractéristiques faciales, la correspondance avec les modèles en base, et la décision d'identification ou de rejet. Plusieurs méthodes sont utilisées pour la reconnaissance, allant des approches classiques basées sur des statistiques et analyses globales ou locales, aux méthodes modernes d'apprentissage automatique comme le deep learning, qui améliorent la robustesse et la précision mais restent souvent opaques algorithmique.

L'exposé insiste sur l'importance d'évaluer un système de reconnaissance faciale au-delà de ses performances techniques brutes, en prenant en compte sa sécurité, ses vulnérabilités, et ses impacts éthiques, sociaux et juridiques. Parmi les limites, on trouve les erreurs liées à des conditions réelles difficiles (faible luminosité, angles extrêmes, masques), les attaques adversariales qui peuvent compromettre l'intégrité des données, ainsi que les risques d'usurpation par deepfakes ou autres techniques de manipulation. Les impacts éthiques concernent la protection de la vie privée, le risque de discrimination dû à des biais algorithmiques, et l'effet dissuasif sur les libertés civiles. D'un point de vue juridique, la conformité au cadre légal, la responsabilité en cas d'erreur, et la traçabilité du système sont des points critiques pour assurer la validité des preuves et la légitimité des usages.

Sur le plan organisationnel et opérationnel, la mise en œuvre de la reconnaissance faciale nécessite des investissements importants en matériel, infrastructure, formation du personnel et procédures rigoureuses. L'acceptabilité sociale et institutionnelle est également un facteur clé, car la résistance ou la méfiance peut nuire à l'efficacité du système. Enfin, l'usage des technologies de reconnaissance faciale doit être défini avec clarté, en respectant la proportionnalité, la finalité et la légitimité, par exemple en limitant l'identification aux seuls cas justifiés par des mandats judiciaires.

L'exposé propose plusieurs recommandations pour un déploiement maîtrisé au contexte camerounais : documentation précise du pipeline technique, tests de performance sur des données locales, intégration de tests de sécurité réguliers, mise en place de mesures anti-usurpation, analyses d'impact éthique publiées, alignement avec les lois nationales, formation des opérateurs, déploiements pilotes contrôlés, et surtout validation humaine des résultats pour toute décision critique. Ces mesures visent à concilier innovation, efficacité opérationnelle et respect des droits fondamentaux.

La conclusion rappelle que la reconnaissance faciale est un outil puissant pour l'investigation numérique et la cybersécurité, capable de traiter rapidement de vastes volumes de données visuelles dans des contextes sensibles. Néanmoins, son succès dépend d'un cadre juridique clair, d'une gouvernance transparente et d'une utilisation proportionnée, afin d'éviter les dérives, les erreurs judiciaires, les atteintes à la vie privée et les discriminations. Une intégration responsable et supervisée de cette technologie est donc essentielle pour garantir son utilité tout en préservant les libertés individuelles au Cameroun. Ce travail apporte ainsi une réflexion complète sur les aspects techniques, éthiques, légaux et organisationnels relatifs à la reconnaissance faciale dans un contexte d'investigation numérique.

7 Conception et analyse d'un faux profil TIKTOK : choix d'une niche dans le cadre d'une investigation numérique

Cet exposé analyse la création et la gestion d'un faux profil TikTok dans une démarche d'investigation numérique à visée pédagogique, centrée sur la cybersécurité. Il s'inscrit dans un contexte où les réseaux sociaux, et particulièrement TikTok, jouent un rôle majeur dans la formation de l'opinion, l'influence des comportements et les interactions, notamment chez les jeunes. Le projet avait comme objectif d'étudier la viralité des contenus liés à la cybersécurité, un domaine technique et sensible, en observant les réactions et interactions générées par ce faux profil, tout en respectant une éthique stricte pour éviter toute atteinte à la vie privée ou usurpation réelle.

La démarche méthodologique a débuté par la création de ce faux profil à l'aide d'une adresse mail temporaire, afin de garantir l'anonymat des véritables auteurs. Le choix de la niche cybersécurité se justifie par l'importance croissante des menaces numériques, des attaques informatiques et de la nécessité de sensibiliser les internautes aux bonnes pratiques de sécurité en ligne. Le contenu diffusé sur le profil mêlait information éducative et ton léger, parfois humoristique, avec pour but d'engager un large public sur des thèmes accessibles : la sécurité des mots de passe, la protection des données personnelles, les arnaques en ligne.

Pour maximiser l'impact, plusieurs outils ont été utilisés, comme TikTok Analytics pour suivre l'engagement, ChatGPT pour la rédaction des messages, Canva pour la création des visuels et Temp Mail pour la gestion du compte. Le profil a rapidement suscité un intérêt notable, avec plus de 100 mentions « j'aime » et six contenus stratégiques publiés, chacun conçu pour être pertinent et respectueux des règles. Ces publications combinaient sensibilisation, mises en situation et appel à la réflexion critique sur la cybersécurité.

L'analyse des résultats a montré que la stratégie déployée a permis non seulement de capter l'attention d'un public diversifié mais aussi de stimuler leur curiosité envers des sujets souvent négligés. Cependant, des limites éthiques ont été soulignées, notamment sur la prudence nécessaire dans l'utilisation des faux profils, même à visée éducative, pour éviter tout malentendu ou exploitation abusive. Ce projet montre aussi combien les réseaux sociaux ont un pouvoir fort de manipulation, d'où la nécessité d'un encadrement éthique rigoureux.

Enfin, des recommandations ont été formulées pour renforcer l'éducation à la cybersécurité dès le secondaire, promouvoir une utilisation responsable des outils numériques, intégrer des exercices pratiques dans les cursus, encadrer légalement l'usage de faux profils pédagogiques et encourager la collaboration entre domaines techniques, juridiques et communicationnels.

En conclusion, ce travail a démontré qu'une investigation numérique bien encadrée, utilisant intelligemment des stratégies de contenu et des outils numériques, permet de sensibiliser efficacement à la cybersécurité sur TikTok. Il met en lumière l'importance cruciale d'une approche éthique et responsable dans ce type de projet, ainsi que la nécessité pour tout acteur du numérique de maîtriser les outils digitaux tout en développant une réflexion critique sur leurs impacts potentiels. Cette expérience confirme que l'éducation à la cybersécurité peut être interactive, engageante et adaptée aux réalités actuelles, offrant une contribution précieuse à la prévention dans un monde de plus en plus connecté.

8 L'utilité de l'investigation numérique dans la police judiciaire

Le premier document expose l'importance de l'investigation numérique pour la police judiciaire, en particulier au Cameroun. Il explique que cette discipline, qui consiste à recueillir, analyser et présenter des preuves numériques, est devenue indispensable dans un monde de plus en plus numérisé et confronté à la cybercriminalité. L'exposé détaille ses apports majeurs : accéder à des preuves invisibles dans le monde physique, lutter contre la cybercriminalité, identifier et tracer les auteurs, reconstituer des événements, produire des preuves recevables en justice et soutenir les enquêtes traditionnelles. Il présente également ses domaines d'application, comme la lutte contre la criminalité financière, le terrorisme, la criminalité organisée ou la pédopornographie, en illustrant par des exemples concrets

camerounais. Enfin, il aboute les outils techniques utilisés, mais aussi les défis et limites auxquels fait face le Cameroun, tels que l'explosion du volume de données, le respect des droits fondamentaux, le manque d'experts, les contraintes juridiques, matérielles et financières. La conclusion souligne que, malgré ces obstacles, l'investigation numérique est un pilier stratégique et qu'il est crucial d'investir dans la formation, les moyens logistiques et l'adaptation du cadre juridique pour renforcer la sécurité nationale.

9 Les 10 cas africains les plus importants en hacking durant les 10 dernières années

Le second document dresse un panorama des cybermenaces en Afrique en se focalisant sur les dix cas de piratage les plus marquants de la dernière décennie. Il commence par contextualiser la cybersécurité en Afrique, notant une numérisation rapide mais une vulnérabilité accrue due à un manque d'infrastructures solides, de compétences locales et de cadres juridiques adaptés. La méthodologie d'investigation numérique est présentée, structurée autour de l'identification, la collecte, la préservation, l'analyse et la restitution des preuves. Les cas sont sélectionnés selon des critères précis : taille de l'attaque, type d'organisation ciblée, volume de données affectées et impact financier ou réputationnel. Parmi les cas emblématiques analysés figurent le rançongiciel contre Transnet en Afrique du Sud, la fuite de données à la CNSS au Maroc, l'attaque contre Eneo au Cameroun, le ransomware GhostLocker 2.0 en Égypte, le scandale Pegasus au Maroc, le piratage de banques en Côte d'Ivoire, la cyberattaque du système de santé tunisien, le piratage d'Ethiopian Airlines, la fraude au mobile money chez MTN Nigeria et l'intrusion à la banque centrale du Nigeria. L'exposé se termine par des recommandations clés, incluant la formation massive d'experts, la création de centres de réponse aux incidents, l'harmonisation des lois cybernétiques et le développement d'une infrastructure cloud souveraine, afin de construire une cybersécurité résiliente et une souveraineté numérique pour l'Afrique.

Conclusion

L'ensemble de ces exposés converge vers un constat clair : la maîtrise du numérique est devenue un impératif stratégique pour la sécurité, la justice et la souveraineté des États, particulièrement en Afrique. Face à la sophistication croissante des cybermenaces – qu'il s'agisse de ransomwares paralysant des infrastructures vitales, de campagnes de désinformation ou de falsifications profondes de preuves –, l'investigation numérique s'impose comme un pilier indispensable. Cependant, son efficacité est étroitement liée à la robustesse des cadres juridiques, à la disponibilité d'expertise technique locale et à la vigilance éthique constante. Les technologies émergentes, qu'elles soient utilisées pour prouver, identifier ou tromper, ne sont ni bonnes ni mauvaises en elles-mêmes ; tout dépend de l'usage qui en est fait et des garde-fous mis en place. Il est donc crucial d'investir massivement dans la formation, la coopération régionale, l'innovation responsable et l'adaptation des lois pour que le numérique reste un espace de confiance et de droit. En définitive, l'avenir de la sécurité numérique en dépend : sans une approche équilibrée, alliant technicité, éthique et gouvernance, la course entre ceux qui protègent et ceux qui attaquent pourrait bien être perdue.