



RÉPUBLIQUE TOGOLAISE



RAPPORT D'ACTIVITÉS

2025



Agence Nationale de la Cybersécurité (ANCy)

RAPPORT D'ACTIVITÉS DE L'AGENCE NATIONALE DE LA CYBERSECURITÉ



2025



Sommaire

Liste des sigles et abréviations	7
Liste des graphiques.....	8
Liste des figures	8
Mot du Directeur Général.....	9
Introduction.....	10

I. Synthèse exécutive

II. Gouvernance et cadre institutionnel

2.1. L'Agence Nationale de la Cybersécurité (ANCy)	16
2.1.1. Fondement juridique	16
2.1.2.1. Les textes portant création, organisation et fonctionnement de l'ANCy.....	16
2.1.2.2. Les textes relatifs à la cybersécurité, à la cybercriminalité et encadrant les services numériques, les infrastructures critiques et les prestataires de services de confiance	16
2.1.2.3. Les conventions et instruments internationaux ratifiés par le Togo	17
2.1.3. Attributions et missions	17
2.1.4. Organisation et gouvernance	18
2.1.4.1. Le Comité Stratégique.....	19
2.1.4.2. La Direction Générale.....	20

III : Performance organisationnelle

3.1. Gestion et évolution des ressources humaines.....	24
3.2. Renforcement interne des compétences.....	24
3.3. Lancement de recrutements stratégiques	24
3.4. Amélioration des capacités logistiques	24
3.4.1. Mise en place d'un cadre d'accueil des stagiaires.....	24
3.4.2. Extension du parking automobile de l'Agence.....	25
3.4.3. Installation de bureaux mobiles.....	25
3.4.4. Acquisition d'équipements mobiliers.....	25

IV : Mise en oeuvre stratégique de la SNCy

4.1. Gouvernance et conformité	28
4.1.1. Supervision des Opérateurs de Services Essentiels (OSE)	28
4.1.2. Lancement du processus de qualification des prestataires de services de confiance.....	28
4.2. Développement des compétences	31
4.2.1. Programme national de formations certifiantes en cybersécurité	31
4.2.2. Focus : Inclusion féminine	33
4.2.3. Capture The Flag National	34
4.3. Promotion d'une culture nationale de cybersécurité	36
4.3.1. Promotion de la culture de cybersécurité dans les enseignements primaire, secondaire et supérieur	36
4.3.2. Tournée nationale de sensibilisation.....	37
4.3.3. Sensibilisation des agents de l'Établissement Public et Autonome pour l'exploitation des Marchés (EPAM).....	39
4.3.4. Sensibilisation lors de la célébration de la Journée internationale des droits des femmes à l'Université de Lomé	41

4.3.5. Sensibilisation du personnel de l'Agence Nationale de l'Aviation Civile (ANAC)	42
4.3.6. Opération rentrée scolaire sûre 2025-2026.....	43
4.3.7. Sensibilisation du personnel administratif de TotalEnergies Togo.....	44
4.3.8. Sensibilisation des jeunes sur la protection des données personnelles	45
4.3.9. Rencontre annuelle de l'ANCy avec les médias nationaux	46
4.3.10. Sensibilisation des étudiants de l'ENA	47
4.3.11. Sensibilisation au Fonds National de la Finance Inclusive (FNFI)	48
4.3.12. Autres sensibilisations	48
4.4. Activités de renforcement des capacités des équipes	48
4.4.1. Renforcement de la posture de sécurité des administrations publiques et structures critiques	48
4.4.2. Participation aux cafés de la cybersécurité	49
4.5. Coopération internationale et positionnement régional	50
4.5.1. Signature de plusieurs mémorandums d'entente.....	50
4.6. Lutte contre la cybercriminalité	51
4.6.1. Typologie des cybercrimes recensés.....	51
4.6.2. Analyse des cas recensés	51
4.6.3. Tendances observées.....	52
4.6.4. Actions futures	52
4.7. Veille, prévention, et gestion des incidents	52
4.7.1. Veille et alerte : les activités SOC	54
4.7.1.1. Chiffres clés de 2025	54
4.7.1.2. Évolution des données au cours de l'année 2025.....	55
4.7.1.3. Évolution des données clés depuis le démarrage du SOC.....	56
4.7.1.3.1. Incidents traités	56
Respect des SLA.....	57
4.7.2. Réponse aux incidents : les activités CERT	58
4.7.2.1. Tableau des incidents traités	58
4.7.2.2. Évolution des incidents traités	59
4.7.2.3. Répartition des incidents CERT traités en 2025	60
4.7.2.4. Audit de sécurité pour les entités gouvernementales	61
4.7.2.5. Alertes sur les vols d'identifiants (Stealers)	61
4.7.2.6. Surveillance des sites web	61
4.7.3. Site web CERT.tg	62
4.7.3.1. Métriques principales 2025.....	62
4.7.3.2. Principales sources de trafic.....	63
4.7.3.3. Audience géographique (Top 20)	64
4.7.3.4. Audiences africaines	65
4.7.4. Formations et sensibilisations à la cybersécurité	66
4.7.4.1. Sensibilisation en présentiel	66
4.7.4.2. Participation à des événements et ateliers	66
4.7.4.3. GC3B (Geneva 14-15 mai 2025)	67
4.7.4.4. Participation à la FIRST Conference 2025 (Copenhague).....	68
4.7.4.5. Les cafés de la cybersécurité	70
4.7.4.6. Forum International pour la Protection des Données à caractères Personnelles	70
4.7.4.7. Rencontre Annuelle du BIC-UEMOA	71
4.7.4.8. La GRIT	73
4.7.4.9. Signature d'un MoU entre CDA et TogoTech	73
4.7.4.10. LOS CON 2025	74
4.7.4.11. Sponsoring de l'Equipe Africaine AFRICC pour le Cybersecurity Challenge Tokyo 2025	75

V : Communication institutionnelle et relations publiques

5.1. Relations presse et médias.....	78
5.2. Communication digitale et supports institutionnels	79
5.3. Événements, conférences et ateliers thématiques	81
5.3.1. African cybersecurity summit (Rabat)	81
5.3.2. Cyber Africa Forum 2025	82
5.3.3. Togo IT Days.....	83
5.3.4. Salon International des Professionnels de l'Économie Numérique de l'UEMOA (SIPEN UEMOA)	84
5.3.5. Convention des Nations Unies contre la cybercriminalité.....	87
5.3.6. Grande Rencontre de l'Innovation Technologique.....	88
5.3.7. Maputo Cyber Week.....	90
5.3.8. La Nuit du Droit	91

VI : Difficultés structurelles

6.1. Difficultés organisationnelles	94
6.1.1. Déficit de compréhension stratégique de certains décideurs.....	94
6.1.2. Insuffisance voire inexistence des budgets dédiés à la cybersécurité	94
6.2. Difficultés opérationnelles.....	94
6.2.1. Difficultés des entités à disposer de RSSI compétents et suffisamment outillés	94
6.2.2. DSI disposant de pouvoirs décisionnels limités	94
6.3. Difficultés techniques	95
6.3.1. Sophistication croissante des cybermenaces (IA et automatisation)	95
6.3.2. Utilisation persistante de logiciels piratés ou non-licenciés	95
6.3.3. Obsolescence des applicatifs et des solutions informatiques	95
6.3.4. Insuffisance des infrastructures numériques sécurisées.....	95
6.3.5. Non-application régulière des correctifs de sécurité (patch management)	96
6.3.6. La sensibilisation et l'adoption des bonnes pratiques	96

VII : Perspectives stratégiques 2026

7.1. Renforcement de la gouvernance nationale de la cybersécurité.....	99
7.2. Montée en compétences et formation des acteurs clés.....	99
7.3. Modernisation et sécurisation des infrastructures numériques.....	99
7.4. Sensibilisation et culture de cybersécurité	100
7.5. Adaptation des programmes de sensibilisation	100

Conclusion

Remerciements

Liste des sigles et abréviations

ADNEC	Abu Dhabi National Exhibition Centre
ANCy	Agence Nationale de la Cybersécurité
ANID	Agence Nationale d'Identification
ARCOP	Autorité de Régulation de la Commande Publique
ARSE	Autorité de Régulation du Secteur de l'Energie
ASAIGE	Autorité de Sécurité de l'Aéroport International Gnassingbé Eyadema
ATD	Agence Togo Digital
CDA	Cyber Defense Africa
CEDEAO	Communauté Économique des États de l'Afrique de l'Ouest
CERT	Computer Emergency Response Team
CIFAF	Centre International de Formation en Afrique des Avocats Francophones
CNDH	Commission Nationale des Droits de l'Homme
CPES	Cellule Présidentielle d'Exécution et de Suivi des projets prioritaires
CSIRT	Computer Security Incident Response Team
CTF	Capture The Flag
DCPJ	Direction Centrale de la Police Judiciaire
EPL	École Polytechnique de Lomé
EPS	Évènement par Seconde
FAIEJ	Fonds d'Appui aux Initiatives Économiques des Jeunes
FIHA	Festival International d'Histoire d'Aného
FISA	Forum International des Secrétaires et Assistant Administratif
FITD	Forum International sur la Transformation Digitale
FNFI	Fonds National de la Finance Inclusive
INAM	Institut National d'Assurance Maladie
IPDCP	Instance de Protection des Données à Caractère Personnel
IYF	International Youth Fellowship
MENTD	Ministère de l'Économie Numérique et de la Transformation Digitale
PME/PMI	Petites et Moyennes Entreprises / Petites et Moyennes Industries
PR	Président de la République
SIEM	Security Information and Event Management
SNCy	Stratégie Nationale de Cybersécurité
SOC	Security Operation Center

Liste des graphiques

Graphique 1 : Nombre de certifiés au 31 décembre 2025 par formation	32
Graphique 2 : Nombre de certifiés au 31 décembre 2025 par genre.....	33

Liste des tableaux

Tableau 6 : Nb Alertes sur les sites web surveillés	61
Tableau 7 : Tableau des métriques du site web cert.tg	62
Tableau 8 : Tableau des sources de trafic du site web cert.tg.....	63
Tableau 9 : Top 20 des audiences géographiques	64
Tableau 10 : Tableau des audiences africaines	65

Liste des figures

Figure 1 : Organigramme de l'ANCy	19
Figure 2 : Géolocalisation de l'ANCy 17.....	20
Figure 3 - Incidents traités.....	54
Figure 4 - Évolution des données collectées en 2025.....	55
Figure 5 - Évolution des incidents traités depuis le démarrage du SOC.....	56
Figure 6 - Niveau des SLA en 2025.....	56
Figure 7 - Évolution du pourcentage de respect des SLAs depuis le démarrage du SOC	57
Figure 8 - Évolution des incidents CERT	59
Figure 9 - Évolution des incidents CERT par mois.....	59
Figure 10 - Évolution des incidents CERT par année	60
Figure 11 - Répartition des incidents CERT traités.....	60

Liste des photos

Photo 1 : Siège de l'ANCy	6	
Photo 2 : Photo des officiels à la cérémonie de lancement des formations	23	
Photo 3 : Une cohorte de bénéficiaires des formations	24	
Photo 4 : Vue partielle de candidates au test de sélection	26	
Photo 5 : Une équipe participante	27	
Photo 6 : Les lauréats posant avec le DG de l'ANCy	28	
Photo 7 : Le classement des 10 équipes participantes avec les scores.....	25	
Photo 8 : Les superviseurs en pleine injection des challenges	29	
Photo 9 : Des membres du comité technique de l'enseignement supérieur en séance de travail	30	
Photo 10 : Vue partielle de l'assistance à Guérin-Kouka (Dankpen)..	31	
Photo 11 : Le préfet de Doufelgou, lors de la sensibilisation à Niamtougou	31	
Photo 12 : Photo de famille des participants à Tandjoaré	32	
Photo 13 : M. GERALDO Malik, Directeur de la Formation, présentant l'ANCy aux populations de Djarkpanga (Mô)	32	
Photo 14 : Ouverture des travaux par la Directrice Générale de l'EPAM, Commissaire Somialo KADJA (au centre).....	33	
Photo 15 : Vue partielle des participants	34	
Photo 16 : Mlle Fabiola KOUDAM (à l'extrême droite), présentant sa communication de sensibilisation	34	
Photo 17 : Vue partielle du personnel sensibilisé	36	
Photo 18 : Sensibilisation sur la TVT dans l'émission L'bala.....	37	
Photo 19 : M. Malik GERALDO, s'adressant personnel sensibilisé	38	
Photo 20 : M. Armel BEHANZIN, Responsable Commercial de CDA entretenant les participants.....	38	
Photo 21 : Le Président de l'IPDCP, Col. Bédiani BELEI, lors de son intervention.....	39	
Photo 22 : L'assistance lors de la sensibilisation	40	
Photo 23 : Photo de famille avec le DG de l'ANCy et les professionnels des médias	41	
Photo 24 : Les étudiants attentifs à la sensibilisation.	42	
Photo 25 : Vue partielle des participants à la sensibilisation	42	
Photo 26 : Des agents de l'ANCy aux côtés du DG de l'ANCy (au centre, en veste sans cravate) et du DG de CDA (à l'extrême droite) lors d'un café de la cybersécurité.	44	
Photo 27 : Le Cdt Gbota GWALIBA, DG de l'ANCy prenant la parole lors d'un café de la cybersécurité.....	44	
Photo 28 : Échange de paraphes après signature de MoU entre le Togo et le Mozambique.....	45	
Photo 29 : M. Simon MELCHIOR, DG de CDA et Mme Belynda LAWSON-BETUM, la responsable marketing de CDA	61	
Photo 30 : Quelques partenaires rencontrés au GC3B	62	
Photo 31 : Des participants à la FIRST 2025	63	
Photo 32 : Des participants aux cafés	64	
Photo 33 : Un panel modéré par la responsable marketing et communication de CDA, à l'extrême gauche	65	
Photo 34 : M. ASSIH (au micro) lors de son intervention	66	
Photo 35 : Le stand de CDA animé par une stagiaire	67	
Photo 36 : Mme le Ministre Cina LAWSON, posant avec Me Alexis ACQUEREBURU, Maire des Lacs 1 (à l'extrême droit), M. Simon MELCHIOR, DG de CDA et Mme Gael EGBIDI, Présidente de TogoTech.....	67	
Photo 37 : Échange de paraphes entre les signataires du MoU	68	
Photo 38 : Daniel GOGO et Charles ASSIMTI, représentants du Togo au ICC Tokyo 2025	69	
Photo 39 : Le DG de l'ANCy (à gauche) et le DT de CDA à l'ACS Rabat 2025.....	73	
Photo 40 : Les représentants de l'ANCy (2è et 4è à partir de la gauche) et de CDA au CAF 2025	74	
Photo 41 : Le Cdt Gbota GWALIBA, DG de l'ANCy lors du panel auquel il participait	75	
Photo 42 : Un panel modéré par la responsable marketing et communications de CDA.....	76	
Photo 43 : Le président vietnamien Luong Cuong posant avec les chefs de délégations participant à la cérémonie d'ouverture	79	
Photo 44 : Madame le Ministre Cina LAWSON (au centre en tenue blanche)posant avec les invités et partenaires à l'ouverture officielle du sommet	80	
Photo 45 : Une promotrice de startup présentantsa solution	81	
Photo 46 : Le Commandant Gbota GWALIBA (premier de la gauche), DG de l'ANCy prenant part à un panel d'experts	82	
Photo 47 : M. OTIMI (au micro), intervenant lors du panel	83	



Les résultats obtenus traduisent une montée en maturité progressive de l'écosystème national de cybersécurité.

Mot du Directeur Général

L'année 2025 marque une étape structurante dans la consolidation de la gouvernance nationale de la cybersécurité au Togo.

Dans un environnement international caractérisé par l'intensification des cybermenaces, la digitalisation accélérée des services publics et l'émergence de technologies disruptives, la cybersécurité constitue désormais un enjeu stratégique de souveraineté, de stabilité institutionnelle et de compétitivité économique.

Conformément à la vision portée par Son Excellence Monsieur Faure Essozimna GNASSINGBÉ, Président du Conseil, l'Agence Nationale de la Cybersécurité a poursuivi, avec rigueur et méthode, la mise en œuvre de la Stratégie Nationale de Cybersécurité à travers des actions structurantes articulées autour de la gouvernance, du développement des compétences, de la conformité des infrastructures critiques et de la coopération internationale.

L'année 2025 a été marquée par des avancées significatives, notamment le lancement du processus national de qualification des prestataires de services de confiance, le démarrage d'un programme de formations certifiantes au profit de 250 informaticiens, le renforcement de la supervision des Opérateurs de Services Essentiels ainsi que la consolidation des partenariats bilatéraux en matière de cyberdéfense.

L'année 2026 sera consacrée au changement d'échelle, avec l'évaluation à mi-parcours de la Stratégie Nationale de Cybersécurité et le renforcement du pilotage par indicateurs de performance.

La cybersécurité n'est plus une option. Elle est une condition de confiance et un moteur de développement.

Commandant Gbota GWALIBA
Directeur Général

Introduction

Au fil des dernières années, le numérique a profondément transformé le quotidien des Togolaises et des Togolais. Les services publics se digitalisent, les entreprises innovent avec un encrage digital et les citoyens utilisent de plus en plus les outils numériques pour communiquer, travailler, accéder aux services et s'informer. Le digital s'impose progressivement comme un levier essentiel de développement économique et social. Cette évolution ouvre de réelles opportunités de développement, mais elle expose également notre pays à de nouveaux risques liés à la cybersécurité.

Protéger les systèmes d'information, sécuriser les données, préserver la confiance des usagers et garantir la continuité des services numériques sont désormais des enjeux quotidiens pour l'État, les organisations et les citoyens. La réussite de la transition numérique du Togo repose donc sur la capacité collective à anticiper et à maîtriser ces risques. Le Gouvernement togolais, conscient de ces enjeux, a fait de la cybersécurité une priorité stratégique, notamment à travers la mise en œuvre de la Stratégie Nationale de Cybersécurité.

C'est pour répondre à ces défis que l'Agence Nationale de la Cybersécurité (ANCy) mène ses actions au quotidien. En 2025, il s'agissait toujours de prévenir les menaces cyber, coordonner les acteurs et accompagner les institutions, les entreprises et les citoyens afin que le numérique reste un outil de progrès et non une source de vulnérabilité. Au-delà de ces aspects, l'ANCy s'est attachée

également à renforcer les compétences nationales et à promouvoir une culture de cybersécurité accessible à tous.

Le présent Rapport d'activités 2025 retrace les principales actions conduites par l'ANCy au cours de l'année. Il met en lumière les efforts réalisés pour renforcer la gouvernance de la cybersécurité, prévenir et gérer les incidents, sensibiliser les différents publics, former les acteurs clés et développer des partenariats solides, au niveau national comme international. Il revient également sur les défis rencontrés et les enseignements tirés.

À travers ce rapport, l'ANCy souhaite partager le chemin parcouru en 2025 et réaffirmer son engagement aux côtés des pouvoirs publics et de l'ensemble des parties prenantes, pour construire ensemble un Togo numérique toujours plus sûr, plus résilient et au service du bien-être des populations.



The background image shows a man in a call center environment, wearing a headset and looking at a computer screen. The image is overlaid with a teal grid pattern. A large, semi-transparent circular graphic is centered on the page, containing the main title. At the bottom, there are several thin, curved white lines.

I. SYNTHÈSE EXÉCUTIVE

Rapport d'activités 2025



I. Synthèse exécutive

L'Agence Nationale de la Cybersécurité (ANCy), créée par la loi n°2018-026 modifiée, constitue l'autorité nationale de référence en matière de cybersécurité au Togo.

En 2025, ses actions se sont articulées autour de quatre axes stratégiques :

1. Gouvernance et conformité ;
2. Développement du capital humain ;
3. Promotion d'une culture nationale de cybersécurité ;
4. Coopération régionale et internationale.

Indicateurs clés 2025

Domaine	Résultats
Personnes sensibilisées	6 500+
Informaticiens formés	250
Certifiés internationaux	50+
Audits OSE restitués	2
MoU signés	5
Candidats CTF	350+



A woman with glasses and braids is shown in profile, looking at a computer screen. The background is a blurred office environment. A large teal circle is overlaid on the image, containing the section header. The bottom of the image features a dark blue background with white curved lines.

II. GOUVERNANCE ET CADRE INSTITUTIONNEL

Rapport d'activités 2025



II. Gouvernance et cadre institutionnel

II.1. L'Agence Nationale de la Cybersécurité (ANCy)

II.1.1. Fondement juridique

Dans un contexte marqué par une dépendance croissante aux technologies numériques, la cybercriminalité s'impose comme une préoccupation majeure pour les États, les organisations internationales et les entreprises. Conscientes de ces enjeux, les autorités togolaises ont progressivement mis en place un cadre juridique et réglementaire renforcé, adossé aux instruments internationaux, afin de faire face de manière efficace aux menaces cyber.

L'intervention de l'Agence nationale de la cybersécurité (ANCy) s'inscrit dans ce dispositif juridique national, élaboré en cohérence avec les engagements régionaux et internationaux du Togo. Ce cadre vise à assurer la sécurité des systèmes d'information, à protéger les citoyens et les organisations, et à encadrer les responsabilités des acteurs du numérique.

Il poursuit quatre objectifs essentiels : la protection des infrastructures critiques, la consolidation de la souveraineté numérique, le renforcement de la coopération internationale, ainsi que la garantie des droits fondamentaux des citoyens face aux risques inhérents au cyberspace.

Ce cadre juridique comprend notamment :

2.1.2.1. Les textes portant création, organisation et fonctionnement de l'ANCy

- La loi n°2018-026 du 07 décembre 2018 sur la cybersécurité et la lutte contre la cybercriminalité modifiée par la loi n°2022-009 du 24 juin 2022 ;
- Le décret n°2019-022/PR du 13 février 2019 portant attributions, organisation et fonctionnement de l'agence nationale de la cybersécurité.

2.1.2.2. Les textes relatifs à la cybersécurité, à la cybercriminalité et encadrant les services numériques, les infrastructures critiques et les prestataires de services de confiance

- Le décret n°2019-095/PR du 08 juillet 2019 relatif aux opérateurs de services essentiels, aux infrastructures essentielles et aux obligations y afférentes ;
- Le décret n°2022-090/PR du 25 août 2022 relatif à la qualification des prestataires de services de confiance de cybersécurité et des produits de sécurité et à l'agrément des centres d'évaluation ;
- L'arrêté n°2022-040/PMRT du 29 juin 2022 portant adoption des règles de cybersécurité en République Togolaise.

2.1.2.3. Les conventions et instruments internationaux ratifiés par le Togo

Il s'agit notamment de :

- La Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel adoptée à Malabo en Guinée Équatoriale le 27 juin 2014 ; et
- La Directive C/DIR/1/08/11 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la CEDEAO.

Dans ce cadre réglementaire, l'ANCy contribue à la mise en œuvre effective des textes, à leur vulgarisation auprès des parties prenantes et, le cas échéant, à leur évolution, afin de tenir compte des mutations technologiques et des nouveaux risques. Cette action normative participe à la construction d'un environnement numérique sécurisé, fiable et respectueux des droits des citoyens.

2.1.3. Attributions et missions

L'Agence Nationale de la Cybersécurité est créée par la loi n° 2018-026 du 7 décembre 2018 modifiée par la loi n° 2022-009 du 24 juin 2022 sur la cybersécurité et la lutte contre la cybercriminalité, et est régie par le décret n° 2019-026/PR du 13 février 2019, qui définit son organisation, ses attributions et son fonctionnement. Elle a pour mission principale de garantir la sécurité et la confiance dans l'espace numérique togolais. À ce titre, elle agit comme un acteur central de prévention, de coordination et d'accompagnement des différentes parties prenantes face aux menaces cyber.

De manière générale, l'ANCy est chargée de :

- Coordonner l'action gouvernementale en matière de sécurité et de défense des systèmes d'information ;
- Répondre aux crises affectant ou menaçant la sécurité informatique des infrastructures essentielles au Togo ;
- Fixer les règles de cybersécurité et veiller à leur application par les divers acteurs ;
- Certifier les dispositifs matériels ou logiciels de cybersécurité en République togolaise ;
- Contrôler le bon fonctionnement du CERT (Computer Emergency Response Team) et du SOC (Security Operation Center) national opérés par CDA ;
- Désigner et auditer les Opérateurs de Services Essentiels (OSE) ;
- Délivrer des agréments aux centres d'évaluation ;
- Qualifier les prestataires de service de confiance en cybersécurité et les produits de sécurité ;

- Participer à la lutte contre la cybercriminalité ;
- Former et sensibiliser le public en cybersécurité.

À travers ces missions, l'ANCy œuvre à faire de la cybersécurité un levier de confiance, de souveraineté et de développement au service des citoyens, de l'État et de l'économie nationale.

2.1.4. Organisation et gouvernance

Pour assurer efficacement ses missions, l'ANCy s'appuie sur une organisation structurée et adaptée à la diversité de ses responsabilités. Ainsi, elle est placée sous l'autorité d'un Comité Stratégique et fonctionne selon des principes de coordination, de transversalité et de complémentarité des compétences.

L'ANCy est dirigée par un Directeur Général, assisté d'unités techniques, administratives et opérationnelles, notamment :

- Le Direction de la Réglementation et du Contrôle de Conformité ;
- La Direction Administrative et Financière ;
- La Direction de la Formation et du Renforcement des Capacités ;

À ces trois directions fondamentales, s'ajoutent les services suivants :

- La Comptabilité Publique ;
- La Communication et Relations Publiques ;
- Le Secrétariat Administratif

Le fonctionnement de l'Agence repose sur des procédures internes claires, une collaboration étroite avec les autres institutions de l'État, ainsi qu'un dialogue constant avec les acteurs du secteur privé, de la société civile, les partenaires techniques et les citoyens. Cette approche favorise une action cohérente, concertée et efficace face aux enjeux de cybersécurité.

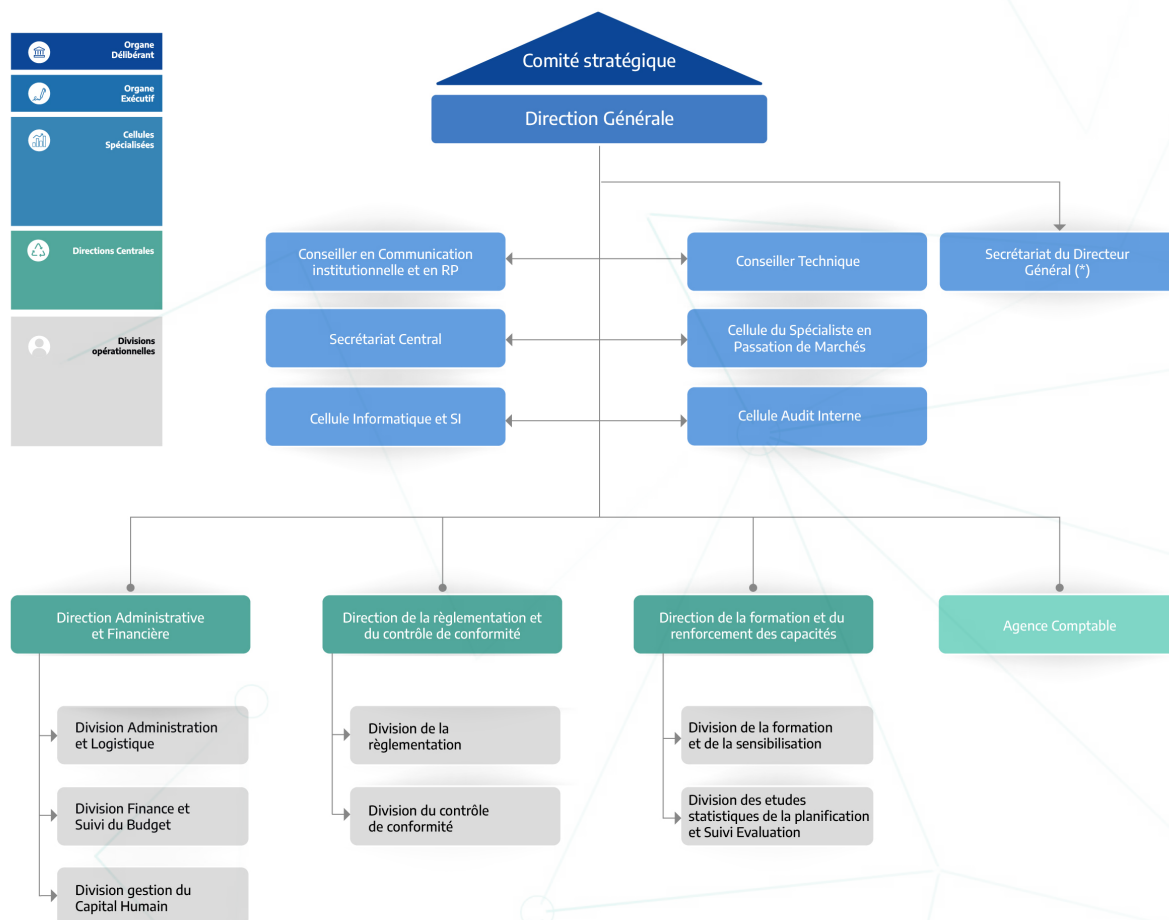


Figure 1 : Organigramme de l'ANCy

2.1.4.1 Le Comité Stratégique

Le comité stratégique est l'organe d'administration et de gouvernance de l'ANCy. Il élabore les dispositions relatives à la politique nationale de cybersécurité, procède aux arbitrages et validations et autorise tous les actes et opérations relatives aux missions de l'Agence.

Le comité stratégique est composé des membres suivants :

le Président du Conseil, **président** ;
 Le Ministre chargé de la sécurité, **membre** ;
 Le Ministre chargé de la défense, **membre** ;
 Le Ministre chargé de la justice, **membre** ;
 Le Ministre chargé de l'économie numérique, **membre** ;
 Deux (2) représentants de la présidence de la République, **membres**.



2.1.4.2 La Direction Générale



Photo 1 : Siège de l'ANCy

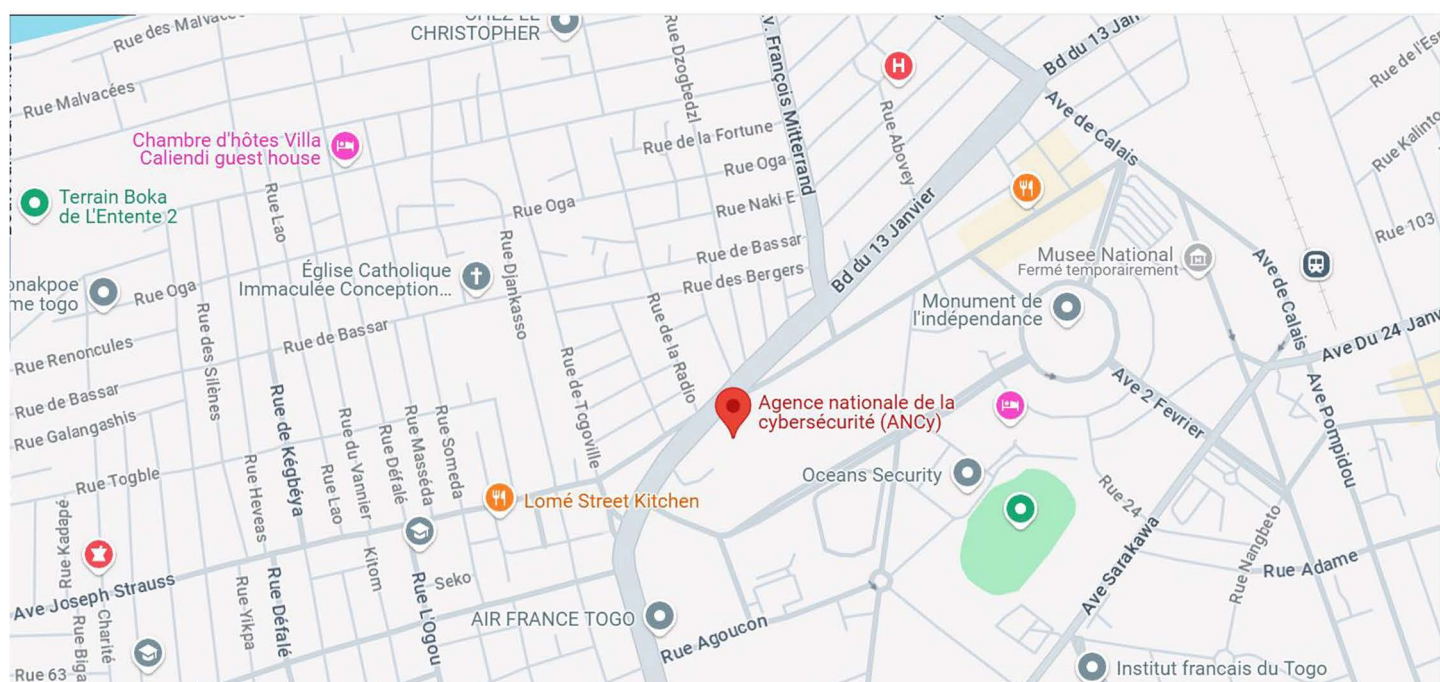


Figure 2 : Géolocalisation de l'ANCy

Le Directeur Général de l'ANCy, nommé par décret présidentiel, qui est chargé de toutes les missions qui ne relèvent pas, de manière spécifique, des attributions du comité stratégique, notamment la direction technique, administrative et financière de l'Agence.

À ce titre, il a pour attributions principales de :

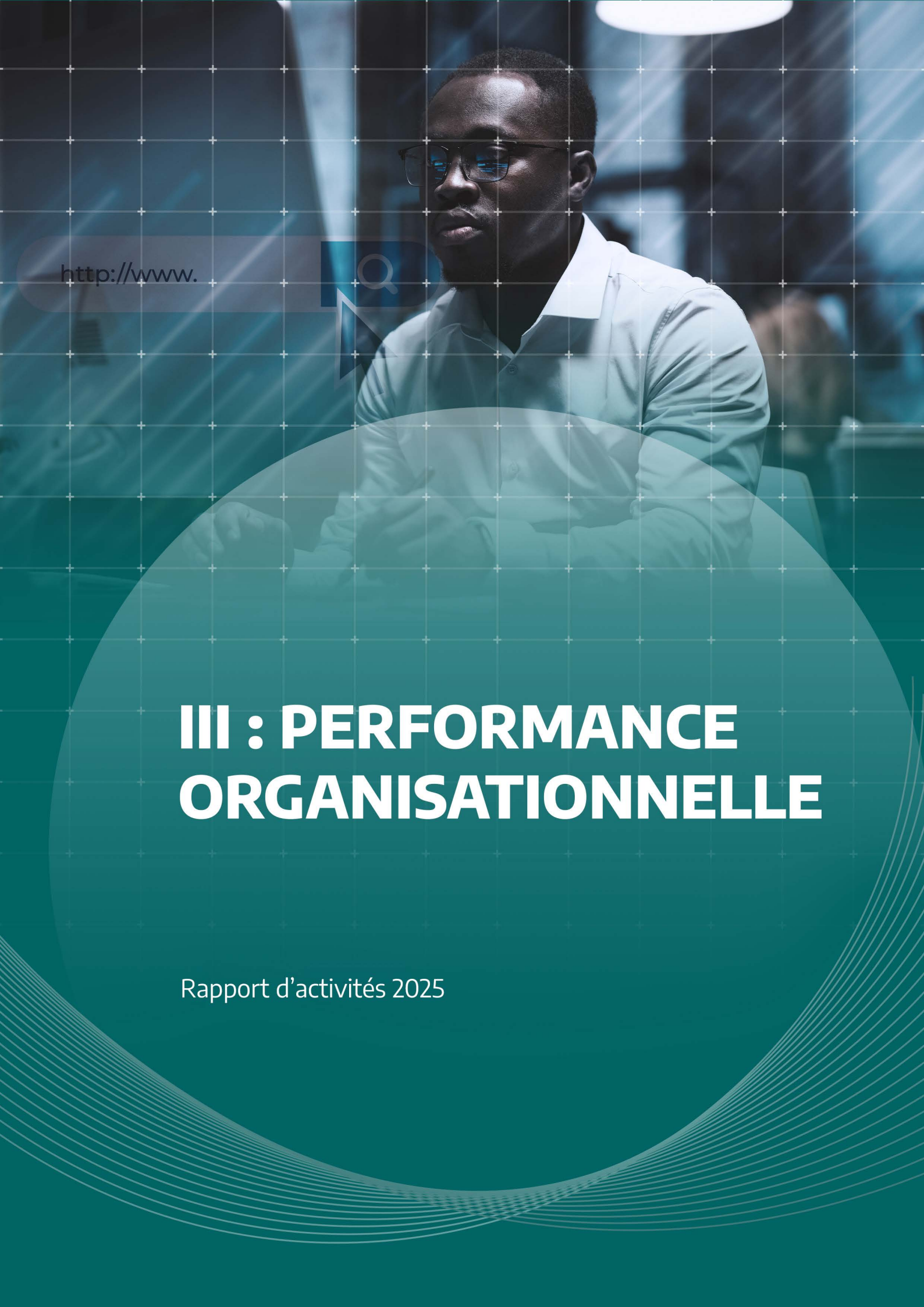
- Proposer des réformes juridiques et institutionnelles pour aligner la législation nationale sur les évolutions des menaces technologiques.
- Négocier et signer, selon les directives du Comité Stratégique, des accords et conventions nationaux et internationaux en lien avec les missions de l'ANCy.
- Établir le plan d'organisation et de fonctionnement des services de l'Agence.

La Direction Générale est subdivisée en trois (03) Directions :

- **La Direction Administrative et Financière** qui assure la gestion des ressources humaines, matérielles et financières de l'Agence ;
- **La Direction de la Réglementation et du Contrôle de Conformité** dont le rôle principal est de superviser l'élaboration des normes et le suivi de leur application ;
- **La Direction de la Formation et du Renforcement des Capacités** qui coordonne les actions de formation et sensibilisation afin de développer une culture nationale de cybersécurité.

Ce cadre de gouvernance repose sur un dispositif juridique solide, garantissant une coordination efficace entre les différents acteurs impliqués dans la cybersécurité au Togo.





<http://www.>

III : PERFORMANCE ORGANISATIONNELLE

Rapport d'activités 2025



III. Performance organisationnelle

Les actions menées dans le domaine de la gestion administrative en 2025 ont porté à la fois sur la gestion des ressources humaines, l'amélioration du cadre de travail et le renforcement des moyens logistiques et techniques. Ces initiatives ont contribué à soutenir efficacement la mise en œuvre des missions de l'Agence et à accompagner la montée en charge de ses activités.

3.1. Gestion et évolution des ressources humaines

En 2025, l'ANCy comptait un effectif stable de 15 agents, répartis entre les fonctions techniques, administratives et de pilotage. Aucune nouvelle arrivée n'a été enregistrée au cours de l'année. Toutefois, l'Agence a connu le départ du Directeur de la Formation et du Renforcement des Capacités en fin d'année, un mouvement qui a nécessité une réorganisation interne afin d'assurer la continuité des activités stratégiques liées au développement des compétences.

3.2. Renforcement interne des compétences

Dans une logique d'amélioration continue de la performance institutionnelle, l'ANCy a investi dans le renforcement des capacités de deux membres de son personnel, à travers des formations spécialisées. Ces actions ont permis de consolider les compétences techniques et opérationnelles des agents concernés, en adéquation avec l'évolution des missions de l'Agence et les exigences croissantes du contexte cyber.

3.3. Lancement de recrutements stratégiques

Afin de répondre aux besoins croissants en matière d'audit, de sécurisation et de gestion des infrastructures numériques, et notamment avec le lancement de la qualification des prestataires de confiance, l'ANCy a engagé en 2025 le processus de recrutement d'un auditeur des systèmes d'information et d'un administrateur systèmes et réseaux. Ces profils stratégiques visent à renforcer les capacités internes de l'Agence et à améliorer son efficacité dans l'accompagnement des administrations et des opérateurs de services essentiels.

3.4. Amélioration des capacités logistiques

3.4.1. Mise en place d'un cadre d'accueil des stagiaires

L'ANCy a mis en place un environnement de stage structuré, destiné à accueillir des étudiants souhaitant se perfectionner aux métiers de la cybersécurité. Cette initiative s'inscrit dans une démarche de contribution à la formation de la relève nationale, tout en favorisant le transfert de compétences et l'émergence de talents locaux dans le domaine de la sécurité numérique.

3.4.2. Extension du parking automobile de l'Agence

Dans le cadre de l'amélioration des conditions de travail et d'accueil, l'ANCy a procédé à l'extension de son parking automobile. Cette action a permis de mieux répondre aux besoins de mobilité du personnel et des visiteurs, tout en améliorant l'organisation logistique du site.

3.4.3. Installation de bureaux mobiles

Afin de faire face à l'augmentation des activités et offrir un cadre de travail adéquat aux nouvelles recrues qui vont arriver, l'ANCy a procédé à l'installation de bureaux mobiles. Cette solution flexible a permis d'accroître les capacités d'accueil de l'Agence sans engager d'énormes ressources.

3.4.4. Acquisition d'équipements mobiliers

L'Agence a également réalisé des acquisitions d'équipements mobiliers destinés à servir dans les bureaux. Cette action vise à améliorer l'ergonomie des espaces de travail, le confort du personnel et, par conséquent, la productivité et l'efficacité des équipes.



A man with short dark hair and a beard, wearing a white button-down shirt, is shown in profile, focused on his work. He is sitting at a desk, typing on a laptop. The background is a server room with rows of server racks and glowing blue lights. A large, semi-transparent blue circle is overlaid on the image, containing the title text. The overall tone is professional and technological.

IV. MISE EN ŒUVRE STRATÉGIQUE DE LA SNCY

Rapport d'activités 2025



IV. Mise en œuvre stratégique de la SNCy

4.1. Gouvernance et conformité

4.1.1. Supervision des Opérateurs de Services Essentiels (OSE)

En collaboration avec son partenaire opérationnel Cyber Defense Africa, l'ANCy a mené deux restitutions d'audits de conformité au profit de deux (2) Opérateurs de Services Essentiels (OSE). Ces séances de restitution ont permis de présenter aux responsables des deux structures les résultats des évaluations réalisées, notamment les vulnérabilités et risques spécifiques à leurs systèmes d'information, et de formuler des recommandations opérationnelles en vue du renforcement de leur posture de sécurité. Cette démarche s'inscrit dans sa mission de sécurisation des infrastructures critiques nationales, en accompagnant les opérateurs stratégiques dans l'amélioration continue de leur résilience face aux menaces cyber.

4.1.2. Lancement du processus de qualification des prestataires de services de confiance

Entre autres missions, l'ANCy est chargée de délivrer des agréments aux prestataires de services de confiance en cybersécurité, et de certifier les dispositifs matériels ou logiciels de cybersécurité en République Togolaise. À ce titre, l'Agence a élaboré et publié un ensemble de référentiels de qualification des prestataires de services de confiance en cybersécurité, et d'agrément des centres d'évaluation et des produits de sécurité.

Le 3 mars 2025, l'ANCy a lancé officiellement le processus de qualification des prestataires de services de confiance en cybersécurité. Il vise à renforcer la protection des services et infrastructures numériques critiques contre les cyberattaques et à garantir une collaboration avec des prestataires de confiance et à promouvoir l'utilisation de solutions de sécurité éprouvées. L'objectif est de mettre à la disposition de l'administration publique et des Opérateurs de Services Essentiels (OSE), et de toute autre personne, des services de confiance répondant à leurs besoins en matière de sécurité des systèmes d'information. La qualification se matérialise par la délivrance d'une reconnaissance officielle de l'ANCy au prestataire en fonction des services qu'il rend.

Le processus de qualification a ainsi démarré avec la mise en ligne de premiers services notamment :

- Demande d'agrément des centres d'évaluation ;
- Demande de qualification des prestataires de services de confiance en cybersécurité ;
- Demande de qualification des produits de sécurité.

Tous ces services sont accessibles à travers le <https://service-public.gouv.tg/> dans la catégorie « licences, agréments et certificats. »

3 services de l'Agence Nationale de la Cybersécurité (ANCy) désormais disponibles sur Service Public



service-public.gouv.tg

Comment faire la demande de qualification des prestataires de services de confiance en cybersecurité ?



service-public.gouv.tg

QU'EST-CE QUE C'EST ?

La qualification des prestataires de services de confiance en cybersécurité est une mission de l'ANCy. Elle a pour objectif de mettre à la disposition de l'administration, des Opérateurs de Services Essentiels (OSE), et de toutes autres personnes, des services répondant à leurs besoins en matière de sécurité des systèmes d'information.

PERSONNES SUSCEPTIBLES DE FAIRE LA DEMANDE

- Toute personne morale ou physique, prestataire de services en cybersécurité exerçant sur le territoire togolais.

service-public.gouv.tg

EXIGENCES SPÉCIFIQUES RELATIVES AUX PERSONNES MORALES

CONDITIONS ADMINISTRATIVES

- Être détenteur d'une carte d'immatriculation fiscale ;
- Avoir une organisation interne comprenant à minima une direction technique ou équivalent ;
- Ne pas être en état de faillite ;
- Le représentant légal ainsi que le personnel technique relevant de la personne morale doivent jouir de leurs droits civiques et ne pas avoir d'antécédents judiciaires ;
- Le représentant légal et le personnel relevant de la personne morale doivent être affiliés à la Caisse Nationale de Sécurité Sociale ;
- Disposer d'une adresse physique sur le territoire togolais.

service-public.gouv.tg

EXIGENCES SPÉCIFIQUES RELATIVES AUX PERSONNES MORALES

CONDITIONS TECHNIQUES

- Détenir un manuel de procédures organisationnelles et techniques permettant d'assurer la qualité de la prestation et de protéger les informations et données qui seront récupérées et traitées contre les risques de dommages, de modifications ou autres pouvant survenir ;
- Utiliser les outils et produits reconnus par l'ANCy pour mener les missions propres à chaque activité.

service-public.gouv.tg

EXIGENCES SPÉCIFIQUES RELATIVES AUX PERSONNES PHYSIQUES

CONDITIONS ADMINISTRATIVES

- Jouir de ses droits civiques ;
- Être détenteur d'une carte d'immatriculation fiscale ;
- Être titulaire au moins d'une licence en informatique ou en télécommunications ou d'un diplôme équivalent ;
- Être détenteur d'une certification dans le domaine de la sécurité de l'information ;
- Disposer d'une expérience professionnelle dans l'activité de cybersécurité objet de la demande de qualification (le nombre minimal d'années d'expérience requis est identifié dans le Référentiel d'exigences de la prestation objet de la demande de qualification) ;

service-public.gouv.tg

CONDITIONS ADMINISTRATIVES (SUITE)

- Être affilié à la Caisse Nationale de Sécurité Sociale ;
- Ne faire l'objet d'aucune condamnation judiciaire.

CONDITIONS TECHNIQUES

- Détenir un manuel de procédures organisationnelles et techniques permettant d'assurer la qualité de la prestation et de protéger les informations et données qui seront récupérées et traitées contre les risques de dommages, de modifications ou autres risques pouvant survenir ;
- Utiliser les outils et produits reconnus par l'ANCy pour mener les missions propres à chaque activité (REF : Liste des outils et produits).

 service-public.gouv.tg 

**Faites maintenant
votre demande via la
plateforme Service
Public**

service-public.gouv.tg/ancy-prestataires-cybersecurite 

 Besoin d'assistance ?
Contactez le **8988**

**Comment effectuer
la demande de
qualification des
produits de sécurité ?**



 service-public.gouv.tg 

QU'EST-CE QUE C'EST ?

La qualification d'un produit de sécurité est un processus permettant d'attester du niveau de robustesse du produit et du niveau de confiance dans un fournisseur de produit de cybersécurité.

La robustesse atteste de la capacité du produit de sécurité à résister à des attaques informatiques, tandis que la confiance atteste que le comportement des personnes physiques ou morales impliquées dans la fourniture dudit produit, est compatible avec les missions de fourniture d'un produit de sécurité à l'administration, aux Opérateurs de Services Essentiels (OSE), ou à tout autre utilisateur.

**PERSONNES SUSCEPTIBLES
DE FAIRE LA DEMANDE**

- Toute personne morale installée sur le territoire togolais, fournisseur ou éditeur de produits de sécurité.

 service-public.gouv.tg 

CONDITIONS

- Détenir une carte d'immatriculation fiscale ;
- Avoir une organisation interne comprenant à minima une direction technique ou équivalent ;
- Ne pas être en état de faillite ;
- Disposer d'une adresse physique sur le territoire togolais.
- Le représentant légal ainsi que le personnel technique relevant de la personne morale doivent jouir de leurs droits civiques et ne pas avoir d'antécédents judiciaires ;
- Le représentant légal et le personnel relevant de la personne morale doivent être affiliés à la caisse nationale de sécurité sociale ;

 service-public.gouv.tg 

**Faites maintenant
votre demande via la
plateforme Service
Public**

service-public.gouv.tg/ancy-produits-securite 

 Besoin d'assistance ?
Contactez le **8988**

4.2. Développement des compétences

4.2.1. Programme national de formations certifiantes en cybersécurité



Photo 2 : Photo des officiels à la cérémonie de lancement des formations

L'année 2025 a été marquée par le démarrage du programme national de formations certifiantes en cybersécurité au profit de 250 informaticiens issus des secteurs public et privé. Le développement des compétences techniques constitue un pilier fondamental de la Stratégie Nationale de Cybersécurité. Face à l'évolution rapide et à la sophistication croissante des menaces cyber, le renforcement du capital humain devient une condition indispensable à la souveraineté numérique et à la résilience des systèmes d'information du Togo. C'est à ce titre que l'ANCy a piloté un programme ambitieux de formation et de renforcement des capacités, visant à doter des informaticiens des deux sexes, issus des secteurs public et privé, des compétences nécessaires pour prévenir, détecter et gérer efficacement les risques cyber dans leurs milieux de travail.

Le programme a été lancé par le Ministère de l'Efficacité du Service Public et de la Transformation Numérique (MESPTN), par l'intermédiaire de l'Agence Nationale de la Cybersécurité (ANCy), en partenariat avec l'Agence Togo Digital (ATD). Il est mis en oeuvre avec l'appui du projet ProDigiT (Projet de Transformation digitale de l'économie togolaise) de la GIZ Togo cofinancé par l'Allemagne, l'Union européenne et le Luxembourg.

Ce programme vise à doter ces professionnelles et étudiants togolais des compétences nécessaires pour anticiper, détecter et gérer les menaces numériques.

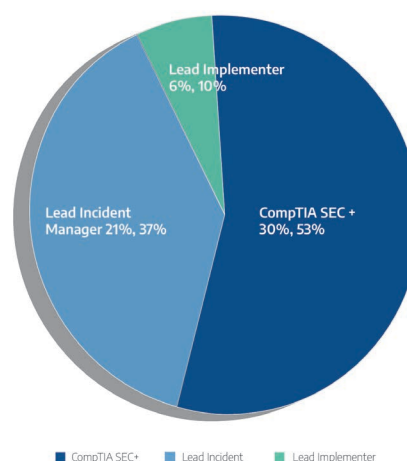


Photo 3 : Une cohorte de bénéficiaires des formations

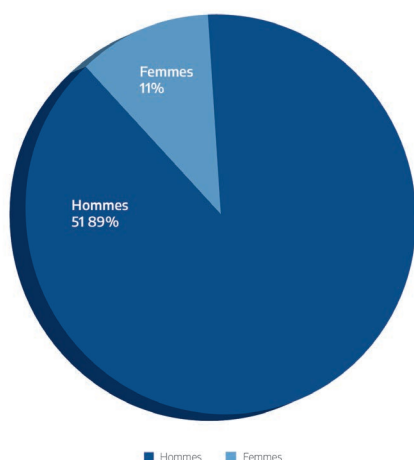
Trois certifications de référence sont proposées :

- **ISO 27001 Lead Implementer** pour acquérir les compétences requises pour concevoir, mettre en oeuvre et gérer un Système de Management de la Sécurité de l'Information (SMSI) conforme à la norme ISO 27001. Cette certification prépare notamment aux fonctions de Responsable de la Sécurité des Systèmes d'Information (RSSI) ;
- **ISO 27035 Lead Incident Manager** pour se former à la gestion des incidents de sécurité de l'information selon la norme ISO 27035, en couvrant l'identification, l'analyse, la réponse et l'amélioration continue des processus de gestion des incidents. Elle prépare les professionnels à l'exercice de la fonction de responsable de la gestion des incidents de sécurité de l'information, notamment dans l'élaboration et la mise en oeuvre des processus de réponse aux incidents, la coordination des équipes de gestion des incidents et l'amélioration continue du système de gestion des incidents ;

→ **CompTIA Security+** Certification de base en cybersécurité, elle valide les compétences essentielles en sécurisation des réseaux, gestion des menaces et protection des systèmes. Elle est reconnue pour sa couverture des concepts fondamentaux en cybersécurité et en gestion des risques. Elle constitue une préparation idéale pour exercer en tant qu'analyste en sécurité, administrateur systèmes et sécurité, consultant en cybersécurité ou spécialiste en gestion des risques liés à la cybersécurité.



Graphique 1 : Nombre de certifiés au 31 décembre 2025 par formation



À la fin de l'année 2025, 57 bénéficiaires avaient déjà passé avec succès leurs certifications internationales, traduisant l'efficacité et la pertinence de cette initiative pour le renforcement de l'expertise nationale.

Graphique 2 : Nombre de certifiés au 31 décembre 2025 par genre

4.2.2. Focus : Inclusion féminine

La promotion de l'inclusion et de l'égalité des chances dans le domaine de la cybersécurité s'est aussi traduite par l'organisation d'une session spéciale de recrutement exclusivement dédiée à la gent féminine pour des formations certifiantes. Près de 300 candidatures ont été enregistrées dans le cadre de l'appel à candidatures.



Photo 4 : Vue partielle de candidates au test de sélection

Grâce à ces certifications reconnues à l'international, les participantes pourront renforcer la sécurité des systèmes d'information de leurs administrations et entreprises et améliorer leur employabilité dans un secteur en pleine expansion. De plus les niveaux d'expertise seront harmonisés sur les standards internationaux en matière de cybersécurité. À terme, le Togo disposera d'un vivier de compétences développées en cybersécurité, prêtes à gérer tout type de situation.

4.2.3. Capture The Flag National

Organisée par l'ANCy, en partenariat avec Cyber Defense Africa (CDA), et avec le soutien de GVA CanalBox, la troisième édition du CTF National s'est tenue à Lomé du 28 au 29 novembre 2025 sous le regard d'un huissier de justice. Comme lors de l'édition précédente, 40 participants répartis en 10 équipes ont pris part à la finale après une phase de présélection en ligne organisée du 14 au 15 novembre 2025, qui a réuni plus de 350 candidats issus de toutes les régions du pays. Un record de participation qui témoigne de l'intérêt croissant pour la cybersécurité au Togo.



Photo 5 : Une équipe participante

Pour cette édition, le niveau de difficulté des épreuves a été sensiblement rehaussé afin de refléter les menaces cyber contemporaines. Malgré cette montée en exigence, les compétiteurs ont su résoudre les défis avec rapidité et efficacité, démontrant l'excellence de la nouvelle génération de spécialistes en cybersécurité.



Photo 6 : Les lauréats posant avec le DG de l'ANCy

Au terme d'une bataille technique particulièrement serrée de 24 heures non-stop mêlant précision technique et créativité, l'équipe 1NTRUD3R5 s'est hissée à la première place avec un total remarquable de 13 921 points, remportant une récompense de 2 000 000 FCFA. Elle est suivie de FireTeam, qui décroche la deuxième place avec 11 514 points et reçoit une enveloppe de 1 200 000 FCFA. En troisième position, APT17 complète le podium avec 7 077 points, empochant 800 000 FCFA. L'édition 2025 a également mis à l'honneur la participation féminine. Une distinction spéciale de 100 000 FCFA a été décernée à mademoiselle Trinity-Wonder BODJONA, seule participante féminine de cette finale.



Place	Équipe	Score
1	1NTRUD3R5	13853
2	FireTeam	10546
3	APT17	7077
4	Z3R07RUST	5250
5	nR4te	5122
6	EOA !!!	4445
7	Th3_d4rk_s1d3	3370
8	SPECTRA_SECTION-X	2298
9	DarkPayload	2098
10	L3g3nd5_of_Th3_Sh3ll	1749

Photo 7 : Le classement des 10 équipes participantes avec les scores

Au-delà des récompenses financières, les membres des trois équipes gagnantes, ainsi que la lauréate féminine, ont bénéficié d'une formation certifiante CompTIA Security+, renforçant leur expertise et consolidant leurs perspectives professionnelles.



Photo 8 : Les superviseurs en pleine injection des challenges

4.3. Promotion d'une culture nationale de cybersécurité

La cybersécurité est avant tout une affaire de comportements responsables et de vigilance collective. Consciente que l'humain est à la fois un maillon vulnérable et un vecteur puissant de résilience, l'Agence Nationale de la Cybersécurité (ANCy) a placé la sensibilisation et l'éducation du public au coeur de ses actions en 2025. Ces activités ont visé à renforcer les connaissances, les attitudes et les réflexes sécuritaires à travers des campagnes ciblées, des ateliers, des formations ou des rencontres thématiques avec des publics diversifiés.

4.3.1. Promotion de la culture de cybersécurité dans les enseignements primaire, secondaire et supérieur

Dans le cadre de la mise en oeuvre du plan d'action de la Stratégie nationale de cybersécurité (SNCy), l'Agence Nationale de la Cybersécurité (ANCy), en partenariat avec le Ministère de l'Éducation nationale, a engagé l'élaboration d'un programme national de formation en cybersécurité destiné aux enseignements primaire et secondaire. À cet effet, un Comité technique a été mis en place pour piloter le processus d'élaboration des manuels pédagogiques et des guides de l'enseignant, à travers des ateliers de travail collaboratifs réunissant les experts sectoriels et les acteurs du système éducatif.

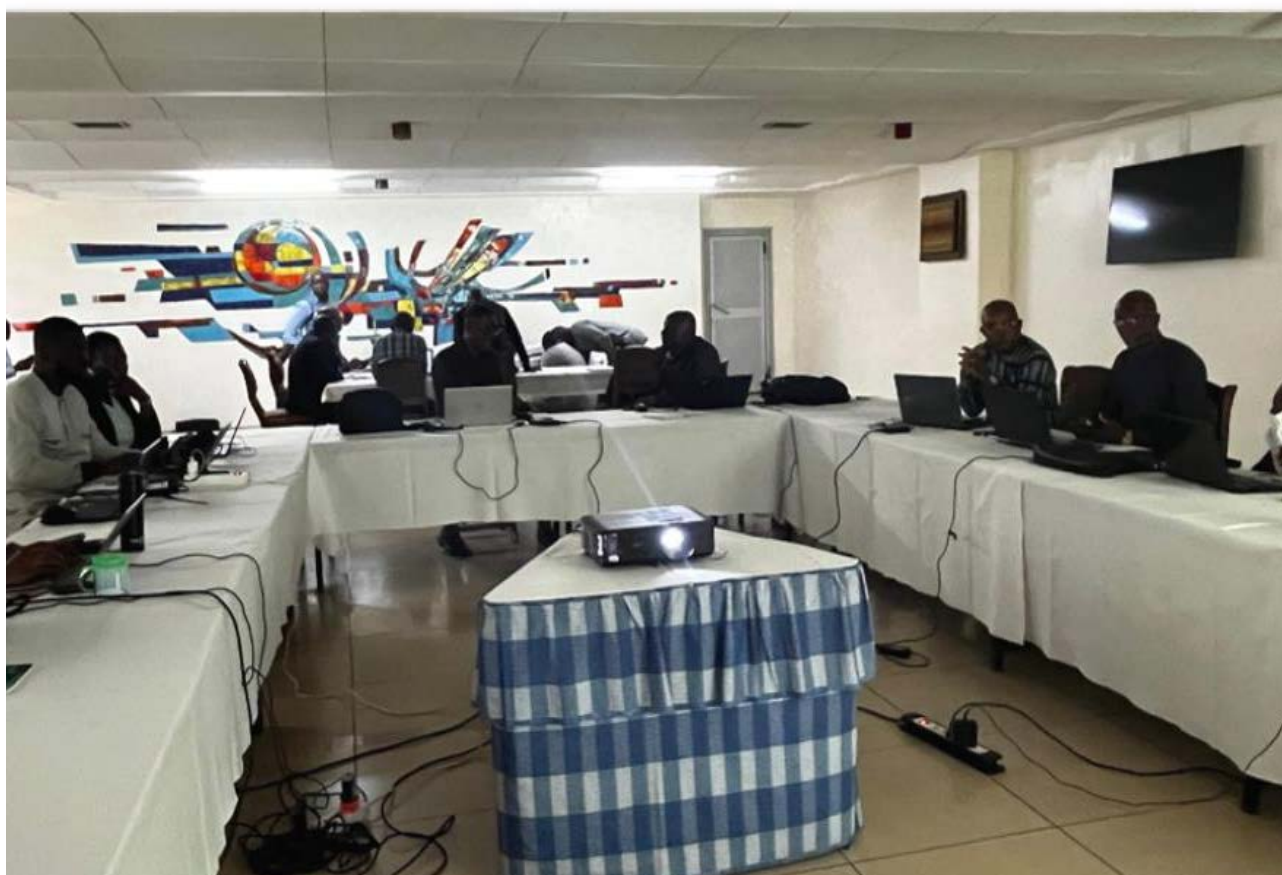


Photo 9 : Des membres du comité technique de l'enseignement supérieur en séance de travail

Ce programme permettra d'intégrer la cybersécurité dans les programmes scolaires et de former les élèves et étudiants à la cybersécurité, tout en développant les compétences techniques nationales dès le plus jeune âge, conformément au pilier 1 de la stratégie nationale de cybersécurité : « Promotion d'une culture de la cybersécurité et développement des compétences techniques nationales ».

En ce qui concerne l'enseignement supérieur, le comité technique est mis en place et commencera ses activités.

Résultats attendus

La mise en oeuvre des manuels de formation et des guides de l'enseignant en cybersécurité au primaire et au secondaire devrait permettre :

1. L'acquisition, par les élèves, de connaissances et de réflexes essentiels pour un usage responsable et sécurisé du numérique ;
2. La réduction des comportements à risque en ligne, notamment en matière de cyberharcèlement et de protection des données personnelles ;
3. L'harmonisation des enseignements de la cybersécurité sur l'ensemble du territoire national ;
4. Le renforcement des capacités pédagogiques des enseignants grâce à des outils structurés et adaptés ;
5. La contribution à l'émergence d'une culture nationale de cybersécurité durable, au service de la protection des jeunes et de la résilience numérique du pays.

4.3.2. Tournée nationale de sensibilisation

Du 3 au 14 mars 2025, une tournée nationale de sensibilisation a été conduite dans les régions des Savanes, de la Kara et de la Centrale, touchant plus de 500 acteurs locaux clés (autorités déconcentrées et décentralisées, opérateurs économiques, organisations de la société civile, citoyens) pour renforcer la culture numérique responsable.



Photo 10 : Vue partielle de l'assistance à Guérin-Kouka (Dankpen)

L'ANCy et son partenaire Cyber Defense Africa ont parcouru cinq (05) préfectures stratégiques (Tandjouaré, Kéran, Doufelgou, Dankpen et Mô) pour sensibiliser les acteurs locaux aux enjeux de la cybersécurité.



Photo 11 : Le préfet de Doufelgou, lors de la sensibilisation à Niamtougou

La tournée a ciblé les autorités déconcentrées et décentralisées, les opérateurs économiques, les organisations de la société civile, les ONG et les associations locales. L'objectif était de renforcer une culture numérique responsable pour mieux protéger les citoyens, les entreprises et les institutions contre les cybermenaces.



Photo 12 : Photo de famille des participants à Tandjoaré

Chaque rencontre a permis aux participants d'identifier les risques spécifiques liés à leurs activités et d'adopter des mesures de protection adaptées. Les thématiques abordées ont couvert plusieurs aspects tels que la protection des données personnelles, la sécurisation des systèmes d'information, la gestion des mots de passe, la prévention des fraudes en ligne et la reconnaissance des cyberattaques les plus courantes.



Photo 13 : M. GERALDO Malik, Directeur de la Formation, présentant l'ANCy aux populations de Djarkpanga (Mô)

Les astuces des attaquants pour infecter les téléphones et pour voler les mots de passe ont été dévoilées. Les arnaques d'ingénierie sociale contre les utilisateurs de Mixx By Yas et Flooz ont été également élucidées. À travers des démonstrations concrètes, les participants ont pu mesurer l'impact réel des cybermenaces et l'importance de la vigilance numérique au quotidien.

4.3.3. Sensibilisation des agents de l'Établissement Public et Autonome pour l'exploitation des Marchés (EPAM)

Dans le cadre du renforcement de la culture de cybersécurité au sein des administrations publiques, l'Agence Nationale de la Cybersécurité (ANCy) a animé avec son partenaire Cyber Defense Africa (CDA), une session de sensibilisation à l'intention du personnel de l'Établissement Public et Autonome pour l'exploitation des marchés (EPAM).



Photo 14 : Ouverture des travaux par la Directrice Générale de l'EPAM, Commissaire Somialo KADJA (au centre)

Cette activité qui s'est tenue les 18 et 19 mars à Lomé visait à renforcer la compréhension des enjeux liés à la sécurité des systèmes d'information, en mettant un accent particulier sur les risques courants auxquels sont exposés les agents publics, notamment le phishing, l'ingénierie sociale, la gestion sécurisée des mots de passe et la protection des données sensibles.

À travers des échanges interactifs et des exemples concrets issus du contexte professionnel, l'ANCy a contribué à améliorer les bonnes pratiques numériques du personnel de l'EPAM, renforçant ainsi la résilience de l'institution face aux menaces cyber et son rôle dans la sécurisation des processus liés à la commande publique.



Photo 15 : Vue partielle des participants

Une attention particulière a été portée à l'utilisation d'un langage simple et adapté, afin de garantir une bonne compréhension des messages et une appropriation effective des bonnes pratiques.

La présence des plus hautes autorités de l'institution souligne l'importance accordée par l'EPAM à la protection des usagers et de son personnel face aux risques numériques.

4.3.4. Sensibilisation lors de la célébration de la Journée internationale des droits des femmes à l'Université de Lomé



Photo 16 : Mlle Fabiola KOUDAM (à l'extrême droite), présentant sa communication de sensibilisation

À l'occasion de la célébration en différé de la Journée internationale des droits des femmes, organisée le 19 mars par l'association Coeurs Solidaires à l'Université de Lomé, l'ANCy a pris part aux activités à travers une communication consacrée aux jeunes et au harcèlement numérique. Dans un contexte où les réseaux sociaux occupent une place centrale dans le quotidien des étudiants, cette intervention a permis d'ouvrir un espace d'échange autour des réalités du cyberharcèlement, de ses différentes formes et de ses conséquences parfois profondes sur les victimes.

CONFÉRENCE-DÉBAT

Thème
**Harcèlement sexuel en milieu universitaire :
Briser le silence, agir pour l'égalité**

Institut Confucius
l'Université de Lomé **19 Mars 2025** **9h00 à 13h00**

**Stop au Harcèlement Sexuel en milieu
universitaire : Parlons-en et Agissons !**

Coeursolidairetogo.org
coeursolidaire.tg@gmail.com
+228 92 20 86 77

Photo 10 : Vue partielle de l'assistance à Guérin-Kouka (Dankpen)

L'ANCy a partagé des conseils pratiques pour adopter des comportements responsables en ligne, savoir réagir face aux situations de harcèlement et utiliser les mécanismes de signalement et de protection existants. Cette rencontre a également été l'occasion de rappeler l'importance de la solidarité et de la vigilance collective pour construire un environnement numérique plus sain, respectueux et protecteur, en particulier pour les jeunes et les femmes.

4.3.5. Sensibilisation du personnel de l'Agence Nationale de l'Aviation Civile (ANAC)

Dans le cadre de sa mission de sensibilisation des administrations stratégiques, l'ANCy a conduit le 29 août au siège de l'ANAC, une activité de sensibilisation avec CDA au profit du personnel de ladite agence. Cette initiative visait à renforcer la vigilance des agents face aux menaces cyber susceptibles d'affecter des systèmes critiques liés à la sûreté, à la sécurité et à la continuité des services aéronautiques.



Photo 17 : Vue partielle du personnel sensibilisé

Les échanges ont porté notamment sur les risques de cyberattaques ciblées, la protection des informations sensibles, les bonnes pratiques en matière d'hygiène numérique ainsi que la prévention des incidents liés à l'ingénierie sociale. À travers cette action, l'ANCy a contribué à consolider la culture de cybersécurité au sein de l'ANAC, en cohérence avec les exigences de sécurité propres au secteur de l'aviation civile et les priorités nationales en matière de résilience numérique.

4.3.6. Opération rentrée scolaire sûre 2025-2026

En 2025, l'ANCy a mené des campagnes de sensibilisation d'envergure nationale, conçues pour toucher différents segments de la population. Parmi celles-ci, l'opération « Rentrée scolaire sûre 2025-2026 » a mobilisé les énergies autour de la sécurité numérique en milieu éducatif.



Photo 18 : Sensibilisation sur la TVT dans l'émission L'bala

Dans ce cadre, l'ANCy a élaboré et diffusé des supports pédagogiques (visuels, messages, recommandations) pour encourager des usages responsables, prévenir le cyberharcèlement et outiller parents, élèves et enseignants face aux risques numériques. Des émissions radio et télé ont également été animées par les experts de l'ANCy.



Image 1 : Un visuel de sensibilisation diffusé sur les réseaux sociaux

4.3.7. Sensibilisation du personnel administratif de TotalEnergies Togo

Dans le cadre de ses actions de sensibilisation à destination des acteurs économiques stratégiques, l'ANCy et son partenaire CDA ont animé le 23 octobre une session de sensibilisation au profit du personnel de TotalEnergies Togo. Cette activité qui s'est déroulée au siège de TotalEnergies à Lomé avait pour objectif de renforcer la compréhension des enjeux de cybersécurité au sein d'un secteur critique, fortement dépendant des systèmes d'information et des technologies industrielles.



Photo 19 : M. Malik GERALDO, s'adressant personnel sensibilisé

Les échanges ont porté sur les principales menaces cyber pesant sur les entreprises du secteur de l'énergie, notamment le phishing, les ransomwares, les risques liés aux environnements industriels (OT), ainsi que sur l'importance de la protection des données, de la gestion des accès et de l'adoption de bonnes pratiques numériques au quotidien.



Photo 20 : M. Arnel BEHANZIN, Responsable Commercial de CDA entretenant les participants

À travers cette initiative, l'ANCy a contribué à renforcer la culture de cybersécurité du personnel de TotalEnergies Togo, en appui à la continuité des activités, à la sécurité des opérations et à la résilience globale du tissu économique national.

4.3.8. Sensibilisation des jeunes sur la protection des données personnelles

La sensibilisation des jeunes constitue une priorité majeure, car ils sont à la fois de grands utilisateurs du numérique et particulièrement exposés aux risques. En collaboration avec l'Instance de Protection des Données à Caractère Personnel (IPDCP), le 31 octobre 2025, l'ANCy a animé une sensibilisation sur la protection des données personnelles qui a touché près de 3 000 jeunes étudiants, leur fournissant des outils et conseils concrets pour adopter de bons réflexes numériques.



Photo 21 : Le Président de l'IPDCP, Col. Bédiani BELEI, lors de son intervention

Cette grande rencontre qui s'est tenue au palais des congrès de Lomé a été structurée autour de deux sujets principaux. D'abord la protection des informations personnelles sur téléphone et Internet qui a permis de présenter les pratiques essentielles de sécurisation des données personnelles dans les usages numériques quotidiens. Ensuite, l'évitement des pièges des réseaux sociaux pour protéger sa vie privée a porté sur l'identification des risques liés aux réseaux sociaux, les modes opératoires courants de la cybercriminalité et les mesures de prévention à adopter pour préserver la vie privée en ligne.



Photo 22 : L'assistance lors de la sensibilisation

Cette approche de sensibilisation préventive constitue l'un des leviers les plus efficaces pour réduire les risques liés à la cybercriminalité. En dotant les jeunes des connaissances et des compétences nécessaires pour comprendre et maîtriser leur environnement numérique, les pouvoirs publics contribuent à la formation d'une génération d'utilisateurs responsables, conscients des enjeux de sécurité et de la valeur stratégique de leurs données personnelles.

4.3.9. Rencontre annuelle de l'ANCy avec les médias nationaux

Les médias jouent un rôle central comme multiplicateurs de messages de prévention et comme partenaires stratégiques dans la lutte contre la cybercriminalité. À cet effet, le 16 décembre 2025, l'ANCy a tenu sa session annuelle de sensibilisation dédiée aux médias nationaux, rassemblant plus d'une centaine de journalistes en mode écrit, audiovisuel et numérique à Lomé. L'objectif principal de cette session était de renforcer les connaissances et les compétences des professionnels des médias sur les enjeux et les risques liés à la cybersécurité, de mieux outiller les rédactions pour la protection de leurs systèmes d'information et de consolider la coopération entre l'ANCy et les médias afin d'assurer une communication efficace et coordonnée en cas d'incident cyber majeur.



Photo 23 : Photo de famille avec le DG de l'ANCy et les professionnels des médias

L'ANCy a mis un accent particulier sur l'usage des médias pour sensibiliser, car les interventions médiatiques régulières augmentent la compréhension des enjeux de la cybersécurité par le public tout en renforçant considérablement sa visibilité et sa crédibilité en tant qu'acteur clé de la cybersécurité. Elles permettent de sensibiliser efficacement un large public aux bonnes pratiques numériques, contribuant ainsi à prévenir les cyber incidents et à promouvoir un usage sûr des technologies. De plus, la diversité des canaux (télévision, radio, presse écrite, numérique), est le meilleur gage pour toucher le maximum différents groupes sociaux et professionnels, dans leur diversité.

4.3.10. Sensibilisation des étudiants de l'ENA

Le 17 décembre 2025, l'ANCy a animé une séance de sensibilisation au profit des étudiants de l'École nationale d'administration (ENA). Cette activité, qui a mobilisé plus de 150 étudiants, visait à renforcer leur compréhension des enjeux de la cybersécurité, des menaces numériques courantes et les bonnes pratiques à adopter dans l'usage des outils numériques, en particulier dans le cadre de leurs futures responsabilités au sein de l'administration publique. Cette action s'inscrit dans la mission de l'ANCy de promotion de la culture de la cybersécurité et de prévention des risques numériques au sein des institutions publiques.



Photo 24 : Les étudiants attentifs à la sensibilisation

4.3.11. Sensibilisation au Fonds National de la Finance Inclusive (FNFI)

Pendant plus de 3h de temps, l'ANCy et CDA ont sensibilisé le personnel et une partie du comité exécutif (COMEX) aux enjeux de cybersécurité en tenant compte du domaine d'activité : la finance.



Photo 25 : Vue partielle des participants à la sensibilisation

4.3.12. Autres sensibilisations

Toujours dans la conduite de sa mission d'éducation du public, l'ANCy, a également sensibilisé le personnel du Fonds National de Finance Inclusive (FNFI), les étudiants de l'Institut Africain d'Informatique (IAI), de même que bien d'autres structures.

4.4. Activités de renforcement des capacités des équipes

4.4.1. Renforcement de la posture de sécurité des administrations publiques et structures critiques

En complément des formations certifiantes, l'ANCy a mené des actions ciblées de renforcement des capacités des équipes nationales, notamment au sein des administrations publiques, des structures critiques et des entités techniques impliquées dans la gestion des systèmes d'information.

Ces actions ont porté sur :

- L'amélioration des compétences opérationnelles en matière de prévention et de gestion des incidents ;
- Le partage de bonnes pratiques et des retours d'expérience ;
- L'appropriation des outils et méthodologies de cybersécurité.

Cette approche a permis de consolider les capacités internes et de favoriser une meilleure coordination entre les différents acteurs techniques du pays.

4.4.2. Participation aux cafés de la cybersécurité

Afin de promouvoir une dynamique d'échange et d'apprentissage continu, Cyber Defense Africa (CDA) organise chaque fin de trimestre, conjointement avec l'ANCy, des « Cafés de la cybersécurité ». Il s'agit d'espaces de discussion ouverts et interactifs réunissant professionnels, experts, étudiants et acteurs du numérique.



Photo 26 : Des agents de l'ANCy aux côtés du DG de l'ANCy (au centre, en veste sans cravate) et du DG de CDA (à l'extrême droite) lors d'un café de la cybersécurité.

Au cours de l'année 2025, ces rencontres ont permis :

- De débattre des enjeux actuels et émergents de la cybersécurité ;
- De vulgariser des thématiques techniques auprès d'un public élargi de professionnels et de décideurs ;
- De renforcer le réseau national des acteurs de la cybersécurité.



Photo 27 : Le Cdt Gbota GWALIBA, DG de l'ANCy prenant la parole lors d'un café de la cybersécurité

Les Cafés de la cybersécurité ont contribué à créer une communauté d'intérêts autour des questions de sécurité numérique et à encourager le partage des connaissances et des expériences. Les thèmes abordés cette année ont concerné la construction d'un budget de cybersécurité comme stratégie gagnante, la gouvernance et la gestion des identités et des accès, l'intelligence humaine face aux nouvelles menaces, etc.

4.5. Coopération internationale et positionnement régional

4.5.1. Signature de plusieurs mémorandums d'entente

En 2025, le Togo a signé des mémorandums d'entente avec plusieurs pays, notamment la Pologne, le Mozambique, le Ghana, la Gambie, le Nigéria et le Cap Vert. L'objectif de ces ententes est de renforcer les capacités opérationnelles des pays dans la protection des infrastructures critiques, la lutte contre la cybercriminalité, le partage d'expertise et d'informations et la mise en place de mécanismes conjoints de réponse aux incidents.



Photo 28 : Échange de paraphes après signature de MoU entre le Togo et le Mozambique

Alors que les deux nations font face à un paysage de menaces en évolution rapide, elles partagent une ambition commune : bâtir des capacités de cyberdéfense solides, agiles et interconnectées pour protéger les citoyens, les institutions et les infrastructures critiques. L'apport particulier de ce MoU est que les Computer Security Incident Response Teams (CSIRTs) des deux pays travailleront ensemble sur :

- Le partage d'informations et de renseignements sur les menaces en temps réel ;
- Des programmes conjoints de renforcement des capacités ;
- Des réponses coordonnées aux incidents cyber ;
- Le transfert de connaissances techniques ;
- L'échange de bonnes pratiques en gouvernance cyber.

Pour le Togo, la signature de ces MoU consolide son positionnement comme acteur engagé dans la promotion d'un espace numérique africain sûr et résilient. In fine, il s'agit de bâtir un écosystème régional capable d'anticiper, de détecter et de contrer des menaces transfrontalières de plus en plus sophistiquées.

4.6. Lutte contre la cybercriminalité

Au cours de l'année 2025, le Laboratoire de Criminalistique Numérique (LCN) a enregistré plusieurs affaires de cybercriminalité touchant aussi bien des particuliers que des personnes morales établies au Togo. Les investigations menées mettent en évidence une diversification des modes opératoires des cybercriminels ainsi qu'une augmentation des impacts financiers et psychosociaux sur les victimes.

4.6.1. Typologie des cybercrimes recensés

Les principaux types de cybercriminalité enregistrés sur la période concernée sont : la cyber-escroquerie ; le cyberharcèlement ; la sextorsion ; le chantage numérique ; le piratage de comptes Mobile Money ; les faux ordres de virement.

4.6.2. Analyse des cas recensés

Les cas de cyber-escroquerie ont principalement porté sur des fraudes en ligne et des manipulations financières visant des particuliers. Les investigations révèlent une forte implication de réseaux transnationaux opérant depuis plusieurs pays de la sous-région.

En ce qui concerne le cyberharcèlement, la sextorsion et le chantage numérique, les victimes ont subi plusieurs formes de préjudices non financiers, notamment la perte de confiance ; le stress psychologique ; des désagréments personnels et professionnels ; des atteintes à la réputation ; des cas de vol d'identité. Ces affaires traduisent une montée des infractions numériques à caractère psychologique et réputationnel, particulièrement sur les réseaux sociaux et les plateformes de messagerie.

Sur le piratage de comptes Mobile Money, les attaques ont principalement ciblé des utilisateurs de

services financiers mobiles à travers des techniques d'ingénierie sociale, d'usurpation d'identité et de compromission de comptes. La difficulté d'identification des auteurs souligne le recours à des procédés d'anonymisation et à des infrastructures numériques complexes.

Quant aux faux ordres de virement, les investigations ont mis en évidence des techniques avancées de compromission de communications professionnelles et d'usurpation d'identité d'entreprises ou de responsables administratifs afin d'émettre de faux ordres de paiement.

4.6.3. Tendances observées

L'analyse globale des incidents enregistrés en 2025 fait ressortir :

- Une prédominance des infractions financières numériques ;
- Une hausse des attaques visant les services de Mobile Money ;
- Une recrudescence des cyberviolences et des atteintes à la réputation en ligne ;
- L'implication récurrente de réseaux criminels transnationaux ;
- Une sophistication progressive des techniques utilisées par les cybercriminels.

Le montant cumulé des préjudices financiers documentés s'élève à au moins cent soixante-trois (163) millions FCFA, sans compter les pertes encore en cours d'évaluation dans certaines procédures.

4.6.4. Actions futures

Au regard des tendances observées en matière de cybercriminalité durant l'année 2025, plusieurs actions prioritaires peuvent être envisagées afin de renforcer la prévention, la détection et la répression des infractions numériques au Togo. L'ANCy envisage donc de :

- Renforcer la sensibilisation des populations ;
- Mettre en place un dispositif national d'alerte et de veille ;
- Renforcer le cadre réglementaire et organisationnel ;
- Renforcer la coopération nationale et internationale ;
- Consolider les capacités techniques d'investigation ;
- Renforcer la sécurité des services financiers numériques ;
- Renforcer l'accompagnement des victimes.

Ces mesures permettront de renforcer la résilience numérique nationale, de réduire les pertes financières et de mieux protéger les citoyens ainsi que les organisations contre les menaces cyber.

4.7. Veille, prévention, et gestion des incidents

Les missions de veille, de prévention et de gestion des incidents sont déléguées à CDA, en tant que bras opérationnel de l'ANCy. Il s'agit principalement de :

- Opérer le CERT national (CERT.tg) 24h/24 et 7j/7 ;

- Opérer le SOC (System Operating Center) national 24h/24 et 7j/7 ;
- Sensibiliser les usagers des équipements, des services et installations informatiques ;
- Faire la prévention des intrusions, la sécurisation et la défense de l'ensemble des systèmes d'information ;
- Coordonner la riposte aux attaques informatiques ;
- Fournir un support technique pour le compte de l'ANCy.

CDA délivre également d'autres prestations nécessaires à la sécurisation des systèmes d'information des organismes :

- Conseil en cybersécurité (rédaction de politiques de sécurité des systèmes d'informations, réalisation de cartographies des infrastructures essentielles, autres...) ;
- Formations avancées en cybersécurité ;
- Intégration de solutions de cybersécurité ;
- Audits et tests d'intrusions.



4.7.1. Veille et alerte : les activités SOC

Cette mission est dévolue à l'équipe SOC. Elle fournit des services payants 24 heures sur 24 et 7 jours sur 7 aux opérateurs de services essentiels et à toutes organisations souhaitant bénéficier de services de protection proactive en cybersécurité. Elle se consacre à la sécurité des entreprises qu'elle protège et utilise le soutien et les services de l'équipe CERT lorsque cela est nécessaire. Les services délivrés par l'équipe SOC sont des prestations de type services managés dits « SOC as a Service » (ou SOCaaS) :

- Administration et maintenance de l'infrastructure SIEM (Security Information & Event Management) nationale et/ou sur le site de chaque organisme bénéficiant des services SOC ;
- Surveillance sur mesure des événements de sécurité 24 heures sur 24 et 7 jours sur 7 ;
- Détection et identification des menaces et des attaques ciblées ;
- Réponse aux menaces et mesures correctives (en collaboration au besoin avec l'équipe CERT) ;
- Assistance dans le processus de correction et de rétablissement du système d'information (en collaboration avec l'équipe CERT) ;
- Analyse ciblée des logiciels malveillants (en collaboration avec l'équipe CERT) ;
- Analyse et gestion des vulnérabilités inhérentes à l'organisme protégé ;
- Rapports périodiques ;

4.7.1.1. Chiffres clés de 2025

Sur l'année 2025, CDA a surveillé via son service SOC, le réseau de plusieurs infrastructures critiques au Togo. Les systèmes ont analysé des données provenant des équipements réseau, des systèmes et des applications surveillés. Ces données analysées ont évolué au fil des intégrations clients pendant toute l'année 2025.

Ces logs sont corrélés et analysés dans le but de rechercher des anomalies dues à une cyberattaque. Les analystes SOC de CDA ont ainsi traité 63 763 incidents de cybersécurité (ou anomalies) au cours de l'année 2025 contre 181 088 en 2024 soit une baisse de 35%.



Figure 3 - Incidents traités

4.7.1.2. Évolution des données au cours de l'année 2025

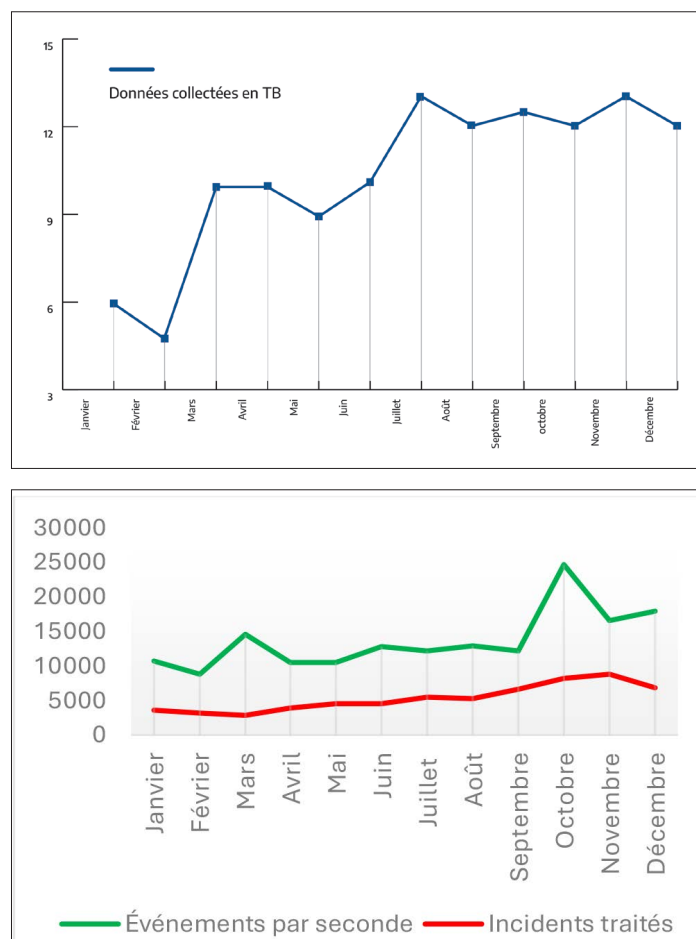


Figure 4 - Évolution des données collectées en 2025

Les Évènements Par Seconde (EPS) restent globalement stables au cours de l'année avec des fluctuations modérées tout au long de l'année 2025. Il y a une hausse au cours de la période de septembre à octobre avant une légère baisse sur les deux derniers mois de l'année (novembre et décembre).

Les incidents de cybersécurité sont le résultat des règles de corrélations définies dans l'outil SIEM par les équipes CDA. Dans le cadre de l'amélioration continue du Service SOC, CDA affine régulièrement (fine tune) non seulement les règles de corrélation mais aussi la sévérité des incidents. Ainsi, les incidents traités d'août à novembre 2025 présente des variations plus importantes. Le nombre d'incidents traités a augmenté de manière significative en octobre et a atteint un pic en novembre 2025 suite à l'ajout de nouveaux clients SOC.

Les données collectées au cours de l'année nous donnent des variations comprises entre 5.61 TB et 13.49 TB. Une hausse notable est observée en juillet et octobre, avec un pic en novembre. De légères baisses de données collectées ont été notées avec un creux en mai à environ 8.54 TB.

4.7.1.3. Évolution des données clés depuis le démarrage du SOC

4.7.1.3.1. Incidents traités

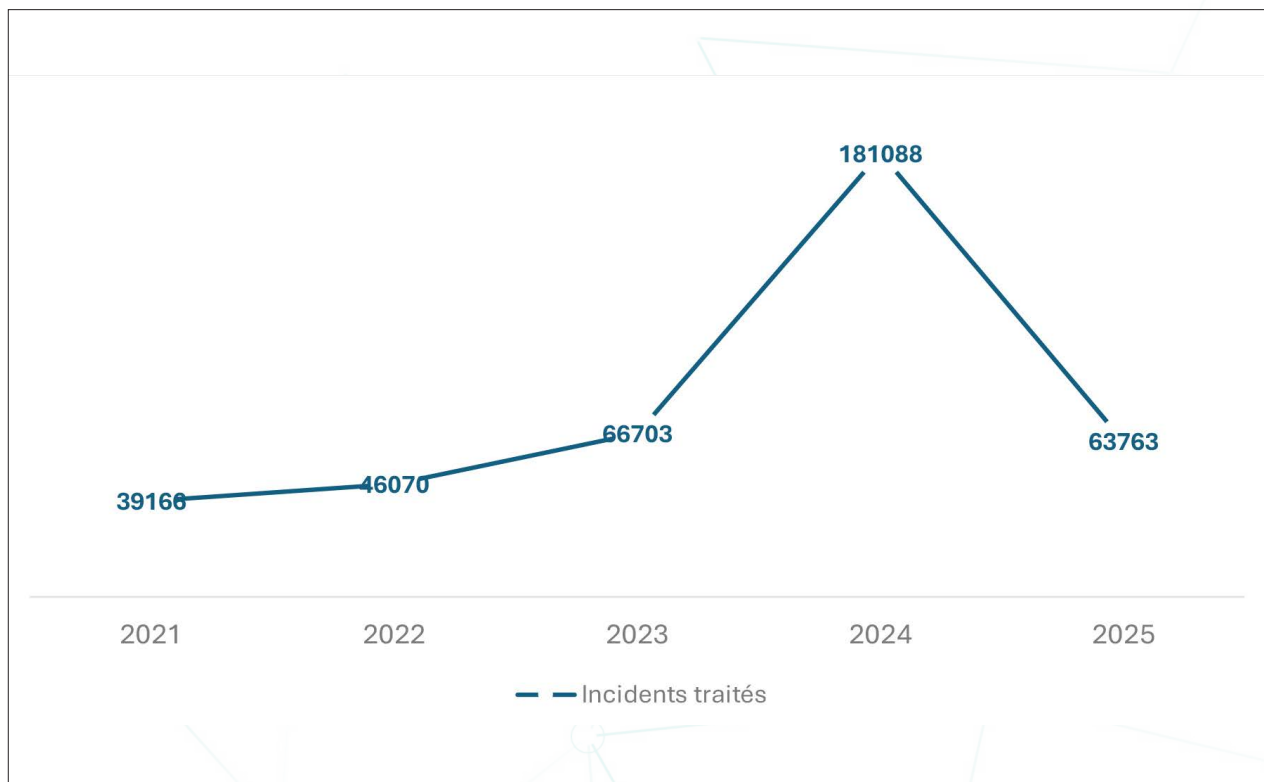


Figure 5 - Évolution des incidents traités depuis le démarrage du SOC

Le nombre d'incidents détectés a fortement diminué en 2025 suite à l'amélioration des règles de corrélations ayant contribué à éliminer les incidents faux-positifs.

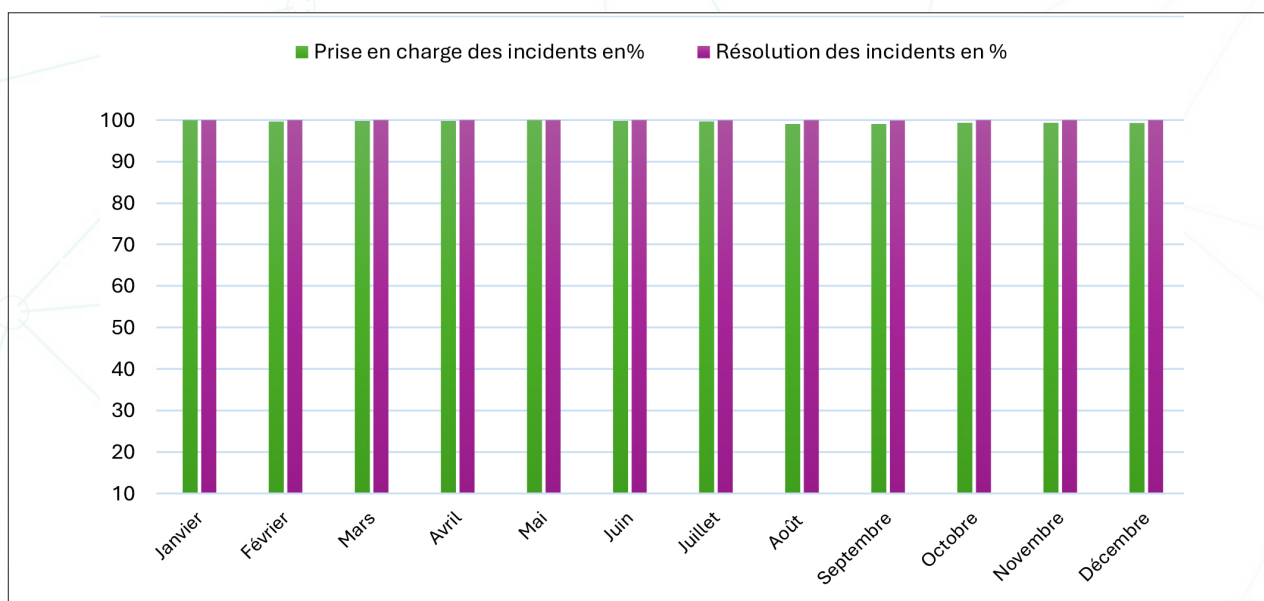


Figure 6 - Niveau des SLA en 2025

CDA est tenu au respect des SLA convenus avec l'ANCy dans le cadre du contrat de délégation de services, à savoir 30 minutes maximum pour la prise en compte d'un incident et 15 jours maximum pour la résolution. Le temps de résolution des incidents est indépendant et n'est pas totalement sous le contrôle de CDA.

Les temps de prise en charge des incidents par CDA en respect des SLAs sont compris entre 99,06 et 100%. La moyenne de respect des SLA sur toute l'année 2025 pour **la prise en charge des incidents est de 99.53% et de 99,96% pour la résolution des incidents.**

Le temps de prise en charge des incidents est resté globalement constant tout au long de l'année 2025, traduisant une continuité des efforts de réponse.

C'est donc un excellent niveau de qualité de service qui a été maintenu depuis 2022 grâce à la mise en place d'alertes sonores lorsqu'un incident survient et le recrutement de nouveaux analystes L1 qui se concentrent uniquement sur la gestion des incidents.

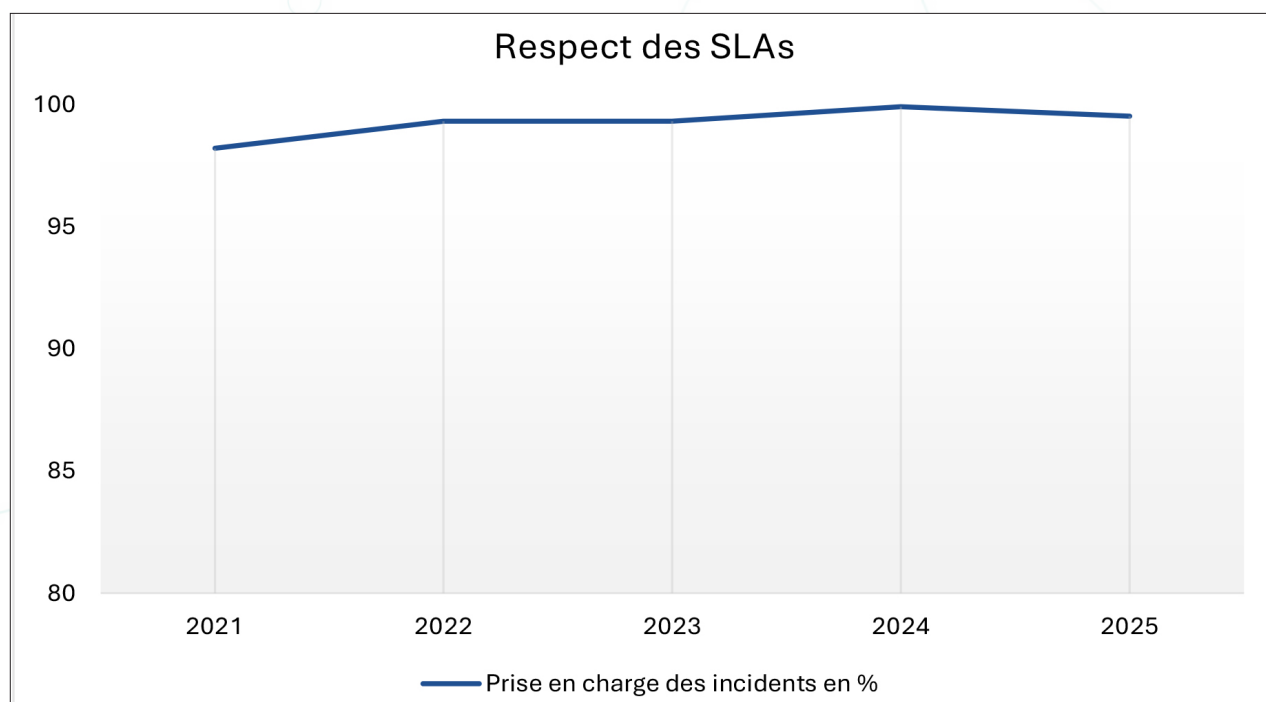


Figure 7 - Évolution du pourcentage de respect des SLAs depuis le démarrage du SOC

4.7.2. Réponse aux incidents : les activités CERT



Le CERT.tg, centre national de réponse aux incidents de cybersécurité, opéré par CDA S.A.S., a poursuivi en 2025 ses missions de surveillance, d'alerte et d'assistance technique. Le CERT national est responsable de la surveillance des risques au Togo associés au cyberspace, de la protection de la société contre les utilisations malveillantes des outils ou services Internet, ainsi que des réponses à apporter aux attaques qui peuvent se produire. L'équipe CERT fournit les services suivants, gratuitement, 24 heures sur 24 et 7 jours sur 7 aux administrations publiques, à toute organisation au Togo et au grand public :

- Analyse des données sur la menace dans le cyberspace togolais selon les informations recueillies auprès de la population togolaise, des entreprises, administrations et autres organisations togolaises ainsi que de la communauté mondiale des CERT et CSIRT ;
- Traitement, réponse et coordination des incidents de cybersécurité nationaux ;
- Notification des menaces détectées et communiquées par les citoyens togolais au centre d'appel, par courrier électronique et sur le site web ;
- Annonce des intrusions, des vulnérabilités et des bulletins de sécurité ;
- Analyse avancée des logiciels malveillants au niveau national et/ou international ;
- Rapports sur les tendances des cyberattaques et leur impact potentiel sur le pays ;
- Formation générale à la cybersécurité et campagnes de sensibilisation proposées au grand public, aux écoles, aux universités, etc. ;
- Réalisation d'audits de sécurité et délivrance de certificats de conformité sous la supervision de l'ANCy ;
- Participation et contribution à des études techniques spécifiques ou à des projets de recherches et développements sur la cybersécurité ;
- Participation à l'élaboration de normes de cybersécurité dans tout le pays.

4.7.2.1. Tableau des incidents traités

CDA a traité 2 528 incidents CERT au cours de l'année 2025 dont **1307 vrais positifs**

4.7.2.2. Évolution des incidents traités

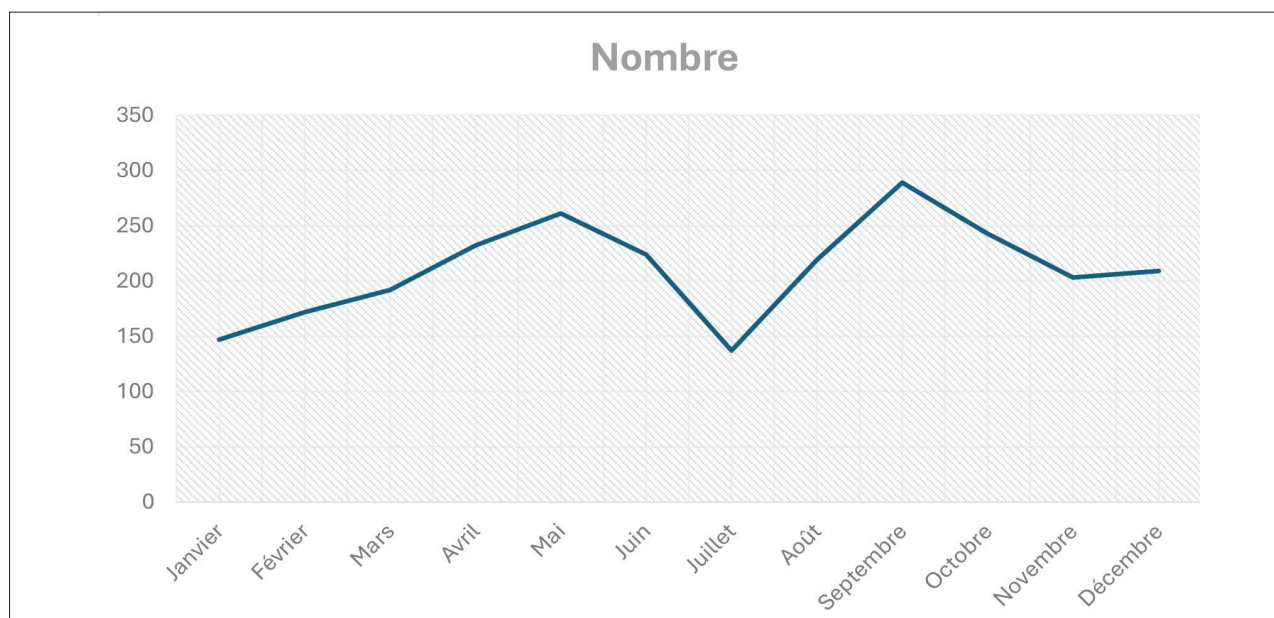


Figure 8 - Évolution des incidents CERT

Les services CERT sont principalement destinés aux citoyens. Nous constatons une évolution des incidents au fur et à mesure que la communication autour de l'ANCy, de CDA et du CERT évolue.

Nous constatons également une tendance qui se répète chaque année avec une forte croissance du nombre d'incidents déclarés par les citoyens togolais en fin d'années relevant des activités d'arnaques ou d'escroquerie en ligne.

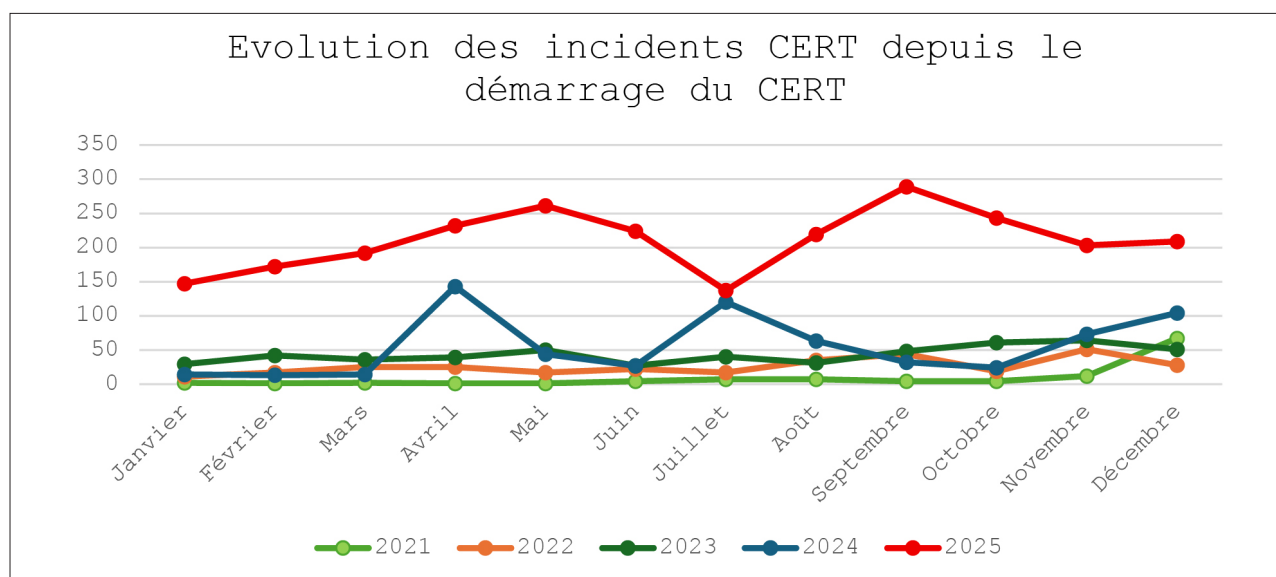


Figure 9 - Évolution des incidents CERT par mois

Evolution des incidents CERT par année

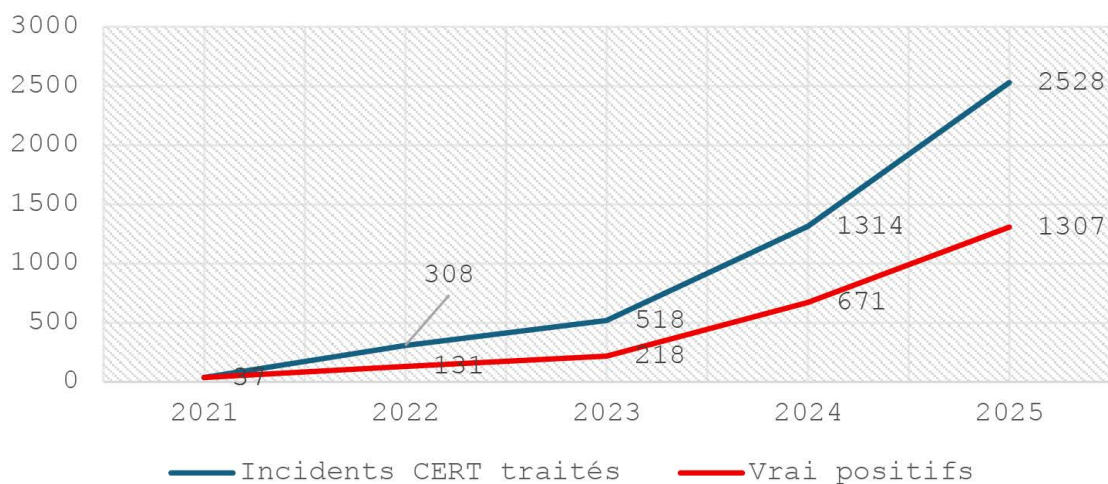


Figure 10 - Évolution des incidents CERT par année

La forte croissance du nombre d'incidents déclarés démontre que les citoyens togolais sollicitent de plus en plus le CERT National lorsqu'ils ont des incidents de cybersécurité.

4.7.2.3. Répartition des incidents CERT traités en 2025

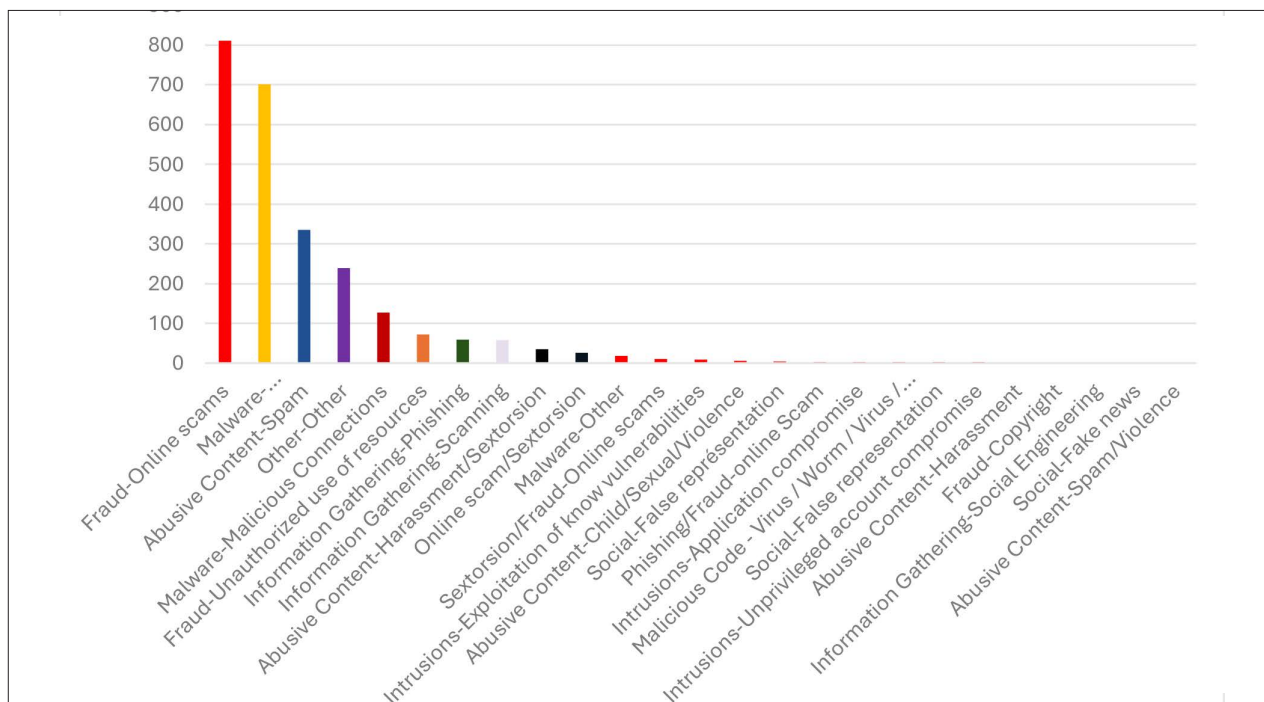


Figure 11 - Répartition des incidents CERT traités

Les incidents les plus fréquemment traités par le CERT.tg sont les fraudes en ligne et les spams comme au cours des 4 dernières années. Bien qu'il y'a une hausse significative du nombre total d'incidents en 2025, la tendance reste presque similaire à celle des années 2023 et 2024, à l'exception des malwares, dont le nombre demeure important depuis l'année 2024.

4.7.2.4. Audit de sécurité pour les entités gouvernementales

En 2025, CDA a réalisé 28 audits d'applications web portées par 9 entités gouvernementales.

4.7.2.5. Alertes sur les vols d'identifiants (Stealers)

CDA effectue une analyse quotidienne des sites web, blogs, groupes, et autres plateformes afin d'identifier des informations susceptibles de compromettre la sécurité du système d'information du gouvernement togolais ou des OSE. Ainsi, CDA a trouvé 1981 identifiants provenant de Stealers.

Les Stealers sont des malwares qui visent à voler des informations telles que les identifiants et les cookies enregistrés dans un navigateur ainsi que d'autres données sensibles. Souvent véhiculés par des logiciels piratés ou usurpés, ils affectent majoritairement des appareils personnels mais touchent couramment les entreprises.

4.7.2.6. Surveillance des sites web

Dans le cadre des activités CERT, CDA surveille les sites web gouvernementaux et autres sites d'importance au Togo. Au cours de l'année 2025, CDA a traité les alertes liées à cette surveillance. Elles se déclinent comme suit :

Incident	Description	# Alertes
Malveillance	Détections critiques (compromissions avérées)	28
Défauts SSL	Certificats expirés, auto-signés ou chaînes incomplètes	560
Timeouts	Latences de connexion suggérant des surcharges serveurs ou des problèmes de connexion.	287
Erreurs HTTP	Codes d'erreurs (principalement 403 et 500)	267
Inaccessibilité	Site inaccessible	982
TOTAL		2124

Tableau 6 - Nb Alertes sur les sites web surveillés

4.7.3. Site web CERT.tg

Le site cert.tg, vitrine officielle du CERT national togolais (Computer Emergency Response Team — Togo), a enregistré une croissance majeure en 2025 avec 23 916 utilisateurs actifs et 26 297 sessions, soit une hausse estimée de +160% des nouveaux utilisateurs par rapport à 2024 (23 528 vs ~9 067). Le site a généré 39 292 pages vues.

L'audience est dominée par deux pôles géographiques : les États-Unis (10 226 utilisateurs, 22% d'engagement, 5s de temps moyen) et le Togo (9 640 utilisateurs, 26% d'engagement, 29s). Le trafic américain, avec son faible engagement, suggère une forte proportion de crawlers et de bots automatisés.

Le trafic est massivement direct (88% des sessions), indiquant soit un accès par URL/bookmark, soit un défaut de tracking des sources (UTM non configurés). Le site reste très orienté desktop (89,6%) avec Chrome comme navigateur quasi exclusif (91,8%).

Chiffre clé : CERT.tg a multiplié par 2,6 ses nouveaux utilisateurs en un an, avec une audience dans plus de 80 pays. Le site est le point d'entrée numérique du CERT national pour le signalement d'incidents et la sensibilisation.

4.7.3.1. Métriques principales 2025

Indicateur	2025	2024 (est.)	Évolution
Utilisateurs actifs	23 916	~9 500	+152%
Nouveaux utilisateurs	23 528	9 067	+160%
Sessions	26 297	11 927	+120%
Pages vues	39 292	—	—
Vues par session	1,49	—	—
Durée moy. Session	1 min 08s	—	—
Scrolls	2 479	—	—
Téléchargements	34	—	—
Clics sortants	311	—	—
Recherches internes	118	—	—

Tableau 7 - Tableau des métriques du site web CERT.tg

La croissance de +160% des nouveaux utilisateurs traduit une visibilité croissante du CERT national. Cependant, les métriques d'engagement sont globalement basses : 1,49 vue par session et 68 secondes de durée moyenne, suggérant que beaucoup de visiteurs ne consultent qu'une seule page avant de quitter le site.

Le nombre très faible de téléchargements (34) et de recherches internes (118) indique que les ressources documentaires sont peu exploitées ou peu mises en avant. C'est un point d'amélioration majeur pour un site de CERT.

4.7.3.2. Principales sources de trafic

Source	Sessions 2025	Sessions 2024
Google (search)	1 498	1 872
ancy.gouv.tg (ANCY)	483	670
Bing	301	240
leadsgo.io	172	0
Facebook (tous)	167	79
cda.tg	78	92
ChatGPT	58	0
LinkedIn	34	27
Twitter/X (t.co)	22	57
CTF.tg	12	64
DuckDuckGo	11	1
Perplexity AI	7	1
africacert.org	8	81

Tableau 8 - Tableau des sources de trafic du site web CERT.tg

Points notables : l'apparition de ChatGPT (58 sessions) et Perplexity AI (7 sessions) comme sources de trafic en 2025 témoigne de la visibilité du CERT dans les modèles d'IA. La baisse d'africacert.org (-90%) et de CTF.tg (-81%) est significative. Le référencement par l'ANCy (ancy.gouv.tg) reste le premier referral institutionnel.

4.7.3.3. Audience géographique (Top 20)

#	Pays	Users
1	États-Unis	10 226
2	Togo	9 640
3	Chine	1 207
4	Ouganda	857
5	Singapour	458
6	France	451
7	Pologne	196
8	Pays-Bas	146
9	Irlande	103
10	Canada	79
11	Allemagne	77
12	Royaume-Uni	53
13	Inde	52
14	Corée du Sud	52
15	Bénin	33
16	Belgique	31
17	Côte d'Ivoire	28
18	Burkina Faso	27
19	Suède	26
20	Brésil	25

Tableau 9 - Top 20 des audiences géographiques

4.7.3.4. Audiences africaines

Pays africain	Users
Togo	9 640
Bénin	33
Côte d'Ivoire	28
Burkina Faso	27
RD Congo	25
Nigeria	24
Maroc	24
Sénégal	22
Ghana	20
Cameroun	13
Tunisie	13
Niger	12
Gabon	11
Mali	11
Tchad	10
Madagascar	10

Tableau 10 - Tableau des audiences africaines

L'audience africaine représente environ 9 923 utilisateurs soit 41% de l'audience totale. Les pays d'Afrique de l'Ouest francophone (Togo, Bénin, Côte d'Ivoire, Burkina Faso, Sénégal) constituent le coeur de cible avec des taux d'engagement nettement supérieurs à la moyenne du site. Le Niger (247s) et le Mali (261s) affichent les temps d'engagement les plus élevés.

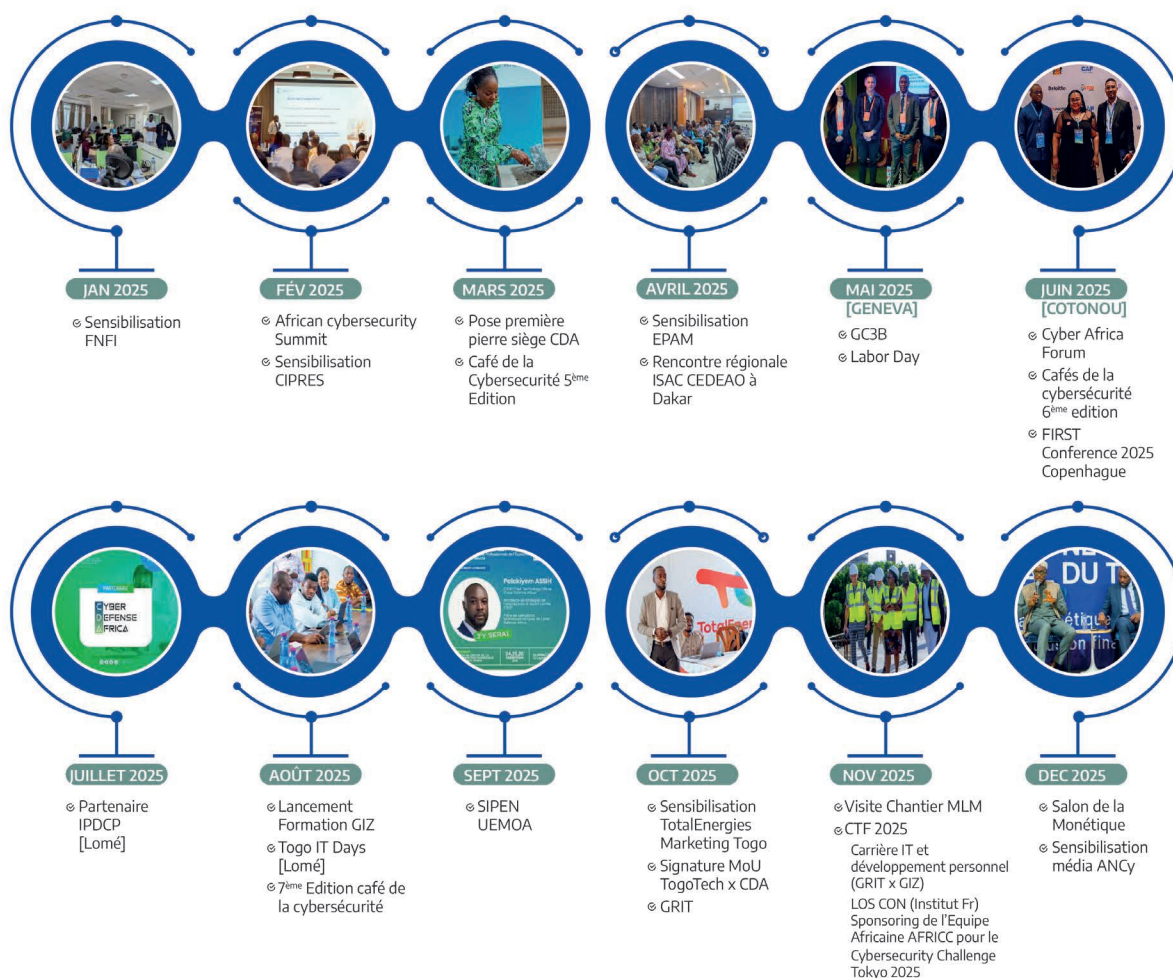
4.7.4. Formations et sensibilisations à la cybersécurité

4.7.4.1. Sensibilisation en présentiel

Tout au long de l'année 2025, nous avons déployé une série de campagnes de sensibilisation visant à informer, éduquer et mobiliser les différentes administrations et entreprises togolaises autour de thématiques essentielles de cybersécurité. Ces initiatives, menées dans divers contextes et auprès de publics variés, ont permis de former un total de 1 107 personnes en 2025. Elles ont ainsi contribué à renforcer la compréhension des enjeux, à encourager des comportements responsables et à favoriser un comportement numérique sain et durable.

4.7.4.2. Participation à des événements et ateliers

2025 a été une année intense sur le plan événementiel. Salons professionnels, conférences techniques, forums régionaux... Ces événements nous ont permis de rencontrer directement nos cibles, d'échanger avec des décideurs et de nouer des partenariats concrets. Ils ont aussi été l'occasion de prendre la parole et de montrer notre savoir-faire.



4.7.4.3. GC3B (Geneva 14-15 mai 2025)

Cyber Defense Africa a pris part à la Conférence mondiale sur le renforcement des capacités en cybersécurité (GC3B), tenue à Genève les 14 et 15 mai 2025. Cette participation s'est inscrite dans une logique de visibilité institutionnelle, de positionnement stratégique et de développement de relations internationales.

Aux côtés du Directeur Général, Simon Melchior, le marketing a joué un rôle actif tout au long de l'événement.



Photo 29 : M. Simon MELCHIOR, DG de CDA et Mme Belynda LAWSON-BETUM, la responsable marketing de CDA

En amont et pendant les deux jours de conférence, une couverture médiatique a été assurée, incluant la production de contenus, la valorisation de la présence de CDA et le relais des interventions de l'entreprise. Le marketing a également accompagné et renforcé la portée des deux panels auxquels Simon Melchior a pris part, en assurant la mise en contexte, la visibilité des messages clés et la présentation de Cyber Defense Africa auprès des différents publics présents.

Par ailleurs, cette participation a permis de conduire plusieurs actions de networking ciblées. Des échanges ont eu lieu avec des acteurs institutionnels, privés et internationaux, notamment en provenance :

- du Gabon,
- de la Jamaïque,
- du Nigeria,
- de la Côte d'Ivoire
- et du Sénégal.
- des USA
- de Royaume Uni

Des rencontres ont également été réalisées avec des professionnels du secteur de la cybersécurité, des représentants d'organisations internationales, ainsi qu'avec la Chief Security Officer d'Adobe. Des discussions directes avec les organisateurs de la conférence ont permis de renforcer les relations avec l'écosystème GC3B et de positionner Cyber Defense Africa comme un acteur engagé et crédible sur les enjeux de cybersécurité et de coopération internationale.



Photo 30 : Quelques partenaires rencontrés au GC3B

Globalement, cette mission a contribué à accroître la visibilité de Cyber Defense Africa, à présenter ses expertises et à élargir son réseau de partenaires et de contacts à l'échelle internationale, confirmant le rôle stratégique du marketing comme levier de représentation, d'influence et de développement.

4.7.4.4. Participation à la FIRST Conference 2025 (Copenhague)

En juin 2025, des représentants de Cyber Defense Africa (Kossi DOH & Anissa KPAKPABIA) ont participé à la FIRST Conference 2025 (FIRSTCON25) ainsi qu'à la conférence NATSCIRT, organisées à Copenhague.

Cette participation s'inscrivait dans le cadre du projet ECOWAS Commission ISAC, soutenu par l'Union européenne, la Commission de la CEDEAO et le Ministère fédéral allemand des Affaires étrangères (Auswärtiges Amt). La FIRST Conference constitue le rendez-vous annuel des équipes de réponse aux incidents (CSIRT) membres du Forum of Incident Response and Security Teams (FIRST).

Durant cinq jours, les équipes de Cyber Defense Africa ont pris part à des sessions techniques, des panels d'experts, des réunions spécialisées (SIG et BoFs), ainsi qu'à une compétition de type Capture The Flag (CTF). Ces activités ont permis de renforcer les compétences techniques en matière de prévention, de détection et de gestion des incidents de cybersécurité, tout en favorisant les échanges avec des acteurs du cyberspace à l'échelle internationale.

À l'issue de FIRSTCON25, Cyber Defense Africa a également participé à la conférence annuelle des CSIRT nationaux (NATSCIRT), tenue les 27 et 28 juin 2025. Cette conférence

a permis d'approfondir les échanges entre équipes nationales de réponse aux incidents et de renforcer la coopération régionale et internationale.

Cette mission s'inscrit dans l'engagement de Cyber Defense Africa, en tant qu'opérateur du CERT-TG sur délégation de pouvoir de l'Agence Nationale de la Cybersécurité (ANCy), à contribuer activement au renforcement de la résilience de l'écosystème cyber en Afrique de l'Ouest et au-delà.



Photo 31 : Des participants à la FIRST 2025

4.7.4.5. Les cafés de la cybersécurité

Les thèmes abordés durant l'année 2025 sont :

1. **Les Menaces du Dark Web** (focus sur les immersions, le CTI, connectivité sécurisée)
2. **Gestion des identités et des accès** (IAM, PAM et retours d'expérience terrain)
3. **Comment construire un Budget de cybersécurité ?** (CAPEX, OPEX et gouvernance des risques)
4. **L'Intelligence humaine face aux nouvelles menaces** (le rôle de l'humain dans la résilience)

Le taux de participation excède les 80% pour chaque édition sur la base des invitations envoyées

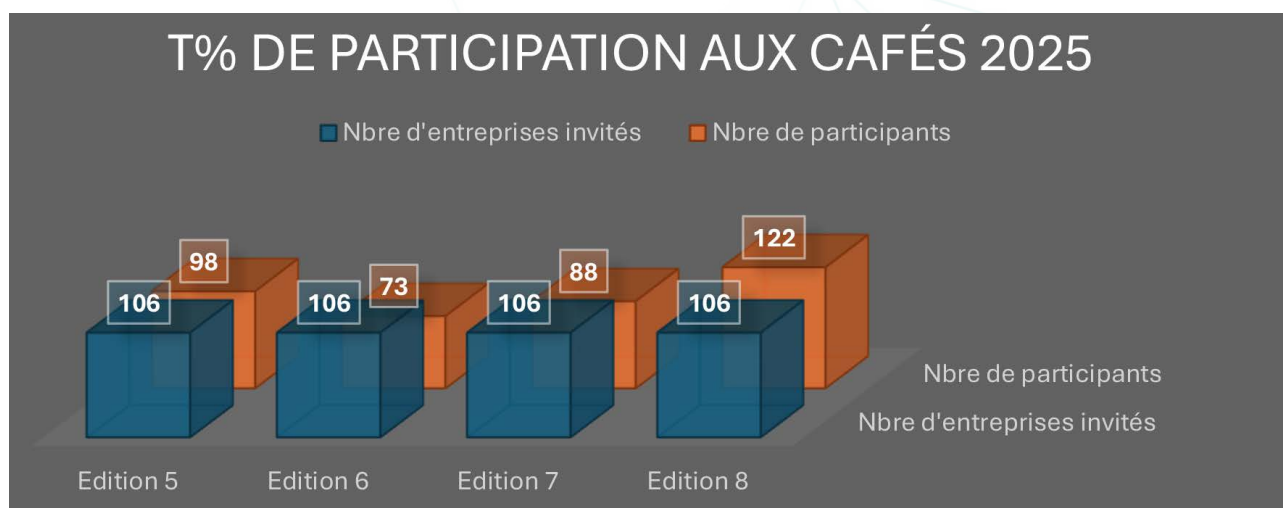


Photo 32 : Des participants aux cafés

4.7.4.6. Forum International pour la Protection des Données à caractères Personnelles

Le Forum International pour la Protection des Données à Caractère Personnel a constitué un temps fort de réflexion et d'échanges autour des enjeux de conformité, de gouvernance des données et de protection de la vie privée.

À cette occasion, le département Marketing & Communication de Cyber Defense Africa a assuré la modération de panels, en anglais et en français, facilitant le dialogue entre autorités, experts et acteurs du secteur. Cette modération a permis de structurer les échanges, de faire émerger des retours d'expérience concrets et de rendre accessibles des sujets techniques à un public élargi.

Cette intervention a contribué à renforcer la visibilité de Cyber Defense Africa sur les thématiques de protection des données et à affirmer son positionnement dans les débats liés à la régulation et à la sécurité de l'information.



Photo 33 : Un panel modéré par la responsable marketing et communication de CDA, à l'extrême gauche

4.7.4.7. Rencontre Annuelle du BIC-UEMOA

Le 9 octobre 2025, Cyber Defense Africa a été représentée à la 7^e Rencontre Annuelle du BIC-UEMOA à Cotonou par son Directeur Technique (CTO), Palakiyem ASSIH, aux côtés d'acteurs majeurs du secteur financier de l'espace UEMOA.

Cette rencontre, placée sous le thème « Cybersécurité et protection des données : un enjeu stratégique pour la gestion du risque de crédit », a mis en lumière les nouveaux défis auxquels font face les institutions financières, dans un contexte de digitalisation accélérée et d'interconnexion croissante des systèmes.

Les échanges ont souligné les risques liés à la manipulation de volumes importants de données sensibles, notamment les attaques ciblant les bases clients, la compromission d'API entre partenaires et les intrusions dans les systèmes de scoring et d'analyse du risque.

À cette occasion, Palakiyem ASSIH a rappelé que la cybersécurité constitue un prérequis à toute digitalisation durable du secteur financier. Il a insisté sur la nécessité de s'appuyer sur des architectures de sécurité robustes, intégrant notamment le chiffrement des données, la segmentation des réseaux, la supervision en temps réel et une approche Zero Trust.

Les discussions menées avec des acteurs tels que l'Union Togolaise de Banque (UTB) et Creditinfo Group West Africa ont porté sur l'équilibre entre sécurité et performance, la conciliation entre conformité aux normes internationales telles que l'ISO 27001 et innovation, ainsi que sur le renforcement d'une cyber-résilience collective à l'échelle régionale.

Cette participation s'inscrit dans l'engagement de Cyber Defense Africa à accompagner les acteurs financiers d'Afrique de l'Ouest dans la sécurisation de leurs systèmes d'information et le renforcement de la confiance numérique, condition essentielle à la stabilité et à la résilience des écosystèmes financiers.



Photo 34 : M. ASSIH (au micro) lors de son intervention

4.7.4.8. La GRIT

La participation de CDA s'est matérialisée par un espace sur le stand des entités gouvernementales. Diffusion de supports (flyers), échanges de réseautage avec la communauté tech venue de plusieurs pays africains, en présence de Madame la Ministre et des institutions du secteur numérique.



Photo 35 : Le stand de CDA animé par une stagiaire

4.7.4.9. Signature d'un MoU entre CDA et TogoTech

La signature d'un MoU formalisant un cadre de collaboration entre CDA et la Synergie TogoTech, positionnant CDA comme référent cybersécurité au sein de l'écosystème startups et intégrant la cybersécurité comme standard de confiance pour les entreprises technologiques émergentes, est intervenue en octobre 2025 en présence de Madame Cina LAWSON, Ministre de l'Efficacité du Service Public et de la Transformation Numérique.



Photo 36 : Mme le Ministre Cina LAWSON, posant avec Me Alexis ACQUEREBURU, Maire des Lacs 1 (à l'extrême droit), M. Simon MELCHIOR, DG de CDA et Mme Gael EGBIDI, Présidente de TogoTech.



Photo 37 : Échange de paraphes entre les signataires du MoU

4.7.4.10. LOS CON 2025

En novembre 2025, CDA a pris part aux temps forts de la conférence Open Source, Linux & Cybersécurité, favorisant les échanges avec la communauté tech autour des enjeux de sécurité des systèmes et des usages numériques.



4.7.4.11. Sponsoring de l'Equipe Africaine AFRICC pour le Cybersecurity Challenge Tokyo 2025

Dans le cadre de l'International Cybersecurity Challenge (ICC), Cyber Defense Africa (CDA) a apporté son soutien à la participation de la Team Africa (AFRICC) à la compétition internationale organisée au Japon. Cette initiative a permis de valoriser l'émergence de jeunes talents africains en cybersécurité, dont deux représentants togolais, Essowèréou Charles ASSIMTI et Daniel GOGO.

À travers ce soutien, CDA affirme son engagement en faveur du développement des compétences, de la détection des talents et du renforcement de la résilience numérique à l'échelle du continent, en accompagnant une nouvelle génération d'acteurs de la cybersécurité.

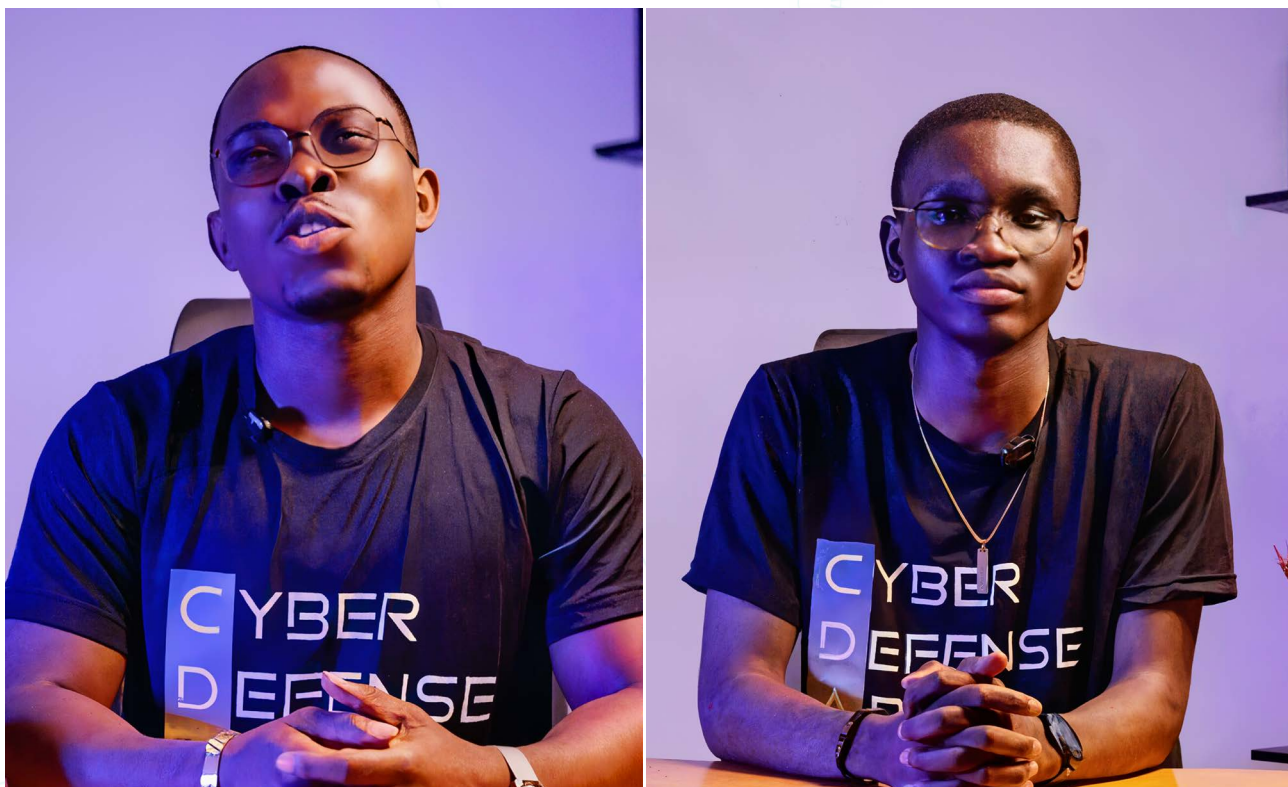


Photo 38 : Daniel GOGO et Charles ASSIMTI, représentants du Togo au ICC Tokyo 2025





V : COMMUNICATION INSTITUTIONNELLE ET RELATIONS PUBLIQUES

Rapport d'activités 2025



V : Communication institutionnelle et relations publiques

La communication institutionnelle et les relations publiques occupent une place stratégique dans l'action de l'ANCy. Elles constituent un levier essentiel pour informer, sensibiliser, renforcer la confiance des citoyens et favoriser l'adhésion des parties prenantes aux politiques publiques en matière de cybersécurité. En 2025, l'ANCy a poursuivi le déploiement d'une communication proactive, pédagogique et inclusive, visant à rendre les enjeux de cybersécurité compréhensibles par tous et à confirmer l'Agence comme institution de référence au service de la sécurité numérique nationale.

5.1. Relations presse et médias

2025 a été l'année du renforcement des relations avec les médias nationaux, considérés comme des partenaires stratégiques dans la diffusion des messages de prévention et de sensibilisation. À travers des rencontres, des interviews, des émissions interactives et la diffusion de communiqués de presse, l'ANCy a contribué à une meilleure compréhension des enjeux liés à la cybersécurité auprès du grand public. Ces actions ont permis de vulgariser les concepts clés de la cybersécurité, d'alerter sur les menaces émergentes et les bonnes pratiques à adopter et de valoriser les actions et initiatives menées par l'ANCy. La collaboration avec les journalistes a également favorisé un traitement médiatique plus responsable et plus précis des questions liées aux incidents cyber et à la sécurité numérique.



Dans ce cadre, plusieurs émissions interactives ont été animées sur des médias de grande audience, notamment Radio Kara, Radio Lomé, la Télévision Togolaise (TVT), Pyramide FM, la Radiotélévision Delta Santé (RTDS), Radio Métropolys, etc. Ces interventions ont permis de vulgariser les concepts clés de la cybersécurité, d'alerter sur les menaces émergentes, de promouvoir les bonnes pratiques à adopter au quotidien et de valoriser les actions et initiatives menées par l'ANCy.

Par ailleurs des interviews ont été accordées par le Directeur Général à des médias en ligne spécialisés à l'instar du magazine panafricain « Africa Cybersecurity Mag » (<https://cybersecuritymag.africa/securite-numerique-au-togo-etat-des-lieux-et-perspectives/>) ou de « CIO-Mag » (<https://cio-mag.com/cybersecurite-gbota-gwaliba-dg-de-lancy-togo/>).



Cette collaboration renforcée avec les professionnels des médias a également favorisé un traitement plus responsable, plus précis et plus pédagogique des questions liées aux incidents cyber et à la sécurité numérique, contribuant ainsi à l'émergence progressive d'une culture de cybersécurité au sein de la population togolaise.

5.2. Communication digitale et supports institutionnels

En complément des médias traditionnels, l'Agence Nationale de la Cybersécurité (ANCy) a fortement mobilisé ses canaux digitaux, faisant de la communication numérique un pilier central de sa stratégie en 2025. À travers son site web institutionnel et ses plateformes en ligne, l'Agence a assuré une diffusion régulière d'informations, de communiqués officiels, d'alertes et de contenus de sensibilisation à destination des citoyens, des administrations publiques et des acteurs de l'écosystème numérique.

Ces contenus ont été relayés de manière continue sur la page Facebook : [@AncyTG \(https://m.facebook.com/AncyTG\)](https://m.facebook.com/AncyTG), le compte X : [@AncyTogo \(https://x.com/ancytg\)](https://x.com/ancytg), la page LinkedIn : [Agence nationale de la cybersécurité – Togo \(https://www.linkedin.com/company/ancytg/\)](https://www.linkedin.com/company/ancytg/), ainsi que sur le site officiel www.ancy.gouv.tg.

Les activités intégrant des supports audiovisuels ont, par ailleurs, été valorisées sur la chaîne YouTube [@ANCyTG \(https://youtube.com/ANCyTG\)](https://youtube.com/ANCyTG), renforçant ainsi l'impact et la portée des messages diffusés.



Parallèlement, l'ANCy a conçu et diffusé une variété de supports institutionnels et pédagogiques (visuels de sensibilisation, plaquettes institutionnelles, posters, etc.) destinés à accompagner efficacement les actions de terrain. Élaborés dans un souci constant de clarté et d'accessibilité, ces supports ont été pensés pour toucher un public large et diversifié, allant des jeunes aux personnes âgées, toutes catégories socioprofessionnelles confondues.

QUI SOMMES-NOUS ?

Créée par la loi n°2018-026 du 7 décembre 2018, l'ANCy est l'institution chargée de la mise en œuvre de la politique nationale de cybersécurité du Togo.

NOTRE VISION

Participer à la transformation digitale du Togo par la sécurisation de son cyberspace.

NOS MISSIONS

- Coordonner la défense numérique de l'État
- Réglementer et contrôler la cybersécurité
- Certifier les produits et prestataires
- Sensibiliser et former les acteurs
- Auditer les services essentiels
- Assurer la veille et la réponse aux incidents (CERT.tg, SOC)
- Lutter contre la cybercriminalité

NOS OFFRES

Pour les citoyens :

- Campagnes de sensibilisation et d'éducation numérique.
- Conseils pratiques pour protéger les données.

Pour les Entreprises et Administrations :

- Qualification des prestataires et produits de cybersécurité
- Audit et accompagnement des opérateurs de services essentiels (OSE)
- Formations et renforcement des capacités des équipes techniques

NOTRE PROPOSITION DE VALEUR

- Protéger les institutions, les entreprises et les citoyens
- Certifier les prestataires et les produits fiables
- Renforcer les compétences et les bons comportements en ligne

RÉALISATIONS PHARES (2020-2025)

- Stratégie nationale de cybersécurité (2024)
- Compétitions nationales de cybersécurité (2023 et 2024)
- Classement du Togo : Tier 2 – "Advancing" (GCI 2024, score 89,8)

VISION 2030

Faire du Togo un pays de référence en matière de confiance et de résilience numérique en Afrique.

ENSEMBLE, CONSTRUONS UN TOGO CYBERSÉCURISÉ ET CONFIANT !

Siège : 63, boulevard du 13 janvier, Lomé, Togo

Site web: www.ancy.gouv.tg Contact : secretariat.ancy@ancy.gouv.tg

Cette présence renforcée et cohérente a contribué à accroître la visibilité de l'Agence, à faciliter l'accès à l'information et à consolider la culture de la cybersécurité au sein de la société togolaise.

5.3. Événements, conférences et ateliers thématiques

En 2025, l'ANCy a pris part à plusieurs événements, tant au niveau national que régional, voire international.

5.3.1. African cybersecurity summit (Rabat)

Cette rencontre s'est tenue du 3-5 février 2025. Événement d'envergure continentale, c'était une initiative de la Direction Générale de la Sécurité des Systèmes d'Information (DGSSI) et de Smart Africa. Il a réuni gouvernements, experts et leaders du secteur pour renforcer la coopération et explorer des solutions innovantes face aux cybermenaces.

Sujets clés :

- IA & Cloud de Confiance : Leviers stratégiques pour la cybersécurité en Afrique ;
- Gestion des Risques Cyber face à la transformation numérique ;
- Sécurisation des Infrastructures Critiques (énergie, pétrole, gaz) ;
- Protection des Grands Événements Internationaux (Coupe du Monde, Jeux Olympiques).

Au programme étaient inscrits des panels de haut niveau et ateliers pratiques, sur l'IA appliquée au contexte africain Réunion annuelle des Autorités Nationales de Cybersécurité Africaines (ANCA).



Photo 39 : Le DG de l'ANCy (à gauche) et le DT de CDA à l'ACS Rabat 2025

5.3.2. Cyber Africa Forum 2025

Les 24 et 25 juin 2025, le Cyber Africa Forum (CAF) a rassemblé à Cotonou, en République du Bénin, plus de 1 500 experts, décideurs et acteurs majeurs du numérique et de la cybersécurité. Après quatre éditions consécutives organisées en Côte d'Ivoire, le choix du Bénin comme pays hôte traduit la volonté du Forum d'élargir son ancrage régional et de promouvoir une réflexion panafricaine sur les enjeux du numérique et de la cybersécurité.

L'ANCy y était représentée par M. Nangbam DIDEMANA, Directeur de la réglementation et du contrôle de conformité, et M. Malik GERALDO, Directeur de la formation et du renforcement des capacités. Leur participation a contribué à renforcer la visibilité de l'ANCy et à promouvoir l'expertise togolaise en matière de gouvernance de la cybersécurité, de développement des compétences et de coopération régionale.

Cyber Defense Africa a également prit part à cette rencontre internationale africaine. Cette participation au CAF a permis à CDA de présenter ses activités et de conduire des échanges avec des partenaires et acteurs du secteur, notamment Fortinet.

Cette présence a contribué au renforcement du réseau de contacts de Cyber Defense Africa et à l'identification d'opportunités de collaboration.



Photo 40 : Les représentants de l'ANCy (2è et 4è à partir de la gauche) et de CDA au CAF 2025

Les échanges et travaux du Forum ont été guidés par un objectif commun : transformer les défis liés aux cybermenaces en leviers de croissance durable, afin de renforcer la souveraineté numérique du continent et de contribuer à la construction d'un avenir numérique sécurisé et prospère pour l'Afrique.

Cette édition a connu une forte mobilisation internationale, avec la participation de plus de 1 500 participants issus de 30 pays. Le programme a été marqué par l'organisation de plus de 45 sessions, incluant panels, ateliers et événements parallèles, la participation de plus de 250 leaders de haut niveau des secteurs public et privé, la tenue d'un HackerLab, la signature de quatre accords stratégiques...

5.3.3. Togo IT Days

Les Togo IT Days 2025 ont constitué un grand rendez-vous réunissant leaders, experts, entrepreneurs et passionnés du numérique. Tenus les 13 et 14 août 2025 à Lomé, ils ont mis en lumière les grandes tendances, les défis stratégiques et les opportunités d'investissement dans des secteurs clés tels que la cybersécurité, la protection des données, l'intelligence artificielle, le machine learning, le numérique responsable, l'entrepreneuriat technologique et le développement des talents.

À cette occasion, l'ANCy a enrichi de sa participation le panel consacré au thème « Cybersécurité & Protection des Données : anticiper, protéger, inspirer confiance », à travers l'intervention de son Directeur Général, le Commandant Gbota GWALIBA., réaffirmant ainsi l'engagement de l'Agence en faveur d'un environnement numérique sûr et de confiance.

Le programme a été marqué par des conférences, des keynotes, des ateliers pratiques, un hackathon d'innovation ainsi qu'un village d'exposition rassemblant entreprises, startups et institutions du secteur numérique.

Présente également, Cyber Defense Africa à travers sa cellule Marketing & Communication, a assuré la modération de panels thématiques, jouant un rôle de facilitateur entre acteurs publics, privés et académiques. L'objectif était



Photo 41 : Le Cdt Gbota GWALIBA, DG de l'ANCy lors du panel auquel il participait

de favoriser des échanges fluides, orientés usages, et de mettre en perspective les enjeux de sécurité dans les projets numériques. Cette présence active a permis de renforcer la notoriété de Cyber Defense Africa au sein de l'écosystème technologique national et de consolider des relations avec des parties prenantes clés.



Photo 42 : Un panel modéré par la responsable marketing et communications de CDA

5.3.4. Salon International des Professionnels de l'Économie Numérique de l'UEMOA (SIPEN l'UEMOA)

Du 24 au 26 septembre 2025, l'Agence nationale de la cybersécurité (ANCy) a pris part au Salon international des professionnels de l'économie numérique de l'UEMOA (SIPEN-UEMOA), organisé à Lomé autour du thème : « L'humain au centre de la transformation numérique dans l'espace UEMOA ». Placée sous l'égide de l'UEMOA et portée par le Regroupement des organisations professionnelles des TIC de l'UEMOA (ROP-TIC), cette troisième édition du salon s'inscrit dans la volonté de pérenniser un cadre annuel de dialogue et d'innovation au service de l'économie numérique régionale.

L'ANCy était représentée à cet événement par M. Nangbam DIDEMANA, Directeur de la Réglementation et du Contrôle de Conformité, et par M. Nagbandjoa DOUNWOURGUE, Chargé de la Communication et des Relations Publiques, contribuant à la valorisation de l'action de l'Agence et au renforcement des échanges avec les acteurs institutionnels et privés de l'écosystème numérique régional.

Cyber Defense Africa a pris part à des panels à travers son Directeur Technique, M. Palakiyem ASSIH. Le département Marketing & Communication de CDA a assuré la modération de panels, contribuant à animer les discussions, à croiser les expériences des différents pays et à mettre en lumière les enjeux communs en matière de cybersécurité. Cette intervention a renforcé la visibilité régionale de Cyber Defense Africa et soutenu le développement de relations institutionnelles et partenariales à l'échelle sous-régionale.

SIPEN-UEMOA
Salon International des Professionnels de l'Économie Numérique de l'UEMOA

3^{ème} EDITION
LOMÉ 2025

UN EVENEMENT HYBRIDE

Palakiyem ASSIH
CISSP Chief Technology Officer,
Cyber Defense Africa

Architecte de stratégies de
cyberdéfense et expert certifié
CISSP

Pilote les opérations
techniques critiques de Cyber
Defense Africa.

J'Y SERAI

THEME DU SALON
L'HUMAIN AU CENTRE DE LA
TRANSFORMATION NUMÉRIQUE
DANS L'ESPACE UEMOA

24,25,26
Septembre
2025

Hôtel 2 Février,
Lomé, Togo

Cette édition togolaise a connu une forte mobilisation, réunissant plus de 10 exposants internationaux, environ 9 000 participants et près de 170 entreprises, confirmant l'intérêt croissant des acteurs de l'espace UEMOA pour les enjeux liés à l'économie numérique et à la cybersécurité.

SIPEN-UEMOA
Salon International des Professionnels de l'Économie
Numérique de l'UEMOA



3^{ème} EDITION
**LOMÉ
2025**

UN EVENEMENT HYBRIDE

Thème

L'HUMAIN AU CENTRE DE LA TRANSFORMATION NUMÉRIQUE DANS L'ESPACE UEMOA



**24,25,26
Septembre
2025**

 **Hôtel 2 Février,
Lomé, Togo**

PARTENAIRES INSTITUTIONNELS



UN EVENEMENT HYBRIDE COORGANISÉ PAR



5.3.5. Convention des Nations Unies contre la cybercriminalité

La première convention mondiale dédiée à la prévention et à la lutte contre la cybercriminalité a été ouverte à la signature à Hanoï, au Vietnam, les 25 et 26 octobre 2025. Vingt-et un (21) pays africains, dont le Togo, figurent parmi les premiers signataires : l'Algérie, l'Angola, le Burkina Faso, la Côte d'Ivoire, la République démocratique du Congo, Djibouti, l'Égypte, le Ghana, la Guinée-Bissau, la Libye, le Maroc, le Mozambique, la Namibie, le Nigeria, l'Afrique du Sud, l'Ouganda, la Tanzanie, le Zimbabwe, le Mali et le Rwanda. Le Togo était représenté par le Directeur Général de l'Agence Nationale de la Cybersécurité (ANCy), le Commandant Gbota GWALIBA.



Photo 43 : Le président vietnamien Luong Cuong posant avec les chefs de délégations participant à la cérémonie d'ouverture

Face à une cybercriminalité qui redéfinit les modes opératoires du crime organisé, cette Convention constitue un instrument stratégique majeur pour renforcer la coopération internationale et doter les États d'un cadre juridique harmonisé.

- Il s'agit du premier cadre mondial pour la collecte, le partage et l'utilisation des preuves électroniques pour toutes les infractions graves. Jusqu'à présent, il n'existait aucune norme internationale largement acceptée en matière de preuves électroniques ;
- Il s'agit du premier traité mondial à criminaliser les crimes cyberdépendants ainsi que les infractions liées à la fraude en ligne, aux contenus pédopornographiques et à la sollicitation d'enfants en ligne ;
- Il s'agit du premier traité international à reconnaître la diffusion non consensuelle d'images intimes comme une infraction ;

- Il crée le premier réseau mondial accessible 24 heures sur 24 et 7 jours sur 7, grâce auquel les pays peuvent rapidement engager une coopération ; et
- Il reconnaît et promeut la nécessité de renforcer les capacités des pays à poursuivre et à coopérer dans le domaine des cybercrimes, qui évoluent rapidement.

Il convient toutefois de rappeler que la Convention de Hanoï entrera en vigueur après sa ratification par au moins 40 pays.

5.3.6. Grande Rencontre de l'Innovation Technologique

La Grande Rencontre de l'Innovation Technologique au Togo (GRIT) s'est tenue à Lomé du 29 au 30 octobre 2025. Elle s'est imposée comme vitrine du dynamisme de l'écosystème numérique togolais et africain, en réunissant plus de 2 000 participants sur deux jours, complétés par trois jours de « side events. » Ces rencontres ont favorisé des échanges ciblés

et approfondis entre entrepreneurs, investisseurs et experts, permettant de découvrir des talents et startups à différents stades de développement.



Organisée par le Ministère de l'Efficacité du Service public et de la Transformation numérique, avec le soutien de la GIZ Togo, du BMZ (Allemagne), du Ministère des Affaires étrangères et européennes du Luxembourg, de l'Union européenne et d'AfricArena, la GRIT a mis en avant des sessions de pitches et des conférences, valorisant des startups à fort potentiel et offrant une plateforme d'échanges, de collaboration et de création d'opportunités pour l'ensemble des acteurs du numérique.



Photo 44 : Madame le Ministre Cina LAWSON (au centre en tenue blanche) posant avec les invités et partenaires à l'ouverture officielle du sommet

Pendant les deux jours de la GRIT, plus d'une quarantaine de startups locales et internationales ont pitché leurs projets devant des investisseurs. Six parmi elles ont suscité un grand intérêt chez les investisseurs, leur permettant de remporter différents prix. Sur le plan national, c'est la startup Kidolé qui a remporté le premier prix. Le deuxième prix pitch a été remporté par Edomatch tandis que la startup Cookeza a remporté le troisième prix. Ces trois startups ont bénéficié de six mois d'accompagnement en levée de fonds ainsi que d'une qualification pour la finale du Grand Summit AfricArena en Afrique du Sud.



Photo 45 : Une promotrice de startup présentant sa solution

L'ANCy y a participé activement avec un stand institutionnel, présentant ses missions et son rôle dans la sécurisation de l'écosystème numérique. Cette présence a permis de sensibiliser startups, investisseurs et porteurs de projets à l'importance d'intégrer la cybersécurité dès la conception des solutions et des projets, tout en promouvant les dispositifs d'accompagnement et de régulation mis en place par l'Agence pour un environnement numérique sûr et de confiance.

5.3.7. Maputo Cyber Week



La Maputo Cyber Week, ou Semaine Internationale de la Cybersécurité du Mozambique (SISCIM), s'est déroulée du 17 au 21 novembre 2025 au bureau du procureur général à Maputo. Cet événement vise à renforcer la résilience numérique nationale et régionale.

Au cours de cette semaine organisée par le ministère des Communications et de la Transformation numérique (MCTD), par l'intermédiaire de l'Institut national des technologies de l'information et de la communication (INTIC).



Photo 46 : Le Commandant Gbota GWALIBA (premier de la gauche), DG de l'ANCy prenant part à un panel d'experts

Au cours de cinq journées, des spécialistes, des décideurs, des universitaires et des partenaires internationaux ont débattu des questions de cybersécurité de l'heure dans le but de réfléchir continuellement au renforcement de l'écosystème de sécurité.

L'évènement a également été le lieu de signature d'un mémorandum d'entente entre le Togo et le Mozambique.

5.3.8. La Nuit du Droit

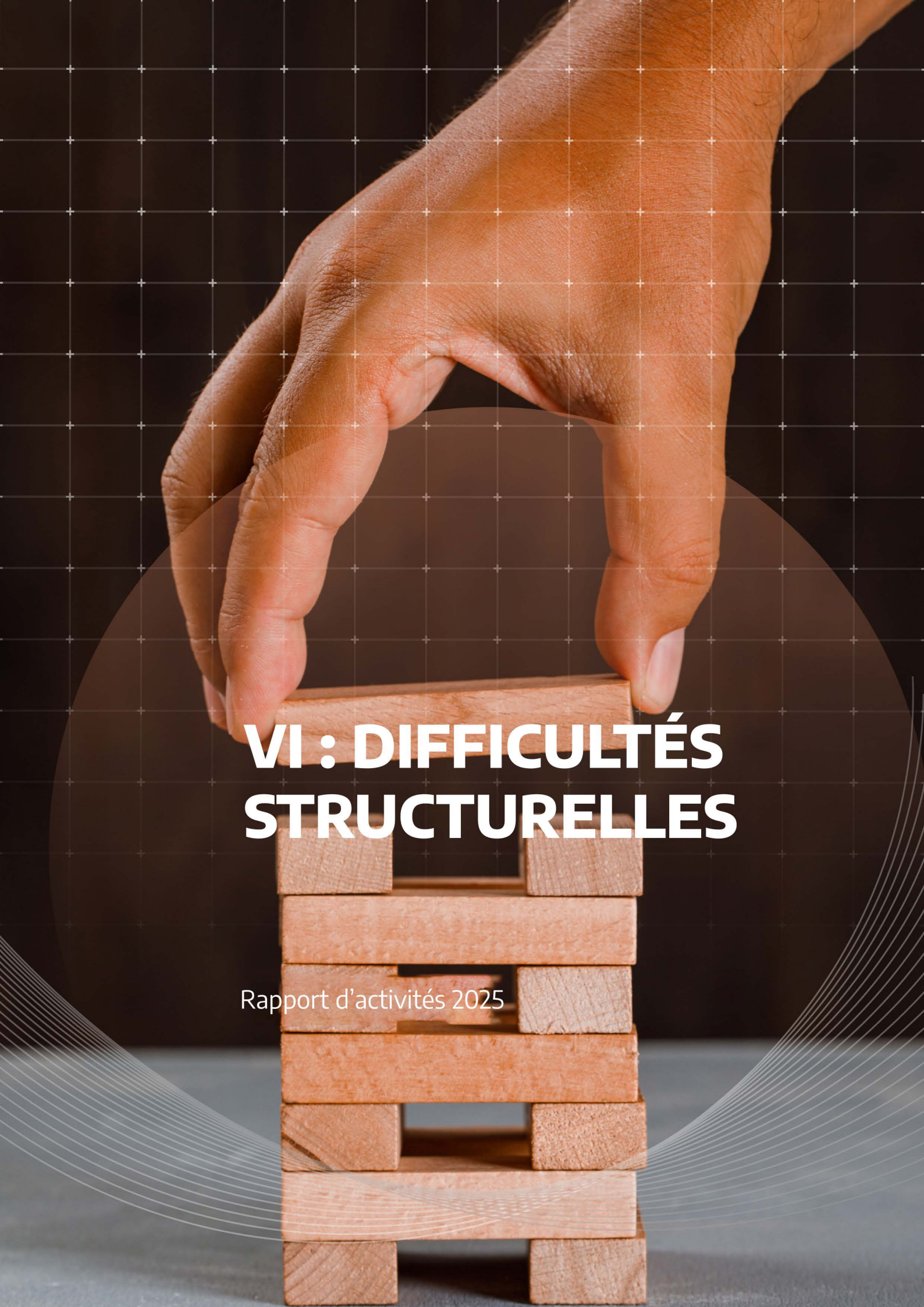
La troisième édition de la Nuit du Droit s'est tenue le 22 novembre 2025 à Lomé autour du thème : « Droit et transformation numérique : vers une société de confiance ? » À cette occasion, l'ANCy représentée par le juriste M. OTIMI Yaouvi, a présenté la vision et l'action du Togo en matière de cybersécurité, dans un contexte de transformation numérique accélérée.



Photo 47 : M. OTIMI (au micro), intervenant lors du panel

Celui-ci a rappelé l'ambition nationale de faire du Togo, à l'horizon 2030, un hub logistique et un centre d'affaires fondé sur un usage sécurisé et maîtrisé des technologies numériques. Il a mis en lumière la Stratégie Nationale de Cybersécurité, articulée autour du développement des compétences, de la protection des services critiques, du renforcement de la réponse aux incidents et de la lutte contre la cybercriminalité, ainsi que les actions concrètes menées en faveur des citoyens, des entreprises et des administrations, notamment à travers la sensibilisation, la formation de plus de 250 informaticiens, l'accompagnement des opérateurs de services essentiels et la qualification des prestataires de confiance. Cette intervention a également permis de souligner les avancées notables du pays, dont son intégration au Tier 2 de l'Index mondial de cybersécurité de l'UIT, témoignant des progrès accomplis et de la volonté des autorités togolaises de bâtir un cyberspace sûr, résilient et inclusif au service du développement et du bien-être des populations.



A close-up photograph of a hand with a light skin tone carefully placing a wooden block onto a tower of Jenga blocks. The tower is built with light-colored wooden blocks, some of which have notches cut out. The background is dark with a subtle grid pattern and a large, semi-transparent brown circle behind the hand and the top of the tower. The overall mood is one of precision and balance.

VI : DIFFICULTÉS STRUCTURELLES

Rapport d'activités 2025



VI : Difficultés structurelles

L'écosystème national de cybersécurité fait face à des difficultés organisationnelles, opérationnelles et techniques qui limitent l'efficacité des mécanismes de prévention et de réponse.

6.1. Difficultés organisationnelles

6.1.1. Déficit de compréhension stratégique de certains décideurs

Un déficit de compréhension stratégique de la cybersécurité subsiste chez certains décideurs, qui la perçoivent encore comme une contrainte technique plutôt qu'un enjeu de souveraineté et de continuité des services. Cette faible culture de cybersécurité et de gestion des risques entraîne des arbitrages défavorables à la sécurité numérique et une absence de leadership en matière de gouvernance cyber avec un impact direct sur la sécurité des systèmes d'information.

6.1.2. Insuffisance voire inexistence des budgets dédiés à la cybersécurité

Dans bien de situations, le défi majeur est que les budgets alloués à la cybersécurité restent souvent limités, notamment dans les administrations publiques et les grandes entreprises, et inexistante dans la majorité des PME. La sécurité des systèmes d'information est bien plus perçue comme un coût et que comme un investissement stratégique. Considéré ainsi, il devient impossible d'acquérir des solutions de sécurité adaptées, des retards sont observés dans la mise à niveau des infrastructures, les systèmes dépendant finalement des solutions obsolètes ou gratuites non sécurisées, et cela expose fortement ces administrations aux cyberattaques majeures.

6.2. Difficultés opérationnelles

6.2.1. Difficultés des entités à disposer de RSSI compétents et suffisamment outillés

Le marché national souffre d'un déficit de profils qualifiés en cybersécurité, notamment des Responsables de la Sécurité des Systèmes d'Information (RSSI). Lorsqu'ils existent, ces profils cumulent souvent plusieurs fonctions et manquent de formations continues adaptées. Dans ces conditions, les risques suivants se présentent : mauvaise évaluation des risques cyber, absence de stratégie de sécurité cohérente, réactions tardives ou inadaptées en cas d'incident, dépendance excessive à des prestataires externes...

6.2.2. DSI disposant de pouvoirs décisionnels limités

Dans de nombreuses organisations, les Directions des Systèmes d'Information (DSI) ne sont pas pleinement associées aux instances stratégiques de décision. La cybersécurité demeure ainsi appréhendée principalement sous un angle technique, alors qu'elle constitue un enjeu fondamental de gouvernance institutionnelle.

Cette situation peut conduire à la prise de décisions stratégiques sans considération suffisante des risques cyber, à une priorisation insuffisante des investissements nécessaires

en matière de sécurité, ainsi qu'à une définition imprécise des responsabilités en cas d'incident majeur. De tels dysfonctionnements fragilisent durablement le système d'information et accroissent la vulnérabilité globale de l'organisation.

6.3. Difficultés techniques

6.3.1. Sophistication croissante des cybermenaces (IA et automatisation)

Les administrations publiques, entreprises et institutions togolaises font face à une montée en puissance de cyberattaques de plus en plus sophistiquées, intégrant des technologies comme l'intelligence artificielle et l'automatisation. Ces menaces (hameçonnage intelligent, rançongiciels ciblés, deepfakes, attaques par ingénierie sociale avancée) exploitent les failles humaines et techniques, souvent dans des environnements numériques encore en phase de structuration. Les risques sont les suivants :

- Contournement des dispositifs de sécurité classiques (antivirus, pare-feu basiques) ;
- Vol de données sensibles (données personnelles, financières, stratégiques) ;
- Paralysie des services publics et privés critiques ;
- Atteinte à la confiance des citoyens et partenaires dans les services numériques.

6.3.2. Utilisation persistante de logiciels piratés ou non-licenciés

L'utilisation de logiciels piratés demeure une pratique encore répandue, souvent liée à des contraintes budgétaires ou à une insuffisante perception des risques encourus. Cette pratique expose toutefois les organisations à des menaces majeures, notamment l'intégration de logiciels malveillants et de portes dérobées facilitant les intrusions, l'absence de mises à jour et de correctifs de sécurité indispensables, ainsi que des situations de non-conformité juridique pouvant entraîner des sanctions. À terme, elle peut conduire à une compromission grave, voire totale, des systèmes d'information.

6.3.3. Obsolescence des applicatifs et des solutions informatiques

De nombreuses structures continuent de s'appuyer sur des applications obsolètes, parfois développées en interne, qui ne bénéficient plus d'une maintenance régulière ni de mises à jour de sécurité. Cette situation expose les systèmes d'information à l'exploitation de vulnérabilités connues par les cyberattaquants, limite la compatibilité avec les solutions de sécurité modernes et complique leur intégration dans des architectures numériques sécurisées. À moyen et long terme, cette obsolescence entraîne également une augmentation significative des coûts de maintenance corrective et fragilise la résilience globale des organisations.

6.3.4. Insuffisance des infrastructures numériques sécurisées

Certaines organisations disposent d'infrastructures limitées (serveurs non sécurisés, réseaux mal segmentés, absence de redondance), souvent héritées de phases initiales de la transformation numérique. Cette situation entraîne souvent des interruptions prolongées des services numériques, la perte ou l'altération des données critiques, des difficultés à mettre en oeuvre des politiques de sécurité robustes ou encore des vulnérabilités importantes des infrastructures critiques.

Cette situation peut conduire à la prise de décisions stratégiques sans considération suffisante des risques cyber, à une priorisation insuffisante des investissements nécessaires

6.3.5. Non-application régulière des correctifs de sécurité (patch management)

Le déploiement des mises à jour de sécurité transmises par l'ANCy est souvent retardé par manque de procédures clairement définies, manque de compétences, lenteur administrative ou par crainte de perturber les services ou systèmes existants. Il en va de la responsabilité des gestionnaires IT d'éviter l'exploitation des failles connues, les attaques automatisées ou encore la compromission de systèmes pourtant récents.

6.3.6. La sensibilisation et l'adoption des bonnes pratiques

Malgré les efforts continus de l'ANCy, la sensibilisation à la cybersécurité et l'adoption effective des bonnes pratiques restent des défis persistants. Une part significative du public ne perçoit pas pleinement les risques liés aux cyberattaques, les considérant souvent comme des événements lointains ou peu probables. La croissance continue des services en ligne accroît le nombre de personnes à atteindre, tandis que des obstacles tels que les barrières linguistiques et l'accès limité à l'information dans certaines zones reculées compliquent la diffusion des messages de prévention. Cette situation souligne la nécessité de renforcer et de diversifier les stratégies de sensibilisation pour toucher l'ensemble de la population et encourager un comportement numérique responsable.





VII : PERSPECTIVES STRATÉGIQUES 2026

Rapport d'activités 2025



Perspectives stratégiques 2026

La montée en puissance des cybermenaces constitue l'un des principaux défis auxquels le Togo est confronté dans le contexte de sa transformation numérique. Les attaques deviennent de plus en plus sophistiquées, notamment avec l'intégration de technologies avancées telles que l'intelligence artificielle et l'apprentissage automatique, capables de contourner les mécanismes de défense traditionnels. Cette évolution rapide impose une veille permanente et une adaptation continue des dispositifs techniques et des programmes de sensibilisation.

Face à ces défis, les perspectives reposent sur le renforcement progressif de la gouvernance nationale de la cybersécurité, en mettant l'accent sur la montée en compétences des acteurs, la clarification des rôles et responsabilités et le positionnement stratégique de la fonction sécurité au sein des organisations. Le développement de programmes de formation ciblés pour les RSSI, DSI et décideurs constitue un levier essentiel pour améliorer la maturité cyber des institutions publiques et privées.

7.1. Renforcement de la gouvernance nationale de la cybersécurité

L'ANCy va poursuivre l'amélioration de la gouvernance nationale de la cybersécurité en clarifiant les rôles et responsabilités des acteurs publics et privés, y compris le positionnement stratégique de la fonction sécurité des systèmes d'information dans les organisations, afin de s'assurer que la cybersécurité soit intégrée aux décisions opérationnelles et aux projets numériques. Cette approche vise à améliorer la coordination entre l'ANCy et les institutions, à réduire les vulnérabilités liées aux prises de décision fragmentées et à renforcer la résilience globale de l'écosystème numérique national.

7.2. Montée en compétences et formation des acteurs clés

Le développement des compétences des responsables de la sécurité des systèmes d'information (RSSI), des directeurs des systèmes d'information (DSI) et des décideurs constitue un axe majeur pour l'année 2026. Des programmes de formation certifiantes et ciblés sont déployés, mais des ateliers pratiques, des simulations d'incidents et des modules de mise à jour continue seront organisés. L'objectif est de renforcer la maturité cyber des institutions publiques et privées, de professionnaliser la gestion des risques et d'assurer une réponse efficace face aux menaces émergentes.

7.3. Modernisation et sécurisation des infrastructures numériques

L'ANCy s'investira à inciter les institutions à acquérir des infrastructures résilientes et sécurisées. Il s'agira également de promouvoir des solutions logicielles conformes et régulièrement mises à jour. L'autre action sera d'encourager l'intégration de la cybersécurité dès la conception des projets numériques ("security by design"). Ceci permettra de limiter les vulnérabilités et de prévenir les incidents. Les efforts seront également dirigés vers la migration des systèmes obsolètes vers des solutions modernes, la standardisation des architectures, des plans de réponse aux incidents et la maintenance proactive des applications et infrastructures critiques.

7.4. Sensibilisation et culture de cybersécurité

L'ANCy intensifiera ses actions de sensibilisation pour toucher l'ensemble des acteurs, des citoyens aux organisations publiques et privées. Ces campagnes s'appuieront sur une veille continue des menaces et sur la diffusion de bonnes pratiques adaptées à chaque catégorie de public. L'objectif est de renforcer la culture cyber, d'augmenter la vigilance face aux risques et d'assurer que la cybersécurité devienne une responsabilité partagée, condition indispensable pour construire un cyberspace national sûr, résilient et de confiance.

7.5. Adaptation des programmes de sensibilisation

Les programmes de sensibilisation sont parfois ponctuels alors que les modes opératoires des cybercriminels évoluent rapidement. L'absence de mécanismes structurés de veille technologique et de partage d'information limite l'anticipation des nouvelles menaces. L'ANCy va donc adapter ses contenus de sensibilisation en fonction de chaque cible (catégories socioprofessionnelles), intensifier les actions de sensibilisation en se fondant sur une veille continue des menaces. Cela contribuera à renforcer la culture de cybersécurité au sein de la population et des organisations, condition indispensable à la construction d'un cyberspace national sûr, résilient et de confiance.

Conclusion

L'exercice 2025 aura constitué une étape décisive dans la consolidation du dispositif national de cybersécurité, en cohérence avec les orientations stratégiques de modernisation de l'État et de transformation numérique de l'administration togolaise.

À travers la mise en oeuvre méthodique de la Stratégie Nationale de Cybersécurité, l'Agence Nationale de la Cybersécurité a contribué à structurer un cadre de gouvernance plus rigoureux, à renforcer la conformité réglementaire des infrastructures critiques, à professionnaliser l'écosystème des prestataires et à développer un vivier national de compétences certifiantes. Ces résultats traduisent une progression mesurable vers une administration plus sécurisée, plus résiliente et mieux préparée aux risques numériques.

La cybersécurité s'inscrit désormais pleinement dans la dynamique de réforme de l'action publique. Elle constitue un levier transversal de modernisation administrative, en ce qu'elle conditionne la fiabilité des services publics digitalisés, la protection des données des citoyens, la continuité des activités gouvernementales et la crédibilité internationale du pays en matière de gouvernance numérique.

Dans un contexte de digitalisation accélérée des procédures administratives, la sécurisation des systèmes d'information n'est plus une fonction support : elle devient un élément structurant de la performance publique. La qualité du service rendu aux usagers dépend désormais de la capacité des institutions à garantir l'intégrité, la disponibilité et la confidentialité des données. Les avancées de 2025 illustrent une évolution vers une administration orientée vers les résultats, fondée sur la mesure des performances, la gestion des risques et la responsabilisation des acteurs sectoriels. Toutefois, la modernisation de l'État appelle une intensification des efforts : industrialisation des audits de conformité, renforcement du pilotage par indicateurs consolidés, optimisation de l'allocation des ressources et intégration systématique des exigences de cybersécurité dans les projets publics numériques.

L'année 2026 devra ainsi marquer une phase d'approfondissement, avec l'évaluation à mi-parcours de la Stratégie Nationale de Cybersécurité et l'alignement accru des mécanismes de cybersécurité sur les principes de bonne gouvernance, d'efficacité administrative et de performance budgétaire. En consolidant les acquis et en renforçant la culture de la maîtrise des risques numériques, l'Agence Nationale de la Cybersécurité contribue directement à l'ambition d'un État moderne, protecteur, performant et digne de confiance, capable d'accompagner durablement la transformation numérique du Togo au service du développement économique et social.

Remerciements

Nos remerciements vont aux institutions et organisations suivantes :

- Présidence du Conseil de la République Togolaise ;
- Ministère de l'Efficacité du Service Public et de la Transformation Numérique ;
- Ministère des Armées ;
- Ministère de la Sécurité ;
- Ministère de la Justice et de la Législation ;
- Ministère de l'Éducation Nationale ;
- Police nationale ;
- Gendarmerie nationale ;
- Cyber Defense Africa (CDA) SAS ;
- Agence Togo Digital (ATD) ;
- Autorité de Régulation des Communications Électroniques et des Postes (ARCEP) ;
- Union Internationale des Télécommunications (UIT) ;
- GIZ – ProdigiT ;
- Union Européenne ;
- République Fédérale d'Allemagne ;
- LuxDev ;
- Universités de Lomé ;
- Université de Kara ;
- Communauté Économique des États de l'Afrique de l'Ouest (CEDEAO) ;
- Moov Africa Togo ;
- Yas Togo ;
- GVA CanalBox







63 Bd du 13 Janvier,
Nyékonakpoe, Lomé-TOGO, 07 BP 7878
Email : secretariat.ancy@ancy.gouv.tg
Tel 1 : +228 97 52 58 58 - Tel 2 : +228 70 60 60 83

