

RÉPUBLIQUE DU SÉNÉGAL

Un peuple – un but – une foi



PRÉSIDENCE DE LA RÉPUBLIQUE

SECRÉTARIAT GÉNÉRAL

Direction générale du Chiffre et de la Sécurité des

Systèmes d'Information (DCSSI)

FORUM DES PRESTATAIRES DE CYBERSECURITE EDITION 2026



KEYNOTE du

Directeur général de la DCSSI



Mercredi 07 octobre 2026

Hôtel Téranga Dakar

Monsieur le Ministre, Secrétaire général de la Présidence,
Monsieur le Ministre des Télécommunications et du Numérique,
Chers collaborateurs et acteurs de l'écosystème numérique,
Mesdames et Messieurs en vos fonctions, rangs, grades et qualités,
Distingués invités,

C'est un privilège et un honneur de prendre la parole devant vous aujourd'hui. Je tiens à exprimer ma profonde gratitude à tous les acteurs réunis au sein de ce forum des prestataires de cybersécurité. Votre disponibilité active et votre expertise à nos côtés sont de précieux atouts pour mener à bien les chantiers structurants liés à la sécurité de nos réseaux et systèmes d'information et à la protection de nos infrastructures d'information critiques.

À l'ère de la transformation numérique accélérée, le cyberspace est devenu à la fois notre plus grand accélérateur de développement et notre vulnérabilité la plus critique. Face aux menaces croissantes qui pèsent sur notre pays, la Direction Générale de la Sécurité des Systèmes d'Information (DCSSI) joue un rôle de boussole et de bouclier. Pour relever ce défi, notre action s'articule désormais autour d'un triptyque stratégique : un cadre législatif renforcé, un écosystème normatif cohérent, et un plan d'actions opérationnel ambitieux.

Mesdames et Messieurs,

C'est ainsi que le premier pilier de notre stratégie repose sur l'arsenal juridique. Cet arsenal dont les bases ont été posées à travers diverses lois en 2008, s'est enrichi cette année d'un texte dont nous pensons qu'il méritera le qualificatif de « fondateur ». Il s'agit de la loi sur **la Protection des Infrastructures d'Information critiques (IIC) et à la Sécurité numérique**, votée par l'Assemblée nationale le 20 août 2026.

Pour comprendre la portée de cette loi, il faut se rappeler que malgré le socle réglementaire bâti en 2008, autour notamment de la confiance numérique et de la lutte contre la cybercriminalité, des lacunes juridiques nous empêchaient de protéger nos systèmes d'information à hauteur d'attente.

Les conséquences de cette lacune doivent être rappelées :

- D'abord, une application à deux vitesses des règles de sécurité, faute de contraintes globales et fermes.
- Ensuite, un paradoxe juridique intenable : nous voulions protéger nos concitoyens, mais nous n'avions même pas les habilitations légales explicites pour encadrer certains droits fondamentaux face à la menace. Nous étions désarmés face au vide juridique.

C'est précisément ces lacunes que la nouvelle loi s'est donnée pour ambition de refermer. Elle a pour vocation de nous faire passer d'une cybersécurité réactive et corrective à une cybersécurité proactive.

Il faut aussi préciser que cette loi s'inscrit dans le cadre stratégique définie par l'Etat et précisément, avec l'Agenda national de transformation *Sénégal 2050*, dont le premier axe dédié à la souveraineté numérique, et l'objectif stratégique 4, consacré à la « *confiance numérique et à la résilience* ».

Cet objectif stratégique de l'Agenda national de transformation, érige la cybersécurité en pilier de la sécurité nationale et considère comme prioritaire « la surveillance des Infrastructures d'Information Critiques (IIC), en modernisant les dispositifs de protection (PKI, CERT national, programmes d'audits) et en s'adaptant aux menaces protéiformes. »

Au point de vue de la démarche la loi sur la Protection des IIC et la Sécurité numérique instaure un double régime de régulation : des règles de base pour les systèmes ordinaires, avec une supervision rapprochée

et ultra-contraignante pour les infrastructures d'information critiques (IIC), considérées comme des actifs stratégiques vitaux.

Enfin, dans une perspective d'autonomie stratégique, cette loi favorise l'émergence de « champions nationaux » en confiant les prestations de services de cybersécurité à des prestataires agréés, structurant ainsi une économie de confiance autour des acteurs privés locaux.

Cette architecture globale est enfin sous tendue par un régime de sanctions administratives et pénales destiné à garantir l'effectivité des exigences de sécurité.

Mesdames et Messieurs,

Au-delà de ce texte fondateur et des exigences qu'il impose à nos systèmes et réseaux, la sécurité numérique ne saurait se décréter par un simple effet de manche ; elle s'impose par une exigence de chaque instant; **elle s'organise méthodiquement à travers un cadre fait de normes à la lisière du droit et de la pratique informatique dont le respect au quotidien doit faire partie de notre culture numérique.**

Dans cette perspective, l'encadrement des activités d'audit des systèmes d'information a été entamé sur la base du référentiel d'accréditation PASI.

Dans la foulée, une série de référentiels, politiques et autres normes de sécurité, sera proposée par la DCSSI mais toujours avec la même approche inclusive.

C'est dans cet esprit que le référentiel de fourniture de services de prestation et de détection d'incidents dit PGIS vous a été transmis pour recueillir vos avis.

A cet égard, notre action quotidienne de conception de référentiels de sécurité rigoureux, de normes éprouvées et de recommandations, vise à uniformiser les pratiques, renforcer les compétences professionnelles et

ancrer durablement la culture de la cybersécurité sur l'ensemble du territoire.

Par conséquent, ce corpus normatif ne constitue pas une contrainte coûteuse en temps et en moyens financiers. Bien au contraire : il structure un écosystème de confiance en encadrant formellement les prestataires de services de cybersécurité, les auditeurs qualifiés et les solutions technologiques mises sur le marché. Il garantit ainsi aux organisations publiques et privées de s'appuyer sur des partenaires irréprochables et fiables.

En outre, en s'imbriquant harmonieusement avec la protection des données à caractère personnel, ce dispositif façonne un environnement juridique protecteur et prévisible, indispensable pour stimuler l'innovation et garantir la pérennité de notre économie.

Mesdames et Messieurs,

Avoir des lois et des normes est une nécessité absolue, mais les faire vivre sur le terrain constitue notre véritable combat à travers le **Plan d'Action Stratégique 2026 – 2030 de la DCSSI**.

Face à la complexité croissante des menaces cybernétiques et à une hyperconnectivité qui expose dangereusement nos fondements économiques et nos institutions politiques, l'application d'une feuille de route rigoureuse et unifiée s'impose comme une urgence nationale.

C'est ce qui est à l'origine du plan d'action de la DCSSI dont je voudrais vous dire quelques mots. Ce plan traduit une volonté politique implacable : ériger la cybersécurité en un bouclier souverain garantissant la stabilité du Sénégal.

Cette vision repose sur une double dynamique fondatrice. D'une part, elle répond à l'impératif de moderniser et de professionnaliser la gouvernance de la sécurité numérique ; d'autre part, elle s'arrime parfaitement au *New*

Deal Technologique tout en capitalisant sur l'évaluation de la stratégie 2020-2022.

Concrètement, ce plan s'articule autour d'axes stratégiques :

- **Axe 1 : Gouvernance et cadre institutionnel ;**
- **Axe 2 : Protection des infrastructures critiques et réponse aux incidents ;**
- **Axe 3 : Capacité humaine et expertise nationale ;**
- **Axe 4 : Innovation, souveraineté technologique et souveraineté numérique ;**
- **Axe 5 : Coopération et leadership international.**

L'Axe 1, ambitionne de consolider notre souveraineté numérique à travers quatre leviers majeurs. Il s'articule d'abord autour du renforcement de l'opérationnalité de la DCSSI et de la réforme de son organigramme, pour disposer d'une gouvernance agile face aux menaces. Sur le plan normatif, il prévoit la mise en œuvre de la loi sur la protection des infrastructures d'information critiques (IIC) et de la sécurité numérique, ainsi que de ses décrets d'application, complétée par la révision de la loi sur la cryptologie afin d'intégrer la cryptographie post-quantique et la PKI nationale pour sécuriser les plateformes digitales de l'Administration. Enfin, cet engagement se traduit concrètement sur le terrain par le déploiement d'un guichet national cyber, conçu comme un point d'entrée unique pour le dépôt des plaintes et des alertes, l'accompagnement des usagers et des acteurs publics, la communication entre la DCSSI et ses partenaires, ainsi que la centralisation des démarches administratives liées à la cybersécurité et à la cryptologie. Il offre en outre un cadre sécurisé pour la gestion des demandes, des vulnérabilités, des incidents et cyberattaques, ainsi que des homologations techniques. La présentation de ce guichet sera d'ailleurs réalisée tout à l'heure au cours des travaux.

L’Axe 2 du plan d’action vise à sanctuariser la résilience opérationnelle des secteurs vitaux en durcissant les exigences de sécurité et de contrôle. Il se traduit par la réalisation d’audits obligatoires des systèmes critiques publics comme privés, par la classification et l’audit approfondi des Infrastructures d’Information critiques (IIC), ainsi que par la mise en œuvre de normes et politiques sectorielles de cybersécurité adaptées (politique de sécurité et référentiel de cybersécurité des IIC, référentiel de classification des actifs, règles et référentiel technique d’externalisation des systèmes d’information des IIC etc .

Afin de garantir la fiabilité de ces écosystèmes, l’homologation des Systèmes d’Information (SI) sensibles devient obligatoire, tandis que la supervision active et proactive des réseaux critiques (énergie, finances, défense, santé, transport, télécom) est fortement renforcée. Enfin, cette architecture de défense intégrée s’appuie sur le déploiement d’un CSIRT/SOC national interconnecté avec les Opérateurs d’Infrastructure d’Information critique (OIIC), et sur l’élaboration d’un plan national de réponse aux crises cyber pour garantir une capacité de réaction immédiate et coordonnée face aux menaces majeures.

Quant à l’Axe 3, il structure le développement du capital humain et l’excellence nationale à travers le lancement du programme SENCYBERJOB et la montée en puissance du Centre de formation Cryptologique et à la Sécurité des Systèmes d’information (CFC-SSI). Il ambitionne de faire de l’ENC-VR un Centre d’excellence africain de référence en cybersécurité, tout en professionnalisant l’écosystème par un cadre de certification nationale des experts SSI et la création d’une base de données dédiée aux compétences en technologies émergentes. Enfin, cette dynamique s’accompagne d’une forte impulsion culturelle et partenariale matérialisée par l’organisation d’une campagne annuelle de sensibilisation dans toutes les parties du pays, d’une semaine annuelle de la cybersécurité et de la cryptologie.

Pour ce qui est de l'Axe 4, il stimule l'innovation souveraine et l'indépendance technologique du pays à travers deux leviers majeurs. D'une part, dans le contexte du New Deal technologique, il prévoit le lancement d'un Fonds souverain cyber destiné à financer des start-ups et des projets de R&D les plus prometteurs dans le domaine de la Cybersécurité. D'autre part, il structure la recherche de pointe avec la création du Centre d'Expertise, d'Innovation et de Recherche en Cybersécurité et Technologies émergentes (InovSec). Ce dernier aura pour missions de développer une cryptographie et une intelligence artificielle souveraines, d'évaluer l'intégration d'une blockchain souveraine pour les systèmes critiques, et de soutenir la recherche appliquée sur les algorithmes de chiffrement post-quantique.

Et enfin l'Axe 5, positionne notre pays comme un acteur clé de la diplomatie et de la coopération numérique régionale et internationale. Il se concrétise par la création d'un observatoire cyber sous-régional basé à Dakar et par le développement d'accords bilatéraux de partage d'informations avec les CERT régionaux.

Afin de renforcer l'influence nationale et d'harmoniser les standards de sécurité, il s'appuie également sur une adhésion active aux structures normatives et aux forums multilatéraux (OIF, UA, ONU, ITU).

Enfin, cette dynamique de coopération s'incarne durablement par l'organisation, tous les deux ans à Dakar, d'un Sommet africain de la cybersécurité, pensé comme le rendez-vous de référence sur le continent.

Mesdames et Messieurs,

Pour conclure, oublions l'idée d'une simple contrainte technique : la cybersécurité est le véritable garant de notre avenir et de notre souveraineté. Ce combat est le nôtre. Il ne sera gagné qu'à travers une synergie indéfectible unissant le régulateur, les exploitants d'Infrastructures d'Information Critiques (IIC), les prestataires de

cybersécurité, le monde économique et les forces vives de la nation, pour façonner ensemble un cyberspace sénégalais fort, résilient et souverain.

Je vous remercie de votre aimable attention.