L'ECONOMISTE

Le Cercle des Experts

# Synergie entre les stratégies Cybersécurité et Maroc Digital 2030

Par Taïeb DEBBAGH - Hicham FAIK - - | Edition N°:6872 Le 23/10/2024

| | |
|---|---|
|  |  |
| Taieb Debbagh est expert en cybersécurité et protection des données personnelles. Ancien secrétaire général du département ministériel en charge du Digital, il a contribué à l'élaboration de la stratégie Maroc Numeric 2013. Il a été président de la commission «Structures organisationnelles» de la Global Cybersecurity Agenda (UIT-Genève). Il est également auteur du livre «15 ans de cybersécurité au Maroc» et co-auteur de «Système de management de la Cybersécurité nationale» (Amazon en avril 2024) | Hicham Faik est un expert international en cybersécurité et confiance numérique reconnu avec plus de 25 ans d'expérience. Certifié CISSP, CISM, ISO27001/27005… Hicham Faik a occupé des postes stratégiques dans les secteurs de l'énergie, l'assurance et la banque. Il a mis en œuvre la stratégie globale de cybersécurité d'un grand groupe bancaire de 2017 à 2022. En 2023, il fonde CybrForge, entreprise spécialisée en cybersécurité |

À l'ère du numérique, la cybersécurité est devenue une composante essentielle pour garantir la pérennité et la prospérité de toute nation. Alors que le Maroc s'engage résolument vers une transformation digitale ambitieuse avec le lancement de Maroc Digital 2030, une stratégie de cybersécurité robuste s'impose pour accompagner cette transition. La Stratégie nationale de cybersécurité 2030 répond à cet impératif en mettant en place un cadre structuré visant à protéger les infrastructures critiques, les citoyens, ainsi que les entreprises marocaines des cybermenaces de plus en plus sophistiquées. Cette tribune propose une analyse de la stratégie cybersécurité, les points d'ancrage avec Maroc Digital 2030, ainsi que des propositions pour renforcer la synergie entre ces deux initiatives nationales.

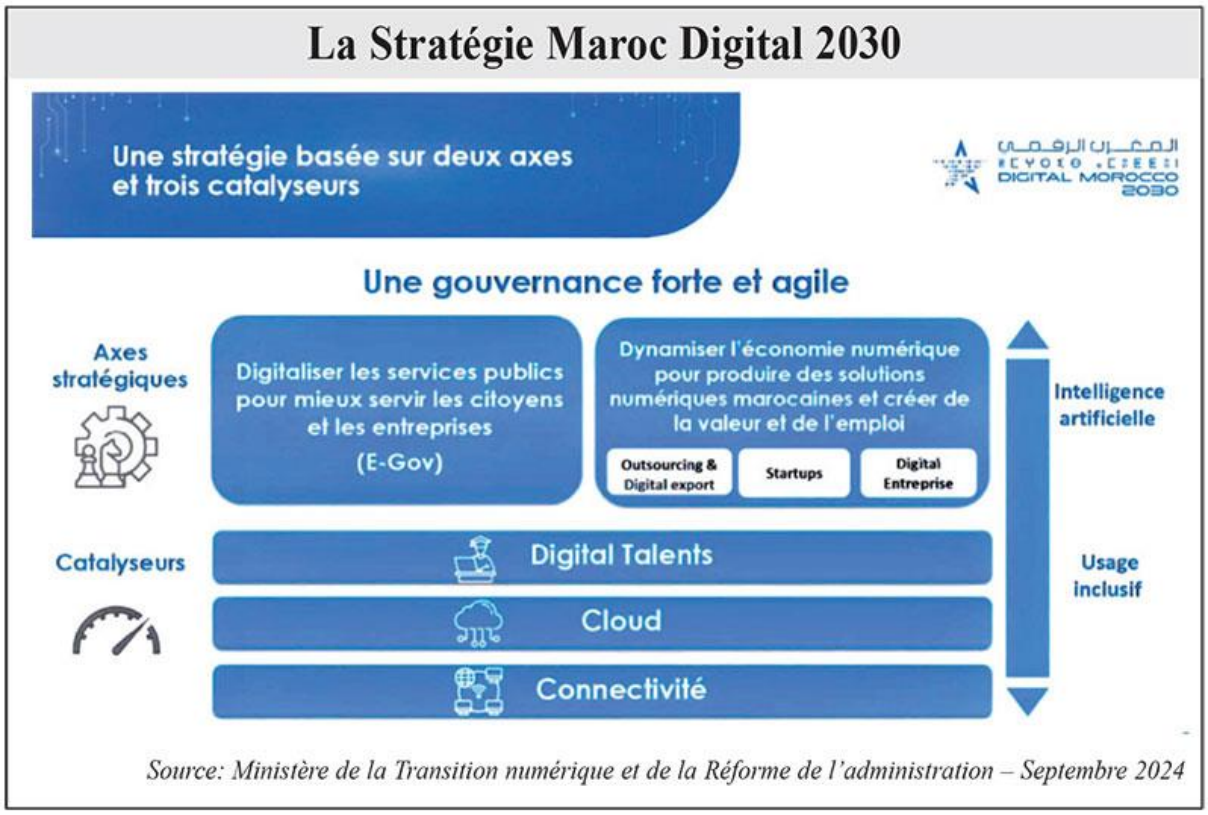
## Stratégie nationale de cybersécurité 2030

La Stratégie nationale de cybersécurité 2030 (SNC 2030) se distingue par sa vision globale et proactive, visant à garantir un cyberespace sûr et résilient pour accompagner la transformation digitale et promouvoir la prospérité économique. Structurée autour de quatre grands piliers, elle adopte une approche holistique pour traiter efficacement les menaces.

Le premier pilier met l'accent sur la **gouvernance** en cybersécurité, avec un cadre juridique agile, adapté aux environnements numériques émergents comme le Cloud. Il prévoit la révision régulière des

lois pour anticiper les cybermenaces et privilégie la coordination intersectorielle, facilitant le partage d'informations en temps réel entre le secteur public, privé, et les entités gouvernementales pour une gestion intégrée des risques.

Le deuxième pilier se concentre sur la **sécurité proactive** et la résilience du cyberespace. Il renforce la détection en temps réel et la gestion rapide des incidents tout en consolidant les défenses pour prévenir les cyberattaques. Ce pilier met l'accent sur l'adoption de normes strictes de cybersécurité au sein des entreprises et infrastructures critiques pour assurer la confiance numérique des utilisateurs et une cartographie précise des infrastructures vitales.




Le troisième pilier porte sur le **développement des compétence**s et la **sensibilisation**. Il promeut la formation d'un vivier de professionnels qualifiés en cybersécurité, tout en encourageant la collaboration entre les secteurs public, privé, et académique pour stimuler l'innovation et créer un écosystème national solide. La stratégie inclut également des programmes spécifiques sur la sécurité du Cloud pour renforcer la protection des systèmes dématérialisés.

Le quatrième pilier traite de la **coopération internationale**, avec une approche proactive de collaboration avec les organismes internationaux et régionaux. Le Maroc cherche à renforcer ses partenariats pour l'échange d'informations critiques en temps réel, l'accès à des expertises spécialisées, et la mutualisation des bonnes pratiques afin de mieux se protéger contre les cyberattaques mondiales.

En somme, cette stratégie ambitieuse propose une **cybersécurité intégrée et anticipative**, avec une forte implication des acteurs nationaux et internationaux. Elle s'appuie sur des actions complémentaires et des objectifs clairs pour soutenir la transformation digitale du Maroc, en lien direct avec la Stratégie Maroc Digital 2030.

**Points d'ancrage entre les deux stratégies**

Maroc Digital 2030 ambitionne de faire du **Maroc un hub numérique régional** en accélérant la transformation digitale dans les secteurs publics et privés. Cette vision repose sur la démocratisation des services numériques, le développement des compétences et l'innovation technologique, tandis que la Stratégie de Cybersécurité 2030 fournit un socle de protection essentiel pour soutenir cette transformation.

Le premier point d'ancrage réside dans la **protection des infrastructures critique**s. Maroc Digital 2030 promeut l'adoption des technologies numériques dans des secteurs essentiels tels que l'énergie, la finance, et la santé. En parallèle, la stratégie de cybersécurité met en place des mécanismes techniques et légaux pour sécuriser ces infrastructures, garantissant leur résilience et renforçant la confiance numérique des utilisateurs, un facteur clé pour l'adoption des services numériques.

Ensuite, la **sécurité des environnements Cloud** est un levier stratégique pour la souveraineté numérique. La Stratégie de Cybersécurité 2030 crée un cadre juridique pour protéger les données sensibles stockées sur le territoire national, conformément aux meilleures pratiques de sécurité, contribuant à la résilience des infrastructures.

Un autre point d'ancrage est le **développement des compétences**. Les deux stratégies accordent une importance à la formation des talents numériques. Tandis que Maroc Digital 2030 forme des experts numériques, la Stratégie de Cybersécurité se concentre sur la spécialisation en cybersécurité, incluant des programmes spécifiques pour l'IA et le Cloud Computing, réduisant ainsi le déficit de compétences dans la cybersécurité.

Enfin, **l'innovation** est un point central. Maroc Digital 2030 promeut un écosystème entrepreneurial pour favoriser les startups technologiques. La stratégie de cybersécurité soutient cette démarche via des clusters dédiés, des programmes R&D, et des fonds pour développer des solutions de sécurité. Cette complémentarité permet de positionner le Maroc comme un leader régional en numérique et cybersécurité.

Ces points d'ancrage montrent que la Stratégie de Cybersécurité et Maroc Digital 2030 se renforcent mutuellement, en garantissant un cadre sécurisé et innovant pour le développement d'un écosystème numérique dynamique et résilient au Maroc.

**Conclusion**

Bien que les Stratégies Cybersécurité nationale et Maroc Digital 2030 soient bien alignées, certaines **propositions** (voir encadré) peuvent renforcer cette synergie, qui assurera une protection robuste des infrastructures numériques, un développement harmonieux des compétences et un encouragement à l'innovation qui constituera une prémice de l'émergence d'une «Industrie de la cybersécurité» au Maroc. La nouvelle Stratégie Cybersécurité nationale offre un cadre sécuritaire propice à la transformation digitale du pays. Cependant, pour renforcer l'impact de cette stratégie, il est nécessaire de multiplier les efforts en matière de sensibilisation, de renforcer la coopération nationale, et d'assurer que les secteurs critiques soient dotés de moyens adéquats de protection et de résilience pour faire face aux défis du cyberespace.


| Les 7 propositions pour renforcer la synergie entre les deux stratégies |
|---|
| ■ **Sensibilisation des TPME:** Les TPME, vulnérables aux cyberattaques en raison de ressources limitées, nécessitent des campagnes de sensibilisation ciblées et des solutions de sécurité à faible coût. Des incitations fiscales pourraient encourager ces entreprises à investir dans des protections de base. |
| ■ **Création de CIRT sectoriels:** Des CIRT sectoriels (banque, industrie, universités…) peuvent être mis en place pour surveiller et répondre aux incidents spécifiques à chaque secteur. Ces CIRT assureraient la coordination avec maCERT, renforçant ainsi la résilience des secteurs critiques. |

■ **Renforcement de la cybersécurité en milieu industriel:** Il est essentiel de développer un programme dédié à la sécurisation des infrastructures industrielles critiques (OT/ICS), incluant des audits réguliers, des formations spécialisées, et l'adoption de standards de sécurité adaptés.

■ **Coopération nationale renforcée:** La cohésion nationale pourrait être améliorée par des plateformes de partage d'informations et des exercices de simulation d'incidents, facilitant la réponse aux cyberattaques à l'échelle nationale.

■ **Sensibilisation des citoyens:** Avec l'essor des services publics numériques, des campagnes de cyber-hygiène intégrées aux programmes éducatifs sont essentielles pour que les citoyens soient mieux informés des risques en ligne.

■ **Intégration de la cybersécurité dans l'innovation:** La cybersécurité devrait être au cœur des projets technologiques (IA, IoT, Blockchain), avec des exigences réglementaires imposant des évaluations de risques dès la conception pour garantir une sécurité intégrée (Security by Design).

■ **Soutien aux startups numériques:** Des programmes dédiés à la cybersécurité pour les startups, incluant des subventions sont nécessaires pour assurer la résilience de ces jeunes entreprises innovantes, qui seront la base d'une «Industrie de la cybersécurité».

*Source: les auteurs*