**République tunisienne**

**Présidence de la République**

**Conseil de sécurité nationale**

# Stratégie nationale en matière de cybersécurité 2020-2025

## Table des matières

# Préambule

Le monde connaît actuellement une croissance rapide et intense de l'utilisation des technologies de l'information et des communications dans tous les domaines et par l'ensemble des communautés, notamment les secteurs public et privé et les individus, dans la majeure partie de leurs activités quotidiennes.

Alors que ces technologies offrent un environnement numérique interconnecté, souple et à croissance rapide qui assure le bien-être de l'individu, celles-ci ne sont pas exemptes de risques pour le cyberespace, s'ajoutant aux menaces internes et externes à l'égard des droits, des libertés et de la sécurité nationale.

Ce développement technologique a produit des concepts nouveaux et en constante évolution, notamment le cloud computing, l'Internet des objets, les télécommunications de cinquième génération, les médias sociaux, l'intelligence artificielle, les cryptomonnaies et les blockchains, de même que l'utilisation intensive et généralisée de l'Internet par les individus, la société et l'Etat, dans des domaines essentiels. Ceci s'est traduit par une incidence plus élevée d'une variété de cyber-risques, menaces et attaques en provenance de diverses sources, en raison de l'ouverture du pays à l'échelle régionale et internationale.

Par conséquent, suite aux délibérations du Conseil de sécurité nationale du 5 juillet 2018, un groupe de travail appartenant au Comité de Sécurité de l'information et des communications du Conseil a été mis en place, sous l'autorité du Conseiller principal pour la sécurité nationale, en vue de rédiger la Stratégie nationale de cybersécurité. Cette stratégie vise à protéger et développer le cyberespace national en renforçant les capacités nationales, en assurant la fiabilité numérique en interaction avec les stratégies sectorielles et du secteur privé et en mettant en œuvre les plans pertinents en coordination avec l'ensemble des parties prenantes, en veillant tout particulièrement aux droits et libertés, conformément aux exigences et dispositions de la Constitution, de même qu'aux conventions et traités internationaux.

Cette stratégie couvre cinq domaines : les orientations et les stratégies sectorielles ; le cadre juridique et règlementaire ; l'éducation, la formation et les compétences ; la culture et la cyber-société ; et les normes et les technologies.

## La vision

L'Etat doit être en mesure de prévenir les cybermenaces et d'y résister en s'appuyant sur les compétences nationales, de maîtriser et gérer le cyberespace national, de consolider la fiabilité numérique, de renforcer la coopération internationale et d'occuper une position de leader dans le domaine numérique.

## La portée de la Stratégie

Cette stratégie couvre le cyberespace national, qui comprend l'ensemble des services d'information, données, réseaux, plateformes et systèmes. Elle implique également toutes les parties prenantes, notamment les citoyens, les institutions, les associations, les sociétés publiques et privées, la société civile et les milieux académiques.

## Les objectifs de la Stratégie

Cette stratégie vise à :

1. **Maîtriser et gérer le cyberespace national** en déterminant les parties chargées de la consolidation du travail de collaboration avec l'ensemble des parties prenantes et en apportant son appui à la coordination entre elles ;
2. **Prévenir et résister aux cyberattaques** par le biais du renforcement des capacités nationales, en consolidant la sensibilisation et en protégeant les infrastructures numériques critiques (INC) ;
3. **Consolider la fiabilité numérique** en créant les mécanismes et procédures nécessaires ;

4. **Atteindre le leadership dans le domaine numérique** grâce au développement d'un environnement numérique sécurisé et en occupant une position de chef de file à l'échelle régionale et internationale ;
5. **Garantir la coopération internationale** en adoptant une approche équilibrée entre la coopération internationale et la garantie de l'intérêt supérieur de l'Etat.

## Les domaines de la Stratégie

La stratégie nationale du cyberespace a été élaborée de manière concertée, avec la participation de toutes les parties prenantes, en tenant compte des résultats des analyses des risques d'utilisation et des menaces du cyberespace national, de même que des références internationales pertinentes.

Cette stratégie définit un ensemble d'orientations relatives à tous les domaines de l'économie et de la société et, une fois mise en œuvre, permet d'assurer la flexibilité et la résilience des services et des infrastructures numériques critiques (INC) à l'échelle nationale, dans le souci de consolider la fiabilité numérique.

Cette stratégie vise également à améliorer le système juridique du cyber-domaine et à déterminer les mécanismes de coopération sectoriels, locaux et internationaux pour la gestion du cyber-risque et assurer des compétences nationales.

Cette stratégie s'appuie sur les domaines suivants :

### 1. Les orientations et stratégies sectorielles

Les principales parties prenantes s'engagent à consolider la sécurité du cyberespace national et à protéger les infrastructures numériques critiques contre les risques et menaces qui pourraient affecter la sûreté nationale, par le biais de l'élaboration de procédures et de mécanismes permettant de traiter des cyber-incidents et de gérer les crises relatives à ce domaine.

**2. Le cadre juridique et règlementaire**

Il convient d'élaborer des textes juridiques et de les aligner sur les développements du domaine numérique, notamment en termes de :

- Liberté d'expression sur l'Internet,
- Protection des données privées et personnelles,
- Protection de l'enfant sur l'Internet,
- Protection du consommateur "numérique",
- Protection de la propriété intellectuelle et industrielle et des brevets sur l'Internet,
- Protection des transactions financières sur l'Internet,
- Lutte contre la cybercriminalité.

**3. L'éducation, la formation et les compétences**

Pour ce faire, il conviendrait de :

- Sensibiliser les individus aux cyber-risques et à la façon de les traiter,
- Elaborer une formation universitaire dans le domaine numérique en s'appuyant sur des formateurs spécialisés en partenariat avec le secteur industriel,
- Développer les compétences spécialisées dans le domaine de la cybersécurité.

**4. La culture et la cyber-societé**

Il convient d'établir une culture de la cybersécurité en sensibilisant les individus à faire preuve de prudence en ce qui concerne les services électroniques sur l'Internet et les médias sociaux, et chercher à protéger leurs données professionnelles et personnelles.

**5. Les normes, les technologies et la recherche universitaire**

Il convient de bien se préparer et de prévenir les risques et menaces potentiels en s'appuyant sur les normes internationales dans ce domaine et en encourageant les diverses parties prenantes à renforcer les capacités et les solutions requises.

## Les priorités de la mise en œuvre de ces domaines

La mise en œuvre des domaines de cette stratégie serait la suivante :

1. **Au plan règlementaire**
    - Améliorer continuellement le cadre juridique relatif à la cybersécurité ;
    - Ratifier les conventions et traités internationaux pertinents ;
    - Etablir une bonne gouvernance de la sécurité numérique, de la gestion de crise et de la coordination entre les parties prenantes ;
    - Etre déterminé à mettre en œuvre les politiques, règles et procédures relatives à la cybersécurité.

2. **Au plan humain**
    - Sensibiliser les utilisateurs et les autorités aux risques d'utilisation des nouvelles technologies et de l'Internet,
    - Apporter les compétences spécialisées et les conserver,
    - Sensibiliser les autorités à l'importance de leur rôle dans la bonne gestion du domaine numérique,
    - Développer les compétences nationales dans la recherche universitaire et encourager les différentes parties prenantes à développer les compétences et les solutions nationales dans ce domaine.

3. **Au plan opérationnel**
    - Chercher à établir des règles de bonne gouvernance des données,
    - Inclure la cybersécurité dans les priorités nationales,
    - Appuyer la formation et les mécanismes de financement dédiés à l'installation des systèmes numériques nationaux et leur exploitation,
    - Consolider les capacités de cyberdéfense,
    - Créer des mécanismes de coordination numérique opérationnels à l'échelle nationale et déterminer les domaines de spécialisation et d'intervention afin de traiter des cyber-incidents.

4. **Les facteurs contextuels**

- Mettre en place les mécanismes requis afin de maîtriser et gérer le cyberespace national,
- Prendre les mesures nécessaires afin de conforter la confiance dans le cyberespace et les services numériques,
- Créer des infrastructures et des services numériques qui répondent aux exigences de sécurité conformément aux normes internationales dans ce domaine,
- Garantir la stabilité nationale aux plans social, économique et politique,
- Consolider la confiance dans le cyberespace.

## Suivi et évaluation

Dans le cadre de la garantie de la souveraineté nationale et de la confiance dans le cyberespace national, l'Etat tunisien s'efforce de prendre les mesures et les procédures requises en vue de mettre en œuvre cette stratégie et de produire les plans détaillés qui comprennent les mesures nécessaires parallèlement à la consolidation de la coopération internationale dans ce domaine.

Cette stratégie est établie pour six ans et est actualisée en fonction de l'évolution de la situation.

Le Comité de Communication et d'information du Conseil de sécurité nationale s'engage à contrôler et à surveiller la mise en œuvre de cette stratégie et à recommander ses mises à jour au Conseil.

# Glossaire

| | Termes | Définition |
|---|---|---|
| 1 | Données | Toute représentation de données ou concepts sous une forme qui soit lisible par tous les moyens. |
| 2 | Services numériques | Tout service fourni à un individu ou un organisme utilisant l'une des composantes ou plus du cyberespace. |
| 3 | Disponibilité | La caractéristique de continuité et de pérennité du service et/ou des données. |
| 4 | Menace | La probabilité d'un événement qui pourrait affecter la disponibilité du service fourni ou la sécurité, la confidentialité et la disponibilité des données dans le cyberespace. |
| 5 | Vulnérabilité | Une faiblesse ou un dysfonctionnement d'une composante du cyberespace qui pourrait être exploitée par quiconque en vue de menacer la sécurité du cyberespace ou de l'enfreindre. |
| 6 | Risque | L'impact de l'exploitation d'une menace sur les vulnérabilités existantes en raison des procédures de sécurité disponibles. |
| 7 | Infrastructures numériques critiques (INC) | Les systèmes d'information qui détiennent des biens et des services sensibles à l'échelle nationale et qui ont un impact sur la sécurité de la sûreté nationale dans le cas où ceux-ci seraient bloqués ou enfreints. |
| 8 | Protection des INC | Offrir les moyens organisationnels et techniques et les procédures permettant de garantir la pérennité des services et la confidentialité, la sécurité et la disponibilité des données sensibles. |
| 9 | Cyberespace | Le cyberespace est un espace numérique qui relie les systèmes de traitement de données électroniques aux réseaux d'information et de communication et comprend les ordinateurs, les réseaux, les plateformes, le contenu, de même que les opérations effectuées au moyen de ces réseaux. |
| 10 | Cybersécurité | La cybersécurité signifie l'apport des ressources requises à la protection du cyberespace contre les menaces qui pourraient affecter la confidentialité, la sécurité et la disponibilité des données et des services. |
| 11 | Cyber-défense | L'ensemble des moyens et procédures organisationnels, techniques et dissuasifs qui permettent la protection /l'atténuation des attaques des INC et leur traitement rapide. |
| 12 | Cyber-criminalité | Il s'agit de "toute infraction relative aux technologies de l'information et de la communication". |
| 13 | Cyber-incident | Un incident imprévu qui provoque des dommages à l'une des composantes ou plus du cyberespace. |
| 14 | Evénement | La découverte d'une activité "anormale" sur le réseau ou le système de traitement (tous les événements ne sont pas préjudiciables). |

## Références

*Code de communication* / *Projet de Code numérique*
Norme ISO 27000
*Guide de la cybersécurité pour les pays en développement*, ITU 2006

*Fichiers pays* : France, Grande Bretagne, Canada, USA, République tchèque, Lituanie.
*Convention sur la cybercriminalité*, Budapest (STE No. 185)
Loi No. 22 de 2016 relative au *Droit d'accès à l'information*
Conclusions de *l'Etude sur l'établissement d'une référence nationale pour classifier les données publiques*