

# Stratégie Nationale de Cybersécurité

**Jean-Paul APATA**

S/D Prospective et Numérotation à  
ATCI

[apata@atci.ci](mailto:apata@atci.ci)

**Abidjan, le 08 juillet 2010**

# Cybersécurité

- Introduction

- Le développement des TIC (la révolution informationnelle) a créé un nouvelle espace, l'Espace numérique ou Cyberespace dans lequel le « bien » est immatériel : l'information ou la donnée numérique
- Espace de base de la société de l'information et de l'économie numérique dont la maîtrise est gage du développement socio-économique des Etats
- Espace de souveraineté des Etats qui doit être sécurisé et défendu au même titre que les espaces terrestre, aérien et maritime

=> Les Etats prennent des mesures pour assurer la sécurité du Cyberespace à travers la Cybersécurité afin d'assurer leur développement durable

# Cybersécurité

- Généralités

- Projet de société dans la mesure où tout le monde est concerné par sa réalisation
- Projet d'ordre économique, politique, humain touchant à la sécurité du patrimoine numérique et culturel des individus, des organisations et des nations
- Enjeux complexes dont la satisfaction passe par une volonté politique de définir et de réaliser une stratégie de développement des infrastructures et services TIC (e-services) qui intègre une stratégie de cybersécurité cohérente, efficace et contrôlable

# Cybersécurité

- **Objet**
  - Contribuer à préserver les forces et les moyens organisationnels, humains, financiers, technologiques et informationnels dont se sont dotées les Institutions, les Etats, pour réaliser leurs objectifs
- **Enjeux**
  - Apporter une réponse adéquate aux dimensions humaine, juridique, économique, sociale et technologique des besoins de sécurité des infrastructures et des populations
  - Apporter une réponse au besoin de maîtrise du patrimoine numérique, de la distribution de biens intangibles / immatériels, du commerce électronique, etc.
  - Instaurer la confiance en l'économie numérique afin de favoriser un développement socio-économique profitable à tous les acteurs de la société

# Cybersécurité

- Finalité
  - Garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'organisation ou de l'Etat. Cela consiste à :
    - diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits
    - permettre le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre
- Parties prenantes
  - le Gouvernement
  - le secteur public et le secteur privé
  - le public

# Cybersécurité

- Démarche

- « Diriger » et maîtriser la sécurité:
  - Garantir l'efficacité des mesures de sécurité dans le temps et dans l'espace
  - Identifier les acteurs et les responsabilités
- Définir une politique de sécurité qui stipule ses exigences de sécurité envers tous les acteurs (Gouvernement, utilisateurs, prestataires de services, etc.)
- Elaborer et mettre en œuvre une stratégie de cybersécurité cohérente, efficace et contrôlable
- Développer une cyber-éthique d'utilisation et de comportement vis-à-vis des TIC

# Cybersécurité

- Démarche
  - Déployer des solutions
    - Adapter le cadre légal et institutionnel
    - Eduquer, former, sensibiliser l'ensemble des acteurs à la cybersécurité
    - Mettre en place des centres d'alerte et de gestion de crise au niveau national
    - Imposer des surveillances, des contrôles (par analogie aux contrôles mis en place sur les réseaux routiers) par des évaluations régulières de vulnérabilités et menaces et faire une analyse stratégique et tactique des cyber-attaques

# Cybersécurité

- Démarche

- Développer les compétences d'une cellule de cyberpolice pouvant contribuer à une coopération internationale en matière de poursuite et d'investigation du cybercrime
- développer des solutions technologiques de gestion des identités, du contrôle d'accès, des mécanismes de cryptographie, etc.

=> Elaboration et mise en œuvre d'une stratégie nationale de cybersécurité, y compris les plans d'actions avec une attention particulière sur les infrastructures critiques nationales

# Cybersécurité / La Stratégie

- 5 piliers d'une stratégie de cybersécurité
  - Cadre légal
    - Loi sur la cybercriminalité
    - Loi sur la sécurité des réseaux et systèmes informatiques
    - Loi sur la protection des données à caractère personnel
  - Cadre organisationnel
    - Désignation d'un responsable national chargé de la cybersécurité
    - Création d'une agence spécialisée chargée de la sécurité informatique
    - Mise en place d'un CERT national et des CERT sectoriels

# Cybersécurité / La Stratégie

- 5 piliers d'une stratégie de cybersécurité
  - Renforcement des capacités
    - Développer une expertise nationale en matière de sécurité des réseaux et systèmes informatiques
    - Former des instances de justice et de police dans le domaine des TIC et des investigations en matière de cybercriminalité
  - Sensibilisation et éducation
    - Sensibiliser à une cyberéthique d'utilisation et de comportement vis-à-vis des TIC
  - Coopération nationale et internationale
    - Collaboration entre le Gouvernement, le secteur privé
    - Coopération internationale (alertes, investigations, etc.)
    - Mise en place de point de contact 24/7

# Cybersécurité : Cas des USA

- Désignation d'un responsable de la cybersécurité en la personne de Howard Schmidt, un ancien de Microsoft
- Stratégie américaine (5 axes)
  - Axe 1 : Système de réponse aux incidents de sécurité du cyberespace
  - Axe 2 : Programme de réduction de la vulnérabilité et la menace du cyberespace national
  - Axe 3 : Programme de sensibilisation et de formation à la sécurisation du cyberespace
  - Axe 4: Sécurisation du cyberespace du gouvernement
  - Axe 5 : Sécurité nationale et coopération pour la sécurité du cyberespace international

# Conclusion

- Développement des TIC et la confiance en l'économie numérique, indispensables au développement harmonieux et durable des Etats, ne pourront se faire que par :
  - La définition d'une politique de cybersécurité
  - L'élaboration et la mise en œuvre d'une stratégie nationale de cybersécurité cohérente, efficace et contrôlable avec un accent particulier sur les infrastructures critiques nationales, dans le respect du droit à la vie privée et des libertés
  - La mise en place de structures spécialisées (CERT, Agence de sécurité informatique, cyberpolice) et la désignation d'un responsable national de la cybersécurité
  - L'implication de toutes les parties prenantes: le Gouvernement, le secteur public, le secteur privé, la population

# Documents et liens utiles

- Union Internationale des Télécommunication (UIT) : [www.itu.int](http://www.itu.int)
  - Résolution 50 sur la Cybersécurité de l'UIT
  - Résolution 58 sur le CERT
  - Guide de la cybersécurité pour les pays en développement ([www.itu.int/ITU-D/cyb/publications/2006/Cyber-Security\\_F.pdf](http://www.itu.int/ITU-D/cyb/publications/2006/Cyber-Security_F.pdf))
  - Recommandations UIT-T (X.805 et X.1205) et des produits/normes ISO/CEI comme cadre pour l'évaluation des vulnérabilités
- Union Européenne
  - Convention sur la cybercriminalité, Budapest, 2001