المملكة المغربية

ires

Institut Royal des Etudes Stratégiques
Royal Institute for Strategic Studies

Les Infrastructures critiques face au risque cybernétique.

Par **M. Ahmed Ghazali**
Président de la Haute Autorité de la Communication Audiovisuelle

الهيئة العليا
للاتصال السمعي البصري
Haute Autorité de la
Communication Audiovisuelle

Introduction

I. Cyber sécurité

1) Systèmes d'information et Infrastructures critiques
2) Sécurité des systèmes d'information
3) Risques et causes
4) Objectifs recherchés
5) Tendances 2012

II. Prise en charge au niveau international

1) Organismes internationaux : IUT, OCDE
2) Benchmarks : France, Tunisie

III. Prise en charge au niveau national

1) Le cadre juridique
2) Les instances

IV. Perspectives

Conclusions

I. Cyber sécurité : Systèmes d'information et Infrastructures critiques

➢ Système d'information

Ensemble de moyens techniques, administratifs, et humains qui servent à la collecte, au classement et à la transmission d'informations entre les membres d'une organisation. (Système de traitement automatisé de données, systèmes informatiques, etc.)

➢ Infrastructure critique :

Installations physiques et des technologies de l'information, les réseaux, les services et les actifs qui, en cas d'arrêt ou de destruction, peuvent avoir de graves incidences sur la santé, la sécurité ou le bien-être économique des citoyens ou encore le travail des gouvernements :

- **Installations et les réseaux dans le secteur de l'énergie;**
- **les technologies des communications et de l'information;**
- **les finances (le secteur bancaire, les marchés des valeurs et les investissements) ;**
- **le secteur des soins de santé; l'alimentation;**
- **l'eau (réserves, stockage, traitement et réseaux);**
- **les transports (aéroports, ports, chemins de fer et réseaux de transit de masse, etc.);**
- **la production, le stockage et le transport de produits dangereux;**
- **l'administration (services de base, installations, réseaux d'information, actifs et principaux sites et monuments nationaux).**
- **Etc.**

I. Cyber sécurité : Sécurité des systèmes d'information

Sécurité des systèmes d'information (SSI)

Gestion des risques liés aux menaces qui exploitent les vulnérabilités des systèmes d'information, par nature complexes, pour causer des dommages.

Elle traite trois composantes :

- **En amont, au niveau des menaces portées sur le système ;**
- **Sur la vulnérabilité du système lui-même ;**
- **Ou encore en aval, au niveau des effets et des conséquences d'une éventuelle atteinte au système.**

Et donc trois niveaux d'analyse et de traitement :

- **Au premier niveau, c'est tout le débat sur la cybercriminalité et sur la fraude informatique,**
- **Au deuxième niveau, la question porte sur la certification électronique, la cryptographie ou encore les normes ISO de la sécurité.**
- **Enfin, au dernier niveau, l'accent est mis sur la protection des données personnelles et sur la propriété industrielle qui analyse le mal par son effet.**

I. Cyber sécurité : Systèmes d'information et Infrastructures critiques

Sécurité des systèmes d'information (SSI)

Concernant plus précisément les infrastructures critiques, il a souvent été fait mention de guerre informatique dans laquelle on distingue trois modes :

- **la guerre <u>contre</u> l'information, qui s'attaque à l'intégrité de systèmes informatiques pour en perturber ou en interrompre le fonctionnement ;**
- **la guerre <u>pour</u> l'information, qui vise à pénétrer les réseaux en vue de récupérer les informations qui y circulent ou y sont stockées ;**
- **la guerre <u>par</u> l'information, qui utilise le vecteur informatique dans un but de propagande, de désinformation ou d'action politique.**

La question se pose donc réellement en terme de sécurité qu'elle soit économique, civile ou nationale dans un environnement ou les échanges sont vitaux dans l'environnement international.

Quels Risques ?

- La perte ou l'altération des données qui les rendent inexploitables
- L'indisponibilité des données ou des traitements pouvant entraîner l'arrêt d'une production ou d'un service ;
- La divulgation d'informations confidentielles ou erronées pouvant profiter à des sociétés concurrentes ou nuire à l'image d'une personne physique ou morale ;
- Le déclenchement d'actions pouvant provoquer des accidents physiques ou induire des drames humains.

Les sources de ces risques sont essentiellement :

- d'origine humaine souvent ignorés ou minimisés, ils sont les plus importants et ont pour cause la maladresse, l'inconscience ou l'ignorance, et la malveillance.
- d'origine technique liés aux incidents matériels, logiciels ou environnementaux.

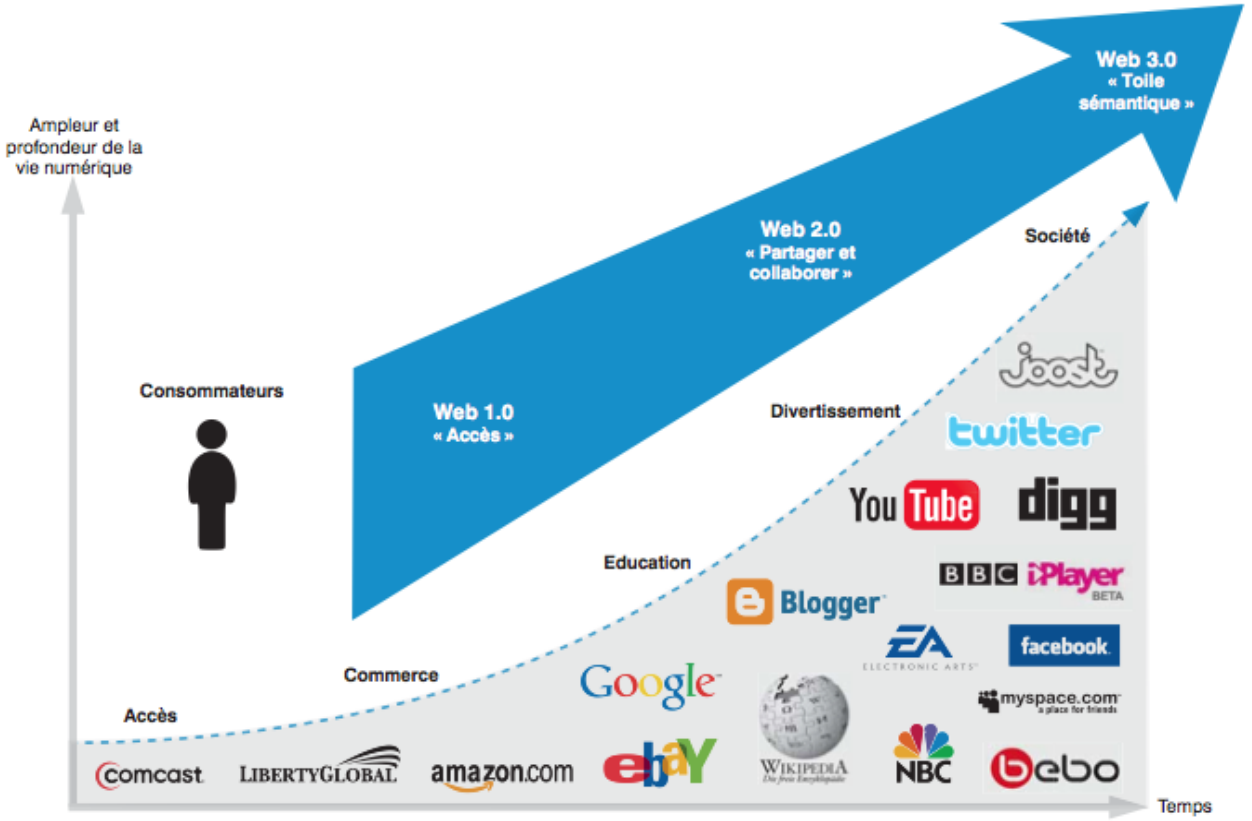
Objectifs recherchés

Les objectifs en matière de sécurité visent d'une part, à s'assurer de la disponibilité de l'information, de son intégrité, de la confidentialité et de la traçabilité, d'autre part, à évaluer les risques pour les prévenir et enfin, à apprécier les sources possibles d'atteintes.

- **Disponibilité : garantie que l'information soit accessible au moment voulu par les personnes autorisées**
- **Intégrité : garantie que l'information soit exacte et complète ;**
- **Confidentialité : garantie que seules les personnes autorisées ont accès aux éléments considérés ;**
- **Traçabilité (ou « Preuve ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.**

I. Cyber sécurité : Les tendances en 2012

Illustration 3: *Développement de la vie numérique*



Source : Booz & Company

I. Cyber sécurité : Les tendances en 2012

Les tendances suivent de facto le développement du numérique :

- **Les technologies des mobiles introduisent de plus en plus de menaces** et leur développement se fait à un rythme supérieur aux capacités d'adaptation des entreprises pour faire face à ces menaces.
- **Les medias sociaux croissent en popularité.** Leur adoption dans les milieux professionnels se fait à un rythme exponentiel, il en est de même des menaces.
- **Les petites et moyennes entreprise sont dans la ligne de mire des 'hackers'.** En effet, ils traitent de grandes quantités de données critiques mais n'ont pas les moyens suffisants pour assurer leur cyber sécurité.
- **Le "cloud computing" se généralise** et entraine de nouvelles brèches ouvertes aux menaces.
- **La coopération entre les entreprises et le gouvernement devient un élément critique nécessaire à la santé des infrastructures et de l'économie.** Le partage d'information entre les secteurs publics et privés devient de plus en plus nécessaire.
- **Les systèmes de géo-localisation devront être de plus en plus contrôlés pour la protection de la vie privée.**
- **La gestion et l'analyse des logs gagneront en importance pour la préparation des réponses aux incidents.** La sophistication et la fréquence des incidents ont augmentés ces dernières années et une des réponses les plus efficaces reste l'analyse des traces.
- **Les CERT vont jouer un plus grand rôle dans les conseils de direction** des entreprises et administrations. L'activité des équipes de réponses aux incidents de sécurité deviendra de plus en plus stratégique et permanente.
- **Les entreprises continueront à négliger certaines vulnérabilités de base tout en se conformant aux aspects règlementaires qui dirigent l'organisation actuelle de la sécurité des systèmes.**

II. Prise en charge au niveau international

Constat : **La sécurité des systèmes d'informations constitue un enjeu majeur pour tous les pays afin de tirer le meilleur profit de la société de l'information, tout en limitant au maximum les vulnérabilités.**

Qui nécessite

l'élaboration d'une stratégie nationale de la cyber sécurité, dans le cadre

- **d'une approche globale et multidisciplinaire,**
- **d'une coopération internationale,**
- **d'un partenariat secteur public / secteur privé,**
- **d'une lutte contre la cybercriminalité,**
- **De la promotion d'une culture de cybersécurité,**

C'est ainsi que les organisations internationales sont actives dans ce domaine :

- **UIT**
- **Europe**

II. Prise en charge au niveau international : UIT

l'UIT

- **Le Sommet mondial sur la société de l'information (SMSI) et la Conférence de plénipotentiaires de l'UIT de 2006 ont confié à l'UIT la tâche fondamentale d'établir la confiance et la sécurité dans l'utilisation des technologies de l'information et de la communication (TIC) et de prendre des mesures concrètes visant à limiter les répercussions des cyber menaces et de l'insécurité liée à la société de l'information.**

- **Lancement le 17 mai 2007 du ITU Global Cybersecurity Agenda qui fournit une trame qui coordonne les travaux des réponse aux défis posés par la cybersécurité,**

- **Le secteur Développement (UIT-D), lors de la conférence des plénipotentiaires de 2006, a été chargé de traiter la problématique de la cyber sécurité et des cyber-menaces et de la lutte contre les spams.**

- **Plusieurs résolutions ont été prises au sommet mondial de l'information et dans les conférences des plénipotentiaires :**
  - ITU Plenipotentiary Resolutions: 130, 174 , 179 , 181 (Guadalajara, 2010)
  - ITU WTDC Resolutions: 45 , 69 (Hyderabad, 2010)
  - ITU WTSA Resolutions:50 , 52 , 58 (Johannesburg, 2008)

- **A titre d'exemple, la résolution 130 renforce le rôle de l'UIT dans l'instauration de la confiance et de la sécurité dans l'utilisation des technilogies de l'information et de la communication.**

II. Prise en charge au niveau international : Europe

- La Convention de Budapest sur la cybercriminalité (23 novembre 2001) constitue le premier traité international sur les infractions pénales commises via l'Internet et d'autres réseaux informatiques.

  - Elle traite en particulier :
    - des infractions portant atteinte aux droits d'auteurs,
    - de la fraude liée à l'informatique,
    - de la pornographie enfantine,
    - ainsi que des infractions liées à la sécurité des réseaux.

  - Elle contient également une série de pouvoirs de procédures, tels que la perquisition de réseaux informatiques et l'interception des données.

  - Son principal objectif, énoncé dans le préambule, est de poursuivre "une politique pénale commune destinée à protéger la société contre le cybercrime, notamment par l'adoption d'une législation appropriée et la stimulation de la coopération internationale".

- L' Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA : European Network and Information Security Agency) est l'agence communautaire compétente en matière de sécurité des systèmes d'information. Créée le 10 mars 2004 par le Règlement du Parlement Européen et du Conseil n° 460/2004, elle est basée à Heraklion, en Grèce.

II. Prise en charge au niveau international : Benchmark

- **France : le cadre juridique**
  - **Loi Godefrain (5 janvier 1981), traite au niveau du droit pénal la fraude informatique et explicitement les cas comme :**
    - **Les atteintes aux systèmes de traitement automatisés de données**
    - **Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données,**
    - **Le fait d'entraver ou de fausser le fonctionnement d'un système automatisé de traitement de données**
    - **Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de modifier frauduleusement les données qu'il contient**
    - **Etc.**
  - **La loi pour la confiance numérique (LCEN du 21 juin 2004) qui transpose la directive européenne sur le commerce électronique. Elle traite, en particulier :**
    - **de la liberté de la communication en ligne et de ses limites,**
    - **encadre les obligations et les responsabilités des prestataires techniques**
    - **et apporte des modifications au code de procédure pénale en matière de saisie des preuves sous format électronique.**
  - **Loi hadopi du 12 juin 2009 favorise la diffusion et la protection de la création sur Internet. Elle sanctionne le partage de fichiers en tant qu'infraction au droit d'auteur.**

II. Prise en charge au niveau international : Benchmark

- **France : Le cadre institutionnel**
  - **Agence Nationale de la sécurité des systèmes d'information (ANSSI) créée le 7 juillet 2009. C'est un service à compétence nationale rattaché au secrétaire général de la défense nationale qui a, entre autre, pour mission**
    - **De mettre en œuvre les moyens interministériels sécurisés de communications électroniques nécessaire au Président et au Gouvernement,**
    - **D'élaborer et coordonner les travaux en matière de sécurité des systèmes d'informations**
    - **De mettre en œuvre les systèmes de détection des évènements susceptibles d'affecter la sécurité des systèmes d'information de l'Etat et coordonne la réaction à ces événements.**
    - **Etc.**
  - **Le centre opérationnel de la sécurité des systèmes d'information (COSSI) assure un service permanent de veille, de détection et d'alerte en cas d'incidents ou de vulnérabilité susceptibles d'affecter la sécurité des systèmes d'informatio de l'Etat et plus largement de la société de l'Information.**
  - **D'autres entités existent comme La Sous direction Stratégie et Règlementation (SR) ou la Sous direction Assistance, Conseil et Expertise (ACE) et apportent leur concours aux administrations et opérateurs d'importance en matière de savoir faire techniques.**

III. Prise en charge au niveau national : Le cadre juridique

La sécurité des systèmes d'informations au Maroc relève de :

- **dispositions du Code pénal qui ont été modifiées pour tenir compte de certaines infractions aux systèmes de traitement automatisé de données.**

- **la réglementation sur :**
  - **les télécommunications,**
  - **en matière de certification électronique,**
  - **de protection des données à caractère personnel,**
  - **des droits d'auteurs et droits voisins**
  - **Etc.**

III. Prise en charge au niveau national : Le cadre juridique

L'arsenal juridique actuel comprend :

- **Dahir n° 1-59-413 du 28 joumada II 1382 (26 novembre 1962) portant approbation du texte du code pénal .**
- **Dahir n° 1-97-162 du 2 rabii II 1418 (7 août 1997) portant promulgation de la loi n° 24-96 relative à la poste et aux télécommunications telle que modifiée et complétée.**
- **Dahir n°1-04-257 du 25 kaada 1425 (7 janvier 2005) portant promulgation de la loi n° 77-03 relative à la communication audiovisuelle.**
- **Dahir n° 1-02-207 du 25 rejeb 1423 (3 Octobre 2002) portant promulgation de la loi n°77-00 modifiant et complétant le Dahir n°1-58-378 du 3 Joumada I 1378 (15 Novembre 1958) formant code de la Presse et de l'Édition.**
- **Dahir n° 1-00-20 du 9 kaada 1420 (15 février 2000) portant promulgation de la loi n° 2-00 relative aux droits d'auteur et droits voisins.**
- **Dahir n°1-07-129 du 19 kaada 1428 (30 novembre 2007) portant promulgation de la loi n°53-05 relative à l'échange électronique de données juridiques.**
- **Dahir n° 1 -09 -15 du 22 safar 1430 (18 février 2009) portant promulgation de la loi n° 09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.**
- **Décret n°2-08-444 du 25 joumada I 1430 instituant un Conseil national des technologies de l'information et de l'économie numérique.**
- **Dahir n° 1-11-03 du 14 rabii I 1432 portant promulgation de la loi n° 31-08 édictant des mesures de protection du consommateur. (B.O. n° 5932 du 7 avril 2011).**

III. Prise en charge au niveau national : Le cadre juridique

Infractions se rapportant aux systèmes d'information et leurs traitements par les textes juridiques

Atteintes aux systèmes de traitement automatisé de données (STAD)			
	Suppression/modification de données	Loi 07-03 modifiant et complétant le code pénal	Art. 607.4
	Altération de fonctionnement		Art. 607.6 Art. 607.7
	Entrave au fonctionnement		Art. 607.5
	Introduction, suppression, modification de données		Art. 607.3, Art. 607.4 Art. 607.6
	Groupement de pirates		Art. 607.9
	Tentative d'infraction sur un STAD		Art. 607.3, Art. 607.4
	Importation, Détention, Offre, Cession, Mise à disposition d'équipement, instrument ou programme informatique conçus ou adaptés pour commettre des infractions aux STAD		Art. 607.10
Terrorisme			
	Infractions aux systèmes de traitement de données considérées comme des actes de terrorisme Apologie des actes de terrorisme par différents moyens d'informations audiovisuels et électroniques	Loi n° 03.03 relative à la lutte contre le terrorisme Titre premier du livre III du code pénal	Art. 218.1 Art. 218.2

III. Prise en charge au niveau national : Les instances

Journal officiel du 17 octobre 2011 : Création de deux instances au sein de la direction de la défense nationale :

- **le Décret n° 2.11.508 portant création de <u>la Commission Stratégique de la Sécurité des Systèmes d'Information, qui a pour rôle :</u>**
  - **Établir les orientations stratégiques dans le domaine de la sécurité des Systèmes d'Information pour garantir la sécurité et l'intégrité des infrastructures critiques marocaines ;**
  - **L'approbation du plan d'action de la Direction Générale de la Sécurité des Systèmes d'Information et l'évaluation de ces résultats ;**
  - **Délimitation des prérogatives de la Direction Générale de la Sécurité des Systèmes d'Information ;**
  - **Statuer sur les projets de lois et des normes relatifs à la sécurité des systèmes d'information.**

- **et le Décret n° 2.11.509 portant création d'une <u>Direction Générale de la Sécurité des Systèmes d'Information qui est chargée principalement de :</u>**
  - **La coordination entre les différents ministères pour l'élaboration de la stratégie nationale de la sécurité des systèmes d'information ;**
  - **Veiller a l'application des recommandations de la commission Stratégique de la Sécurité des Systèmes d'Information ;**
  - **Proposition et de normes et standards de sécurité et gestion des autorisations liées à l'utilisation des certificats électroniques ;**
  - **Assister et conseiller les infrastructures publiques et privées à l'instauration de normes de sécurité des Systèmes d'information ;**
  - **Audit de sécurité des institutions publiques ;**
  - **Création avec les différents groupes ministériels d'un système de veille, d'interception et de réponses aux attaques sur les infrastructures informatiques du pays et la coordination de la réponse aux incidents ;**
  - **Maintenir la commission informé de toute urgence ou menaces sur le système d'information du pays ;**
  - **Assurer la veille technique en sécurité pour anticiper les attaques et proposer les améliorations adéquates ;**
  - **Etc.**

III. Prise en charge au niveau national : Le Ma-CERT

Le MA-CERT

- **Le 5 octobre 2010, le ministère de l'Industrie, du Commerce et des Nouvelles Technologies et l'Agence coréenne de Coopération internationale (KOICA) ont signé, une convention portant sur la mise en place du Centre marocain d'alerte et de gestion des incidents informatiques "MA-CERT : Morocco Computer Emergency Response Team".**

- **Rôle : assurer la surveillance et la coordination des systèmes de sécurité informatique au niveau national.**

- **Missions : coordonner, prévenir et proposer divers services portant sur la sécurité des systèmes dont, en particulier :**
  - **Le traitement des incidents liés à la sécurité des SI, notamment les cyber attaques.**
  - **La prévention et la proposition de solutions de lutte contre les menaces d'usurpation, de vol, ou de corruption de donnée.**
  - **L'analyse et la restauration des systèmes attaqués/infectés.**

III. Perspectives et Conclusions

Pour la Sécurité des systèmes

- **Appuyer l'harmonisation du cadre juridique marocain, en prenant en considération les tendances SSI au niveau international, tant au niveau réglementaire qu'institutionnel**
- **Adopter de bonnes pratiques notamment des '' politiques de sécurité certifiée'' et ''d'audit annuel'' ou périodique**
- **Etablissement de chartes et de codes déontologiques aussi bien par les exploitants que par les utilisateurs des réseaux et systèmes d'information**
- **Adoption d'une loi spécifique pour encadrer les conditions et les modalités de mise en œuvre d'une politique nationale en matière de SSI ? ou apporter les modifications nécessaires, le cas échéant, aux textes existants ?**
- **Adopter les normes et standards internationaux en vigueur**

III. Perspectives et Conclusions

En vous remerciant pour votre attention….