CHAPITRE 4 : La Cybersécurité : Principes, Enjeux et Eléments de solution.

I. INTRODUCTION

Enjeux de société, enjeux économiques, enjeux politiques, enjeux humains, qu'elle soit dénommée sécurité de l'informatique et des télécoms ou **cybersécurité**, la sécurité informationnelle touche 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 du numérique (e-services) qui intègre une stratégie pluridisciplinaire de la **cybersécurité** cohérente, efficace et contrôlable. Obtenir un niveau de sécurité informatique suffisant pour prévenir les risques technologique et informationnel est primordial pour le bon fonctionnement des Etats et des organisations. En effet, l'adoption des technologies du numérique, la dépendance des organisations et des Etats à ces mêmes technologies et l'interdépendance des infrastructures critiques, introduisent un degré de vulnérabilité non négligeable dans le fonctionnement normal des Institutions. Ceci peut mettre en péril leur pérennité ainsi que la souveraineté des Etats.

L'objet de la **cybersécurité** est de contribuer à préserver les forces et les moyens organisationnels, humains, financiers, technologiques et informationnels, dont se sont dotées les Institutions, pour réaliser leurs objectifs. La finalité de la sécurité informatique est de garantir qu'aucun préjudice ne puisse mettre en péril leur pérennité. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre.

Ainsi, le contexte de la sécurité des infrastructures de communication est analysé à la lumière du constat de la vulnérabilité et de l'état d'insécurité associé aux technologiques de l'information et des communications.

II. Le Cyberespace et la société de l'information.

A) Généralités sur la Dématérialisation et L'Information Numérique.

Les technologies informatiques induisent des modifications structurelles importantes car tous les **objets** sont devenus manipulables électroniquement au travers de l'information les modélisant.

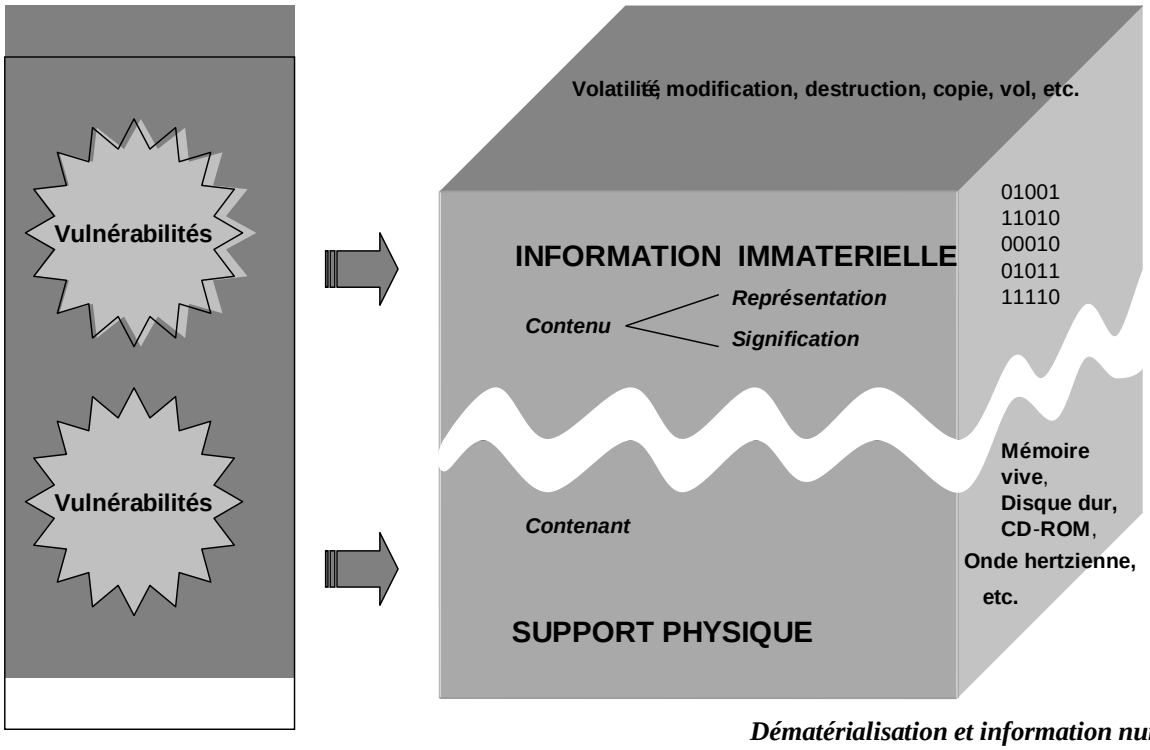
Dans ce cadre la technique de numérisation crée une image digitale ou double virtuel ou encore double numérique des entités existantes. Quelle que soit sa nature (voix, données, image), toute information est numérisable et possède une représentation homogène, c'est-à-dire uniforme.

L'information n'est plus associée physiquement à son contenant, c'est-à-dire à son support de représentation et de stockage puisque sa valeur ajoutée provient directement de l'information elle-même (contenu ou content), et en plus les coûts de diffusion et de mémorisation de l'information sont peu élevés par rapport à ceux de sa conception.

B) Révolution Informationnelle et les Dangers

Le passage à l'ère informationnelle révèle l'importance des technologies de l'information et de leur maîtrise. En considérant les dimensions nouvelles qu'elles introduisent sur les plans techniques et socio-économiques, la nécessité d'assurer la sécurité des systèmes et infrastructures informatiques et de télécommunications, est devenue fondamentale. Elle souligne le caractère stratégique et critique de la gestion et de la mise en œuvre de la **cybersécurité**, tant pour les Etats, les organisations que pour l'individu.

Dans la mesure où les Etats ont effectué des efforts financiers, matériels et humains importants pour réaliser leur infrastructure informatique et de télécommunication, il est primordial qu'ils se dotent des moyens permettant de les sécuriser, de les gérer et de les contrôler.



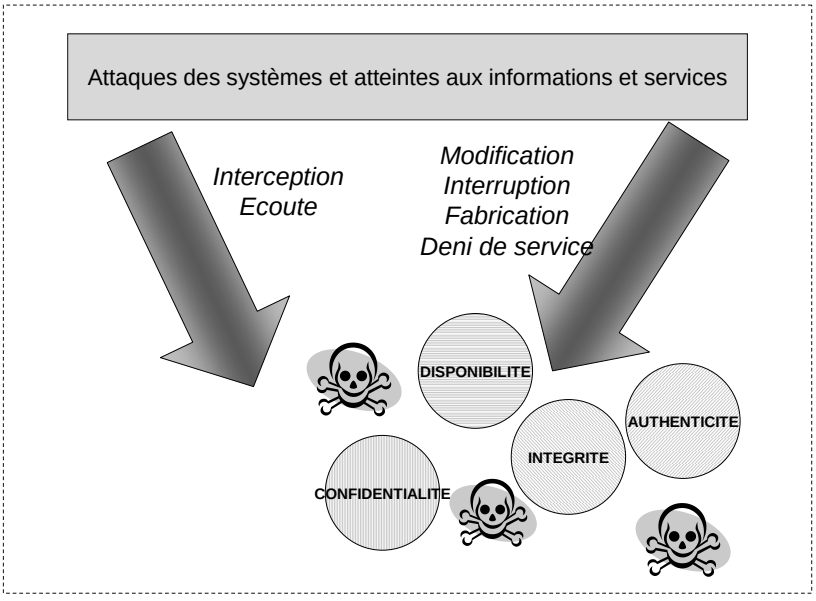
Dématérialisation et information numérique

III. La Cybersécurité

A) Le Contexte de la sécurité des infrastructures de communication

Les infrastructures de télécommunication et les services et activités qu'elles permettent de développer et de générer doivent être pensés, conçues, mise en place et gérées en termes de sécurité. La sécurité est la pierre angulaire de toute activité et doit être vue comme un service permettant de créer d'autres services et de générer de la valeur (e-gouvernement, e-santé, e-éducation, etc.). Au-delà des technologies, les outils de communication basiques mis à disposition, n'intègrent pas des moyens suffisants et nécessaires à la réalisation ou à la garantie d'un niveau minimal de sécurité.

Les systèmes informatiques mis en réseau sont des ressources accessibles à distance et deviennent des cibles potentielles d'attaques informatiques. Cela accroît les risques d'intrusion des systèmes et offre un terrain favorable à la réalisation, à la propagation des attaques et des délits. Au-delà des systèmes attaqués ce sont les informations qu'ils manipulent qui sont convoitées. Les attaques portent atteintes à la capacité à traiter, sauvegarder, communiquer le capital informationnel, aux valeurs immatérielles et aux symboles, aux processus de production ou de décision de ceux qui les possèdent. Les systèmes informatiques introduisent un risque opérationnel dans le fonctionnement des institutions qui les possèdent.



B) Définitions (Cybersécurité et Cybercriminalité)

La Cybersécurité : ensemble de mesures de prévention, de protection et de dissuasion d'ordre technique, organisationnel, juridique, financier, humain, procédural et autres actions permettant d'atteindre les objectifs de sécurité fixés à travers les réseaux de communications électroniques, les systèmes d'information et pour la protection de la vie privée des personnes.

L'**ANSSI** (Agence nationale de la Sécurité des Systèmes d'Information) a définit la **cybersécurité** comme un « état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

La **cybersécurité** fait appel à des techniques de sécurité des systèmes d'information et s'appuie sur la lutte contre la cybercriminalité et sur la mise en place d'une **cyberdéfense**.

De manière pratique le terme **cybersécurité** désigne l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formation, bonnes pratiques et technologies qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels (connectés directement ou indirectement à un réseau) des états et des organisations (avec un objectif de disponibilité, intégrité et authenticité, confidentialité, preuve et non-répudiation).

La **cybersécurité** concerne la sécurité de chaque Etat. C'est pourquoi une grande majorité des Etats ont reconnu la nécessité de s'organiser et d'assurer la sécurité et la défense de leurs systèmes techniques.
Des stratégies nationales de ***cybersécurité*** et ***cyberdéfense*** sont nées afin de lutter contre la cybercriminalité.

Cybercriminalité : ensemble des infractions s'effectuant à travers le cyberespace par des moyens autres que ceux habituellement mis en œuvre, et de manière complémentaire à la criminalité classique.
(loi N°2010/012 du 21 décembre 2010).

C) Les Enjeux de la Cybersécurité.

Un *enjeu* est une valeur matérielle ou morale que l'on risque dans un jeu, une compétition, une activité économique ou une situation vis-à-vis d'un aléa.

Le risque d'une attaque informatique contre les infrastructures nationales est une des menaces majeures actuellement. Le développement de la société de l'information, l'utilisation croissante des réseaux dans les processus vitaux de l'État et de la société font de la prévention et de la réaction aux attaques informatiques une priorité majeure de nos dispositifs de sécurité.

Les principaux Enjeux de la cybersécurité :

1. **Au niveau des Etats**

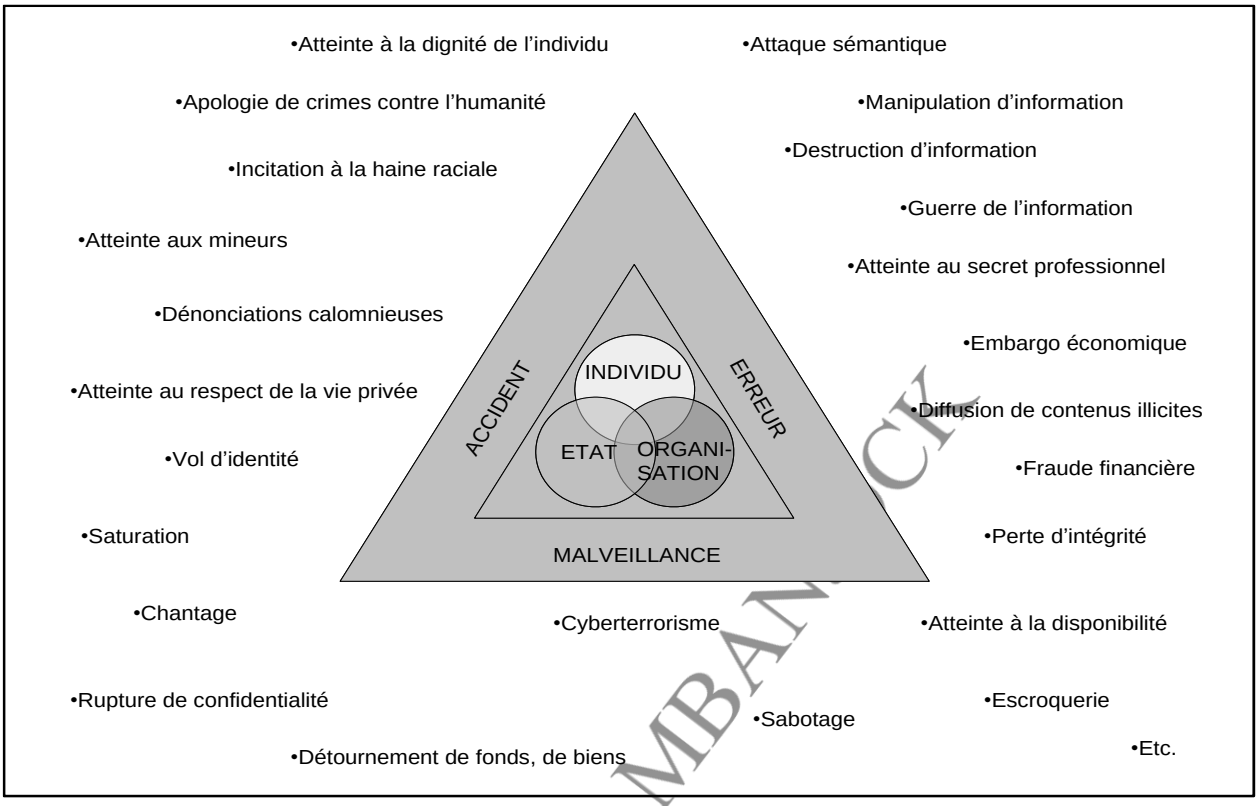
Pour chaque Etat, il s'agit d'un enjeu de souveraineté nationale. Tout Etat a en effet la responsabilité, de garantir aussi bien la sécurité de ses propres systèmes d'information, la continuité de fonctionnement des institutions et des infrastructures vitales aussi bien les activités socio-économiques du pays que la protection des entreprises et des citoyens.

2. **Au niveau des entreprises**

Pour plusieurs entreprises, l'information et la technologie qui la supporte constituent les actifs les plus précieux. En effet, l'informatique est passée du stade où elle était considérée comme un outil de support, au stade de levier stratégique de développement des organisations et constitue désormais un facteur déterminant pour garantir les performances et développer les perspectives de croissance.

3. Au niveau du grand public

Le principal enjeu réside dans le degré de confiance du public en l'économie numérique en ce sens que les entreprises et les gouvernements dotés de systèmes informatiques devraient être en mesure de sécuriser les systèmes et les transactions tout en protégeant efficacement les données et les renseignements personnels des citoyens.



Différents niveaux de la cybersécurité: individus, organisations, Etats

Le développement des activités basées sur le traitement de l'information permettant une réduction de la fracture digitale passe par la mise à disposition:

- d'infrastructures informationnelles fiables et sécurisées (accessibilité, disponibilité, sûreté de fonctionnement et continuité des services garanties);
- de politiques d'assurance;
- d'un cadre légal adapté;
- des instances de justice et de police compétentes dans le domaine des nouvelles technologies et capables de coopérer au niveau international avec leurs homologues;
- d'outils de gestion du risque informationnel et de gestion de la sécurité;
- d'outils de mise en œuvre de la sécurité qui permettent de développer la confiance dans les applications et services offerts (transactions commerciales et financières, e-santé, e-gouvernement, e-vote, etc.) et dans les procédures qui permettent le respect des droits de l'Homme notamment pour ce qui concerne les données à caractère personnel.

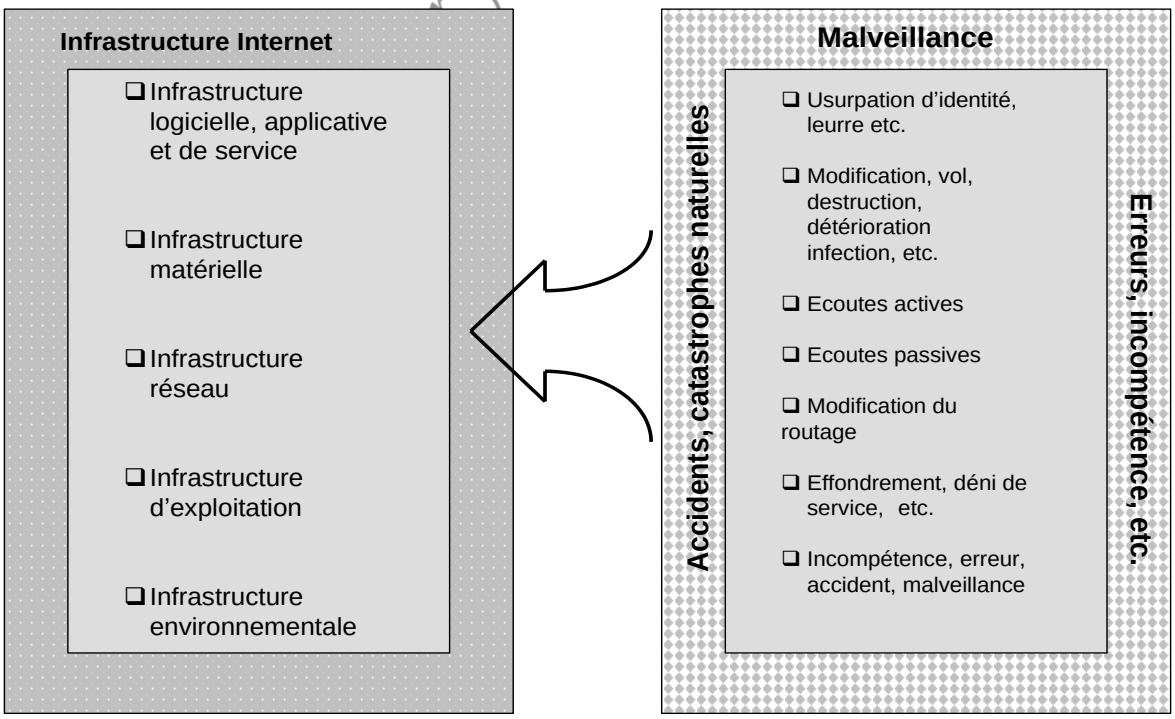
D) Finalité et Démarche de la Cybersécurité

La **finalité** de la sécurité informatique est de garantir qu'aucun préjudice ne puisse mettre en péril la pérennité de l'organisation. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à en limiter les atteintes ou dysfonctionnements induits, et autoriser le retour à un fonctionnement normal à des coûts et des délais acceptables en cas de sinistre.

La **démarche** de **cybersécurité** est un projet de société dans la mesure où chacun est concerné par sa réalisation. Sa validité sera renforcée si une **cyberéthique** d'utilisation et de comportement vis-à-vis des technologies de l'information est développée et si une véritable politique de sécurité stipule ses exigences de sécurité envers les utilisateurs, acteurs, partenaires et prestataires de la sécurité des nouvelles technologies.

E) Le Constat de l'insécurité numérique

La réalité de l'insécurité des technologies de traitement de l'information et des communications trouve ses origines dans les caractéristiques des technologies de l'information et du monde virtuel. La dématérialisation des acteurs, les accès à distance, un relatif anonymat, les problèmes de conception, de mise en œuvre, de gestion, de contrôle de l'informatique et des télécoms, associés aux pannes, dysfonctionnements, erreurs, incompétences, incohérences ou encore aux catastrophes naturelles, confèrent *de facto* un certain niveau d'insécurité aux infrastructures informatiques (Figure I.4).



Infrastructure de l'Internet et multiplicité de l'origine des problèmes

F) Les Principes à prendre en compte

1. La Gouvernance de la sécurité Informatique

La «**gouvernance**» de la sécurité est un ensemble d'outils qui permettent de garantir que les mesures de sécurité sont optimales dans le temps et dans l'espace. Cette notion répond aux interrogations suivantes:

- Qui fait quoi ? Comment ? et quand?
- Quels sont les acteurs qui élaborent les règles, qui les définissent et les valident, qui les mettent en œuvre et qui les contrôlent?

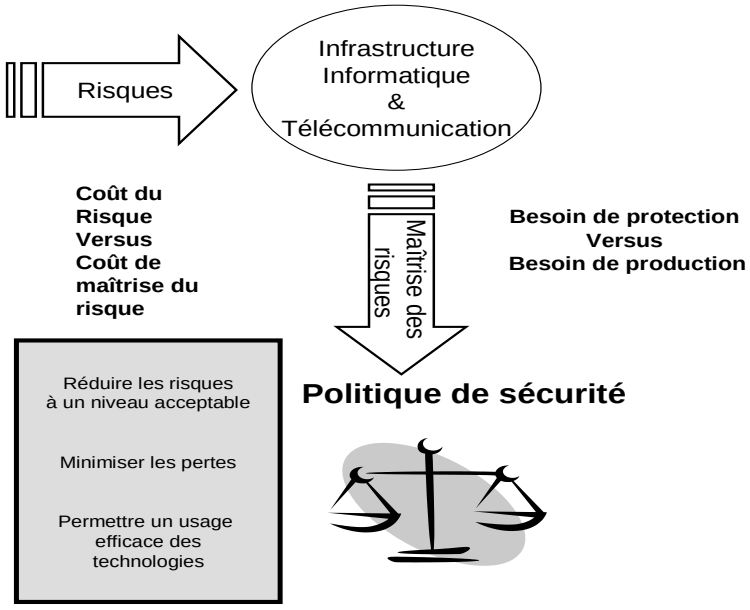
2. Identification et gestion des risques

Un risque est un danger éventuel plus ou moins prévisible. Il se mesure à la probabilité qu'il se produise et aux impacts et dommages consécutifs à sa réalisation. Un risque exprime la probabilité qu'une valeur soit perdue en fonction d'une vulnérabilité liée à une menace, à un danger.

Le risque informatique est un risque opérationnel qui doit être maîtrisé. La gestion des risques constitue le point de départ de l'analyse des besoins de sécurité qui permet la définition de la stratégie et de la politique de sécurité. Plusieurs questions se posent retenons entre autres, les suivantes:

- Qui est responsable de l'analyse des risques, de la gestion des risques?
- Comment effectuer une telle analyse?
- Quels sont les outils et méthodologies disponibles?
- Quels sont leurs niveaux de fiabilité?
- Quelle importance à accorder aux résultats? Combien cela coûte?
- Faut-il externaliser cette fonction?
- Etc.

Un compromis entre le coût du risque et celui de sa réduction permet de déterminer le niveau de protection et les mesures de sécurité à mettre en œuvre.



Différents compromis pour la maîtrise des risques: un choix politique

3. Définition d'une Politique de sécurité

Une **politique de sécur**ité spécifie entre autres, les moyens, l'organisation, les procédures, les plans de défense et de réaction qui permettent une véritable maîtrise des risques opérationnel, technologique et informationnel.

La politique de sécurité permet de traduire la compréhension des risques encourus et de leurs impacts, en des mesures de sécurité à implémenter. Elle facilite l'adoption d'une attitude préventive et réactive faces aux problèmes de sécurité et permet de réduire les risques et leurs impacts.

La norme **ISO 17799** qui propose un code de pratique pour la gestion de la sécurité, présentée comme :

- un référentiel permettant de définir une politique de sécurité,
- une liste de points de risques à analyser (*check list*),
- une aide à l'audit de la sécurité en vue ou non d'une procédure de certification,

- un point de communication sur la sécurité.

La version 2005 de la norme (ISO/IEC 17799:2005)1 met l'accent sur l'évaluation et l'analyse des risques, la gestion des valeurs et des biens ainsi que la gestion des incidents. La dimension managériale de la sécurité y est décrite.

Elements d'une politique de securite
Organisation de la sécurité
Attribuer des responsabilités à des personnes compétentes possédant l'autorité et les moyens nécessaires
Identifier les cibles sécuritaires de chaque domaine et composant du système d'information
Définir les menaces – Identification des vulnérabilités
Définir les mesures de sécurité
Définir les comportements de sécurité

Que protéger?
De qui? De quoi doit-on se protéger?
Pourquoi?

Quels sont les risques réellement encourus?
Ces risques sont-ils supportables?

Quel est le niveau actuel de sécurité de l'entreprise? Quel est le niveau que l'on désire atteindre?

Quelles sont les contraintes effectives? Quelles sont les moyens disponibles? Comment les mettre en œuvre?

Gérer la sécurité passe par la définition d'une politique de sécurité

La qualité de la sécurité informatique dépend de l'identification et de l'évaluation de la valeur du patrimoine informationnel, de la mise en œuvre opérationnelle de mesures de sécurité adaptées à partir d'une définition correcte d'une politique de sécurité et d'une gestion efficace.

4. Déployer des solutions

Les principales mesures à déployer pour contribuer à sécuriser des infrastructures informatiques et de télécommunications sont :

- éduquer, former, sensibiliser l'ensemble des acteurs à la **cybersécurité**;
- mettre en place des structures qui permettent de fonctionner comme centre d'alerte et de gestion de crise au niveau national, de fédérer les moyens à mettre en œuvre pour les réaliser, les partager pour un ensemble de pays, pour une région;
- imposer des surveillances, des contrôles (par analogie aux contrôles mis en place sur les réseaux routiers);
- développer les compétences d'une cellule de **cyberpolice** pouvant contribuer à une coopération internationale dans le domaine de la poursuite et de l'investigation du crime informatique;
- développer des solutions technologiques pour ce qui concerne la gestion des identités, le contrôle d'accès, l'usage de plate-formes matérielle et logicielle sécurisées, les infrastructures de secours, les protocoles cryptographiques, la gestion opérationnelle.

G) Les principaux aspects de Mise en œuvre d'une Politique de Sécurité.

1) Au Point de vue managérial

a) La Gestion dynamique

La politique de **cybersécurité** est déterminée au niveau le plus élevé de la structure concernée. Il existe plusieurs stratégies de sécurité, de politiques de sécurité, de mesures, de procédures ou de solutions de sécurité que d'organisations et de besoins sécuritaires à satisfaire à un moment donné.
Le processus de découverte et de correction des failles de sécurité se fait avec :

- une publication périodique des correctifs (***patches*** ou rustines de sécurité).
- les lettres d'informations (***newsletters***) plus ou moins personnalisées permet de se tenir informer de la découverte des failles et de la manière d'y remédier.

Dans le but de maintenir un certain de niveau de sécurité, le responsable sécurité ou l'administrateur système, doit au fur et à mesure de leur publication installer les ***patches*** de sécurité, contrôler le processus de mise à jour (acceptation ou non de l'installation des correctifs), implémenter un mode automatisé permettant de déléguer implicitement à l'éditeur et au fournisseur l'installation régulière et systématique des correctifs.

b) Externalisation et dépendance

La stratégie d'externalisation de la sécurité concerne notamment la définition de la politique et sa mise en œuvre, la gestion des accès, de pare-feu (*firewall*), la télémaintenance des systèmes et réseaux, la tierce maintenance applicative, la gestion des sauvegardes, etc.
En proposant des filtres anti-virus ou anti-spam, ces fournisseurs de service gèrent une partie de la sécurité de leurs clients.

c) La Démarche de prévention et de réaction

L'appréhension de la criminalité informatique s'inscrit, généralement dans une démarche de réaction et de poursuite qui s'effectue après la survenue d'un sinistre qui traduisant de ce fait la défaillance des mesures de protection.
Il est nécessaire dans ce cas :

- de prévenir et de dissuader les cyber-abus, en développant des mécanismes de justice et d'investigation,
- d'identifier dans les politiques de sécurité, les mesures qui permettront de réagir aux attaques et d'en poursuivre leurs auteurs,
- de concevoir et de réaliser des plans de secours et de continuité qui intègrent les contraintes liées à l'investigation et à la poursuite de la criminalité informatique à des logiques de travail et à des objectifs différents, dans des échelles de temps distinctes.

2) Au Point de vue politique

a) La Responsabilité de l'Etat

L'Etat possède des responsabilités importantes pour la réalisation d'une sûreté numérique.
Il doit donner les moyens aux différents acteurs d'apprendre à gérer les risques technologique, opérationnel et informationnel qui les menacent en fonction de l'usage fait des nouvelles technologies.
L'Etat doit aussi :

- favoriser le signalement des agressions liées au **cybercrime** et instaurer la confiance entre les différents acteurs du monde économiques et les services de justice et de police.
- définir une véritable politique de développement de la société de l'information en fonction de ses valeurs propres et de mettre à disposition les moyens nécessaires pour cette réalisation.

b) La Souveraineté des Etats

Les Etats doivent contribuer à imposer:

- De pouvoir disposer de la sécurité en mode natif (sécurité par défaut) et de manière conviviale, compréhensible, transparente, contrôlable et vérifiable;
- D'éviter que les individus et Institutions se mettent en situations dangereuses (éviter les configurations permissives, les comportements à risques, la dépendance excessive, etc.);
- Le respect des normes de sécurité;
- Une réduction des vulnérabilités dans les technologies et dans les solutions de sécurité.

3) Au Point de vue économique

La sécurité ne permet pas directement de gagner de l'argent mais évite d'en perdre.
Le coût de la sécurité est fonction des exigences des organisations et dépend des valeurs à protéger, du coût des préjudices consécutifs à un défaut de sécurité. Aussi, il n'existe pas de réponse prédéfinie aux questions suivantes:

- Comment évaluer l'exposition de l'organisation aux risques, notamment aux risques sériels dus à l'interconnexion des infrastructures inter-organisations?
- Comment estimer correctement les coûts indirects de l'insécurité, résultant par exemple d'une perte d'image ou de l'espionnage?
- Que peut rapporter la sécurité pour l'organisation qui la met en œuvre?
- Quelle est la valeur économique de la sécurité?
- Quel est le retour sur investissement de la sécurité?

4) Au Point de vue social

Il est important de sensibiliser l'ensemble des acteurs du monde de l'Internet aux enjeux de la maîtrise de la sécurité et aux mesures élémentaires qui, si elles sont bien définies et mise en œuvre, renforceront le niveau de sécurité.
Éduquer l'ensemble des cybercitoyens à adopter une démarche sécurité à travers des actions d'information et d'éducation civique à une société de l'information responsable, sur les enjeux, les risques et les mesures préventives et dissuasives de sécurité.

5) Point de vue juridique

A l'heure actuelle, la **cybercriminalité** est mal maîtrisée comme continu de le démontrer les chiffres des sondages du **CSI** (*Computer Security Institute*) ou les statistiques du **CERT** (*Computer Emergency and Response Team*).

De manière pratique, les mesures de sécurité mises en place par les institutions tendent à protéger un environnement donné dans un contexte particulier, mais ne peuvent aucunement empêcher la conduite d'activités criminelles via l'Internet. Les raisons de cette situation sont notamment liées:

- aux caractéristiques du **cybercrime** (capacité à être automatisé, savoir-faire embarqué dans le logiciel, réalisation à distance);
- à la possibilité offerte au **cybercriminel** d'usurper facilement et sans risque excessif, l'identité d'utilisateurs légitimes, ruinant par là même la capacité de la justice à identifier les auteurs réels d'une infraction;
- à la détermination des compétences pour réaliser une enquête;
- à la pénurie de ressources humaines et matérielles au sein des services chargés de la répression – des crimes et délits informatiques;
- au caractère transnational de la cybercriminalité qui nécessite des recours fréquents à la coopération et à l'entraide judiciaire internationale. Cette dernière implique des contraintes de

temps non compatibles avec la rapidité d'exécution des agressions et les besoins de reprise immédiate des systèmes informatiques concernés par les cyberattaques;
- à la difficulté de qualifier les faits au regard de certaines législations pénales;
- à la nature mal définie et à la volatilité de la plupart des preuves informatiques.

Pour toutes ces causes, le système judiciaire dans le contexte de l'Internet, n'est pas efficace.
Des législations nées de la nécessité de définir un cadre juridique approprié à l'usage des nouvelles technologies, doivent compléter la plus part des législations existantes qui sont valides dans le cyberespace ; en apportant des moyens pratiques pour les appliquer.

H) Les Concepts Fondamentaux de la Cybersécurité

Les critères de base de la sécurité que sont : ***la disponibilité, l'intégrité et la Confidentialité*** (critères **DIC**). A ces trois premiers critères s'ajoutent ceux qui permettent de prouver l'identité des entités (notion d'authentification) et que des actions ou évènements ont bien eu lieu (notions de non répudiation, d'imputabilité voire de traçabilité).

1) Description des Critères Fondamentaux

Les Critères de Sécurité	Caractéristiques
Disponibilité	Elle est mesurée sur la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la capacité d'une ressource (serveur ou réseau par exemple). La disponibilité d'une ressource est, en outre, indissociable de son accessibilité.
Intégrité	Le respect de l'intégrité des données, traitements ou services permet d'assurer qu'ils ne sont pas modifiés, altérés ou détruits tant de façon intentionnelle qu'accidentelle. Cela contribue à assurer leur exactitude, leur fiabilité et leur pérennité. L'intégrité des données ne sera garantie que si elles sont protégées des écoutes actives qui peuvent modifier les données interceptées. Cette protection pourra être réalisée par la mise en œuvre de mécanismes de sécurité tels que: – Un contrôle d'accès rigoureux; – Un chiffrement des données; – des moyens de protection contre les virus, les vers ou les chevaux de Troie.
Confidentialité	La confidentialité est le maintien du secret des informations, des flux, des transactions, services ou actions réalisées dans le cyberespace. Il s'agit de la protection des ressources contre une divulgation non autorisée. La confidentialité peut être réalisée par la mise en œuvre de mécanismes de contrôle d'accès ou de chiffrement. Le chiffrement des données (ou cryptographie), contribue à assurer la confidentialité des informations lors de leur transmission ou de leur stockage en les transformant de façon à ce qu'elles deviennent inintelligibles aux personnes ne possédant pas les moyens de les déchiffrer.
Identification et authentification	L'authentification doit permettre de ne pas avoir de doute sur l'identité d'une ressource. Cela suppose que toutes les entités (ressources matérielles, logicielles ou personnes) soient correctement identifiées et que certaines caractéristiques puissent servir de preuve à leur identification. Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent notamment de gérer l'identification et l'authentification des entités. (seuls les ayant droits identifiés et authentifiés peuvent accéder aux ressources ; contrôle d'accès et les modifier s'ils sont habilités à le faire);

Non répudiation	Mécanisme nécessaire pour prouver la réalisation de certains évènements (action, transaction). A la non-répudiation sont associés les notions de responsabilité d'imputabilité, de traçabilité et éventuellement d'auditabilité. La non répudiation et l'imputabilité (les entités identifiées et authentifiées ont réalisé action spécifique), la preuve de l'origine d'un message, d'une transaction (une entité identifiée et authentifiée a effectué une émission), la preuve de la destination (une entité identifiée et authentifiée est destinatrice d'un message).Non répudiation aux Données, et Non répudiation à la Remise.

Capacité d'un système à:	Objectifs de sécurité	Moyens de sécurité
Pouvoir être utilisé	▪ Disponibilité ▪ Pérennité ▪ Continuité ▪ Confiance	▪ Dimensionnement ▪ Redondance ▪ Procédures d'exploitation et de sauvegarde
Exécuter des actions	▪ Sureté de fonctionnement ▪ Fiabilité ▪ Durabilité ▪ Continuité ▪ Exactitude	▪ Conception ▪ Performances ▪ Ergonomie ▪ Qualité de service ▪ Maintenance opérationnelle
Permettre l'accès aux entités autorisées (aucun accès illicite)	▪ Confidentialité (maintien du secret) ▪ Intégrité (aucune modification)	▪ Contrôle d'accès ▪ Authentification ▪ Contrôle d'erreur ▪ Contrôle de cohérence ▪ Chiffrement
Prouver des actions	▪ Non-répudiation ▪ Authenticité (aucun doute) ▪ Aucune contestation	▪ Certification ▪ Enregistrement, traçabilité ▪ Signature électronique ▪ Mécanismes de preuve

Fondamentaux de la cybersécurité

2) La Sécurité physique

Les environnements qui abritent les postes de travail, les serveurs, les zones d'exploitation informatique et de logistique (air conditionné, tableaux de contrôle de l'alimentation électrique, etc.) doivent être physiquement protégés contre des accès indus et des catastrophes naturelles (feu, inondation, etc.). La sécurité physique représente le contrôle le plus fondamental et le plus courant des systèmes informatiques.

3) Les Solutions de sécurité

Face aux problèmes sécuritaires que subissent les infrastructures, et sur la base du constat que les solutions de sécurité ne manquent pas, les questions suivantes sont posées :

- Les solutions de sécurité sont-elles adaptées aux besoins?
- Sont-elles implantées et gérées correctement?
- Peuvent-elles s'appliquer, s'adapter à un environnement en perpétuelle mutation?
- Peuvent-elles pallier le pouvoir excessif accordé aux administrateurs systèmes?
- Comment peuvent-elles faire face aux problèmes sécuritaires dont l'origine est à rechercher dans la négligence, l'incompétence, les défaillances lors de la conception, de la mise en œuvre ou de la gestion des technologies et des solutions de sécurité?
- etc.