COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

SESSION 10

Guide d'élaboration d'une stratégie sur la cybersécurité et la lutte contre la cybercriminalité

Abuja, 11-13 septembre 201

Adel Jomni
Enseignant-chercheur, Université de Montpellier
Directeur diplôme: Cybercriminalité et Droit
Expert auprès du Conseil de l'Europe

Objectifs de la présentation

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Partager des réflexions, avec les participants, sur les politiques et les stratégies à mettre en œuvre pour renforcer la cybersécurité et la lutte contre la cybercriminalité.

- ✓ Introduction sur les actions prioritaires à prévoir dans le cadre d'une stratégie nationale dans le domaine de la cybersécurité et la lutte contre la cybercriminalité.

Cybersécurité

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

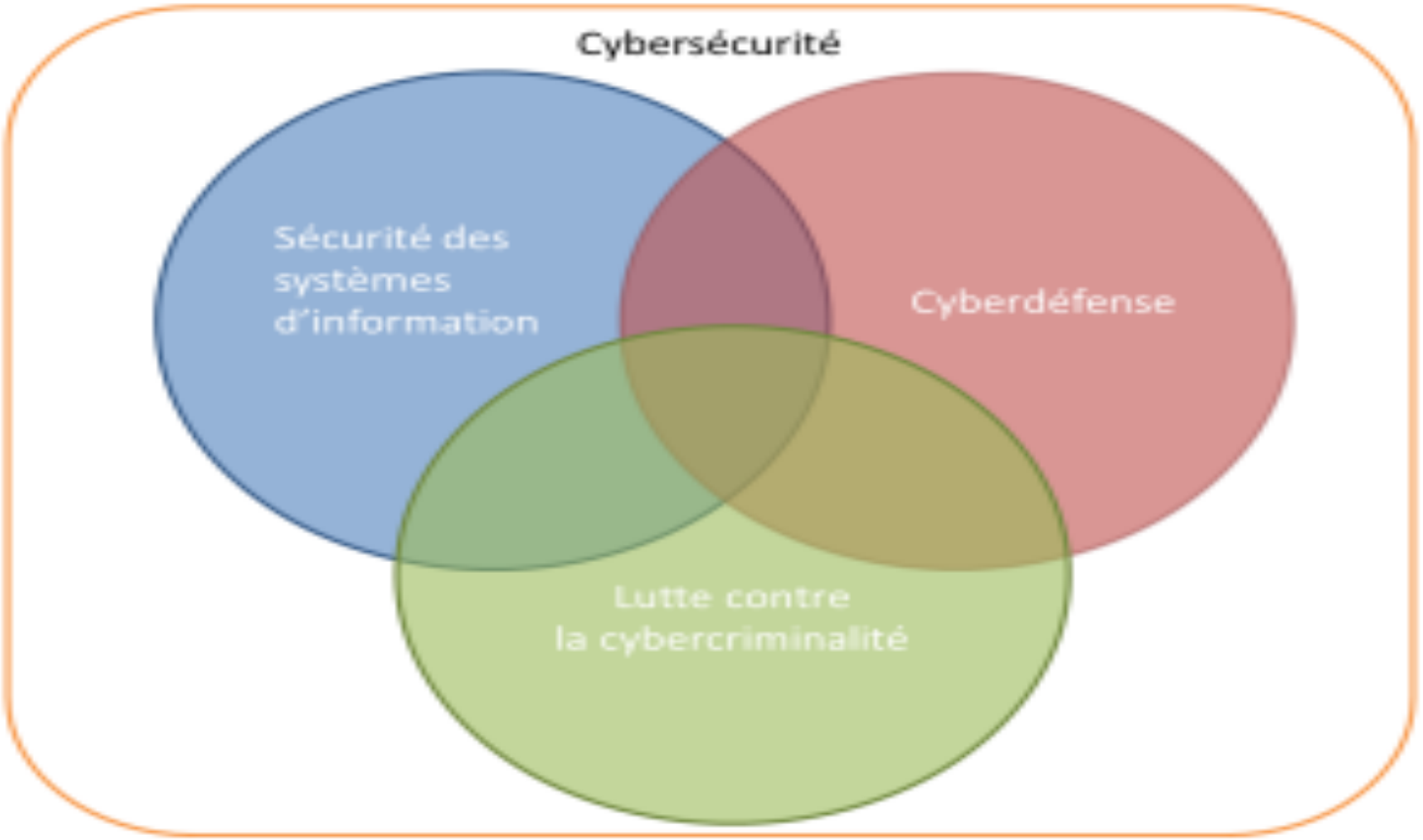
Etat recherché pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

Cybersécurité

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

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.



Sécurité des systèmes d'information (SSI)

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaire et mis en place pour conserver, rétablir, et garantir la sécurité du système d'information »

L'objectif est de prévenir les menaces et d'assurer la disponibilité, la confidentialité et l'intégrité d'un système d'information.

Cyberdéfense

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Ensemble des mesures techniques et non-techniques permettant à un État de défendre, dans le cyberespace, les systèmes d'information jugés essentiels

La cyberdéfense: enjeu mondial, une priorité nationale

Il s'agit de se défendre contre les attaques informatiques susceptibles de porter atteinte aux intérêts fondamentaux de la Nation.

Cyber-terrorisme

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
CEDEAO ECOWAS

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- Utilisation de l'information et du contrôle des systèmes d'information, par des groupes organisés ou par un individu, comme arme stratégique pour exercer des pressions et intimider l'adversaire.
- Il se manifeste essentiellement par de manipulation de l'information, de désinformation, de piratage, d'infiltration de réseaux, etc.
- Le Déni de service (DDoS) est un exemple type d'attaque qui peut être utilisée à des fins cyberterroristes.
- La manipulation de l'information est une forme de cyberterrorisme

Les enjeux de la cybersécurité

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Pour les Etats : souveraineté nationale

- Stratégique (une problématique de défense et sécurité nationale)
- Diplomatique
- Economique
- Militaire
  - ✓ déstabiliser l'ennemi en portant atteinte, voire en détruisant ses systèmes informatiques.

✓ Le cyberespace devient un lieu d'affrontements géopolitiques.

✓ La cyberdissuasion est devenue une nouvelle doctrine de défense nationale.

Les enjeux de la cybersécurité

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Pour les entreprises

- Financier (perte de chiffre d'affaires, perte d'avantage concurrentiel...)
- Juridique (amendes, non respect des libertés individuelles…)
- Perte d'image (réputation, confiance des clients…)

A méditer

« Il faut environ 20 ans pour construire une réputation, et seulement 5 minutes pour la ruiner ! » ***Warren Buffet***

Pour les citoyens,

- protéger ses données personnelles et sa vie privée.

Axes prioritaires d'une stratégie nationale

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
CEDEAO ECOWAS

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

1. Renforcement des capacités de cybersécurité
2. Adaptation du cadre légal et réglementaire
3. Renforcement de la lutte contre la cybercriminalité
4. Développement d'une politique de Cyberdefense
5. Formation - Sensibilisation
6. Développement de la coopération public-privé
7. Renforcement de la coopération régionale/internationale
8. Favoriser l'instauration de la confiance numérique
9. Adoption des instruments de normalisation
10. Elaboration de statistiques nationales sur les infractions cybercriminelles
11. Elaboration d'une feuille de route de mise en œuvre des actions stratégiques
12. Mesurer l'impact des actions réalisées dans le cade de la stratégie adoptée.

1- Renforcement des capacités de cybersécurité

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Objectifs:

- Mise en place d'une unité nationale de sécurité des systèmes d'information de l'Etat: **se donner les moyens de défendre ses intérêts fondamentaux dans le cyberespace**

- Cette unité jouera le rôle d'une structure de renseignement, de veille et de prospective.
- Elle servira aussi de plateforme de coordination des activités liées à la cybersécurité

Autres actions

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- Disposer d'une politique de réponse aux incidents
  - Création d'un CERT national
  - Création de CERTs sectoriels (banque, universités ...)
  - Obligation de déclaration des incidents

CERT (Computer Emergency Response Team): un centre d'alerte et de réaction aux attaques informatiques, destiné aux entreprises ou aux administrations

- Définir ou adapter sa stratégie de résilience face aux cyberattaques
  - PCA (plans de continuité d'activité)
  - PRA (plans de reprise d'activité)

Développement d'une politique de Cyberdéfense

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Une importance particulière doit être accordée à la sécurité des infrastructures revêtant une importance vitale (OIV) pour le bon fonctionnement des services de l'état

- Identifier et recenser une liste d'opérateurs d'importance vitale (ou infrastructures critiques)
- Renforcer la sécurité des opérateurs d'importance vitale (transport, énergie, télécom, hôpitaux, etc.)
- élaboration d'un cahier des charges intégrant un ensemble de règles de sécurité que doivent suivre les OIV.
- obligation de déclaration des incidents
- prévoir un encadrement juridique pour ces obligations
- créer un dispositif de communication et d'alerte d'urgence entre les OIV
- Organiser, régulièrement, des contrôles sur le respect des règles de sécurité imposées aux OIV

Développement d'une politique de Cyberdéfense

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Introduction de normes dans la commande publique
- ✓ Promouvoir l'usage de la cryptologie (sur la base du service technique central du chiffre et de la sécurité des systèmes d'information
- ✓ Anticiper la cyber surveillance de masse de pays tiers
- ✓ Création d'un centre national de Cyberdéfense qui coordonnera les instruments préventifs et les démarches de cybersécurité de l'Etat

Renforcement de la lutte contre la cybercriminalité

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Renforcement des moyens (investigation, surveillance, anticipation, Etc) en adéquation avec l'évolution et la complexité des nouvelles cyber-menaces.
- ✓ Améliorer et adapter les dispositifs de prévention et de répression.
  - Améliorer le niveau de sensibilisation et de prévention contre les Cybermenaces des particuliers, des acteurs économiques et des collectivités territoriales.
- ✓ Améliorer la coordination entre les services (publics et privés) en charge des dispositifs de prévention
- ✓ Disposer en permanence d'une vision claire et actualisée de l'état des Cybermenaces en assurant une veille au profit des différents acteurs (Etat/Entreprises ...)
- ✓ Adapter les dispositifs de répression afin de prendre en charge les nouvelles infractions liées au numérique

Adapter les dispositifs de répression afin de prendre en charge les nouvelles infractions liées au numérique

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Objectifs: Mise en adéquation du corpus juridique par rapport à l'état des menaces

Exemples:

- amender le code de procédure pénale notamment sur la question touchant l'enquête sous-pseudonymes, la perquisition à distance et la captation des données. Les enquêtes sous pseudonyme ne sont pas encore suffisamment encadrées.
- réfléchir sur les réformes législatives sur la conservation rapide des données électroniques y compris les données relatives au trafic tout en assurant une protection adéquate des droits de l'homme et des libertés.
- Relecture et confrontation : mise en cohérence des textes existants (tant sur le plan national qu'international)

Formation / sensibilisation

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Sensibilisation des acteurs économiques: élaborer un plan national de sensibilisation permettant de relayer et coordonner l'action du gouvernement en matière de cybersécurité et la lutte contre la cybercriminalité.
- ✓ Envisager la sensibilisation des jeunes en proposant des interventions régulières dans les lycées et les universités. Associer le Ministère de l'Education Nationale et les représentants des Universités dans l'élaboration du plan de sensibilisation.
- ✓ Evaluation de l'offre de formation initiale et continue dans le domaine de la cybersécurité.
- ✓ Réfléchir à la création d'une filière cyber-sécurité pour disposer de compétences locales capables de répondre aux besoins des institutions publiques et privées en matière de compétences dans le domaine de la cybersécurité.

Formation

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
CEDEAO ECOWAS

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- Préparer un plan de "formation continue" destiné aux personnels du secteur public et privé, en attendant la formation de nouveaux ingénieurs et leur arrivée sur le marché du travail (4 à 5 ans pour former un ingénieur). Les formations doivent être de deux types:
  - catégorielle (Force de l'ordre, Magistrats, RSSSI, ...)
  - transversale et interdisciplinaire (Magistrat, responsable de systèmes d'information, acteurs économiques, responsable de protection des données personnelles, ..)
  - Favoriser la formation des Magistrats et des forces de l'ordre pour une bonne application des dispositions législatives et un bon déroulement des procédures d'investigation numériques

Partenariat public-privé

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Echange et partage d'informations entre les différents acteurs de la prévention et de la répression de la cybercriminalité
- ✓ Incitation de tous les acteurs à des actions communes (analyse de la menace, prévention, formation, retour d'expérience). Le secteur privé peut en effet faire bénéficier les services étatiques de son expérience et de ses moyens financiers et opérationnels.
- ✓ Définition d'un cadre d'échanges avec les fournisseurs de service internationaux (GAFA) et les acteurs institutionnels chargés de la cybersécurité et de la lutte contre la cybercriminalité.

Renforcement de la coopération régionale et internationale

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Renforcement de la coopération interministérielle et également entre les départements dépendant de la Présidence.
- ✓ Création d'une commission nationale de concertation permettant de définir un cadre d'échange régulier et de partage entre les acteurs de la cybersécurité
- ✓ Promouvoir la mobilisation des états de la sous région pour faciliter les enquêtes et éviter les "paradis cyber"
- ✓ Parfaire la coopération internationale en s'appuyant sur les mécanismes proposés par les conventions contin,entales et internationales (la Convention de Budapest / Malabo; Coopération judicaire et policière internationale, réseau 24/7, ..)

Favoriser l'instauration de la confiance numérique

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Cette confiance est réclamée par les entreprises de toutes tailles et les particuliers. Les actions proposées pour instaurer cette confiance reposent sur:
  - Protection des données personnelles et de la vie privée. Elle passe par une vigilance accrue des pouvoirs publics sur l'utilisation des données personnelles.
  - Mise en place d'un dispositif d'assistance aux victimes de cybermalveillance.
  - Favoriser la sensibilisation des citoyens sur l'usage des réseaux sociaux et des conséquences d'une exposition de leurs données personnelles sur le Net.
  - Garantir aux individus le contrôle de leurs données personnelles
  - Assurer la protection des droits et libertés fondamentaux des citoyens (Droit à la vie privée et familiale, professionnelles, confidentialité des communications, liberté d'expression, d'aller et de venir, d'association, etc.) dans la lutte contre la cybercriminalité
  - Créer un cadre d'échanges avec les fournisseurs de service internationaux (GAFA)

Adoption des instruments de normalisation

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Promouvoir des solutions techniques de protection (entreprises, développement économique, gratuité … Ex : outils de sécurisation bancaire)

Elaboration de statistiques nationales sur les infractions cybercriminelles

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ Créer, dans les secteurs publics et privés, de plateformes de signalement d'infractions cybercriminelles et favoriser le partage des informations recueillies.
- ✓ Améliorer la chaîne pénale afin d'intégrer les nouvelles infractions liées au monde numérique.
- ✓ Disposer de statistiques officielles sur les infractions cybercriminelles.
- ✓ Confier à un centre national la responsabilité de la coordination de l'élaboration des statistiques et leur publication.

Elaboration d'une feuille de route de mise en œuvre de la stratégie

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ proposer un calendrier réaliste tenant compte des acquis, des moyens et du potentiel du pays pour la réalisation des objectifs prévus dans le rapport stratégique
- ✓ avoir une visibilité sur les échéances de mise en œuvre de la stratégie
- ✓ désigner un groupe de travail interministériel permettant le suivi des réalisations et la communication au niveau national et international autour de ces réalisations

Mesurer l'impact des actions réalisées dans le cade de la stratégie adoptée

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE
CEDEAO ECOWAS

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

- ✓ création d'un groupe de travail interministériel permettant, chaque année, de vérifier et d'évaluer l'apport des actions stratégiques dans le domaine de la cybersécurité et la lutte contre la cybercriminalité (aspects techniques, économiques, sociaux et juridiques)
- ✓ adaptation de la stratégie pour prendre en compte l'évolution des cyberattaques et réduire par conséquent l'impact négatif de ces infractions

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

Merci de votre attention

Questions?