

LA TOURMENTE DE LA SOCIETE DE L'INFORMATION

LA CYBERCRIMINALITE



**FFGI
2017**

Mercredi 30 août 2017

**OUEDRAOGO François
DG ANSSI**

PLAN

- LES DANGERS DU CYBERESPACE : LA CYBERCRIMINALITE EN QUESTION ET SES ACTEURS
- DEFINITION DE LA CYBERCRIMINALITE
- LA CONVENTION DE BUDAPEST
- LA NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE

Aucune définition universelle de la cybercriminalité

La cybercriminalité apparaît comme une nébuleuse, par ses acteurs et ses procédés techniques essentiellement évolutifs.

Elle demeure une réalité difficile à cerner à cerner par les dispositifs du droit matériel.



CYBERCRIMINALITE DEFINITION

La cybercriminalité ne définit pas à elle seule une infraction, mais un ensemble d'atteintes aux biens ou aux personnes commises via l'utilisation des nouvelles technologies.

Par nouvelles technologies, on entend tout mode de communication, à savoir l'Internet mais également la téléphonie mobile, peu importe le protocole utilisé.

Cette notion de cybercriminalité peut concerner les infractions relatives au contenu qu'il s'agisse de textes (insultes, propos négationniste ou xénophobes) ou d'images (fichiers pédo – pornographique).

Elle peut concerner également les atteintes à la propriété intellectuelle, qui constitue un véritable fléau pour l'économie.

Parfois, l'utilisation directe des NTICS qui peut constituer à elle seule une infraction.

CYBERCRIMINALITE

Infractions pour lesquelles les Technologies de l'Information et de la Communication (TIC) sont l'objet même du délit

Infractions pour lesquelles les nouvelles technologies sont un moyen ou un support

Les technologies utilisées déterminent les infractions

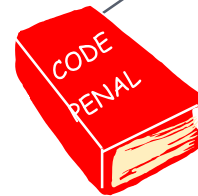
Infractions classiques de droit commun (crimes et délits)



Infractions liées à la téléphonie cellulaire

Infractions liées à la télécommunication

Infractions informatiques



Infractions prévues par des textes spécifiques (presse)

Infractions prévues par le code pénal

CYBERCRIMINALITE DEFINITION

CYBERDEFENSE
Domaine Etatique ,
ANSSI

CYBERSECURITE,
ANSSI , CIRT-BF
sécurité des SI ,
entreprises

CYBERCRIMINALITE
Domaine du judiciaire

La **Convention sur la cybercriminalité**, aussi connue comme la **Convention de Budapest sur la cybercriminalité** ou **Convention de Budapest**, est le premier traité international qui tente d'aborder les crimes informatiques et les crimes dans Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations. Il a été rédigé par le Conseil de l'Europe avec la participation active d'observateurs délégués du Canada, du Japon et de la Chine.

À la fin d'août 2011, plusieurs pays européens avaient signé le traité.

CYBERCRIMINALITE DEFINITION

En rapport avec la pratique au niveau international, le choix a été de fait de considérer les menaces en 09 groupes conformément à **la convention de BUDAPEST.**

NO	GROUPES DE MENACES
1	Accès illégal
2	Interception illégale
3	Atteinte à l'intégrité des données
4	Atteinte à l'intégrité du système
5	Abus de dispositifs
6	Falsification informatique
7	Fraude informatique
8	Pornographie enfantine
9	Atteinte propriété intellectuelle et droits connexes

Convention de Budapest

- **système informatique**
- **données informatiques**
- **fournisseur de services**
- **données relatives au trafic**

Convention de Budapest

Article 1 – Definitions

- A** l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;
- B** l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
- C** l'expression «fournisseur de services» désigne:
- I.** toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et
 - II.** toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.
- D** «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent

Convention de Budapest

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 2 – Accès illégal

Sénégal - Article 431-8 :

Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique, sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

Est puni des mêmes peines, celui qui se procure ou tente de se procurer frauduleusement, pour soi-même ou pour autrui, un avantage quelconque en s'introduisant dans un système informatique.



LA CYBERCRIMINALITE EN CONCLUSION

UNE AFFAIRE LUCRATIVE

MOTIFS	ACTEURS	MONTANTS
POLITIQUE	Etats. Organisations terroristes. Nationalistes.	< 200 Milliards d'Euros.
PROFIT	Criminalité organisée et internationale. Terroristes. Economie.	Dizaines de Milliers. Millions d'Euros.
INDIVIDUEL	Extrémistes. Joueurs frustrés. désœuvrés.	Millions Milliers d'Euros

NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE

BATIR UN ECHOSYSTEME CYBERSECURITAIRE

CARACTERISTIQUES DE SECURITE	TYPE DE MESURE DE SECURITE
<i>Disponibilité</i>	<ul style="list-style-type: none">- Dimensionnement- Redondance- Procédures d'exploitation et de sauvegarde
<i>Intégrité</i> <i>Confidentialité</i>	<ul style="list-style-type: none">- Chiffrement- Contrôle d'accès- Sécurité physique- Authentification- Détection, prévention d'intrusion, virus- Contrôle d'erreur, de cohérence
<i>Non Répudiation</i> <i>Authenticité</i> <i>Imputabilité</i> <i>Conformité aux lois</i>	<ul style="list-style-type: none">- Certification- Enregistrement, traçabilité- Signature électronique- Mécanismes de preuve
<i>Fiabilité</i> <i>Durabilité</i> <i>Continuité</i>	<ul style="list-style-type: none">- Conception- Performances- Ergonomie- Qualité de service- Maintenance opérationnelle

NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE

ETABLIR DES SERVICES TECHNIQUES

<i>Services réactifs</i>	<i>Services proactifs</i>	<i>Gestion de la qualité de la sécurité</i>
Alertes et avertissements. Traitement des incidents Analyse des incidents. Traitement des vulnérabilités. Traitement des artefacts.	Annonces. Veille technologique. Audits ou évaluations de la sécurité. Configuration et maintenance de la sécurité. Développement/ recherche d'outils de sécurité. Services de détection des intrusions. Diffusion d'informations relatives à la Sécurité.	Analyse des risques Continuité de l'activité et reprise après sinistre. Consultance en matière de sécurité. Sensibilisation Éducation/formation. Évaluation ou certification des produits.

NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE



Au niveau International

- Réseau FIRST, IMPACT
- Organisations UIT, FRANCOPOL

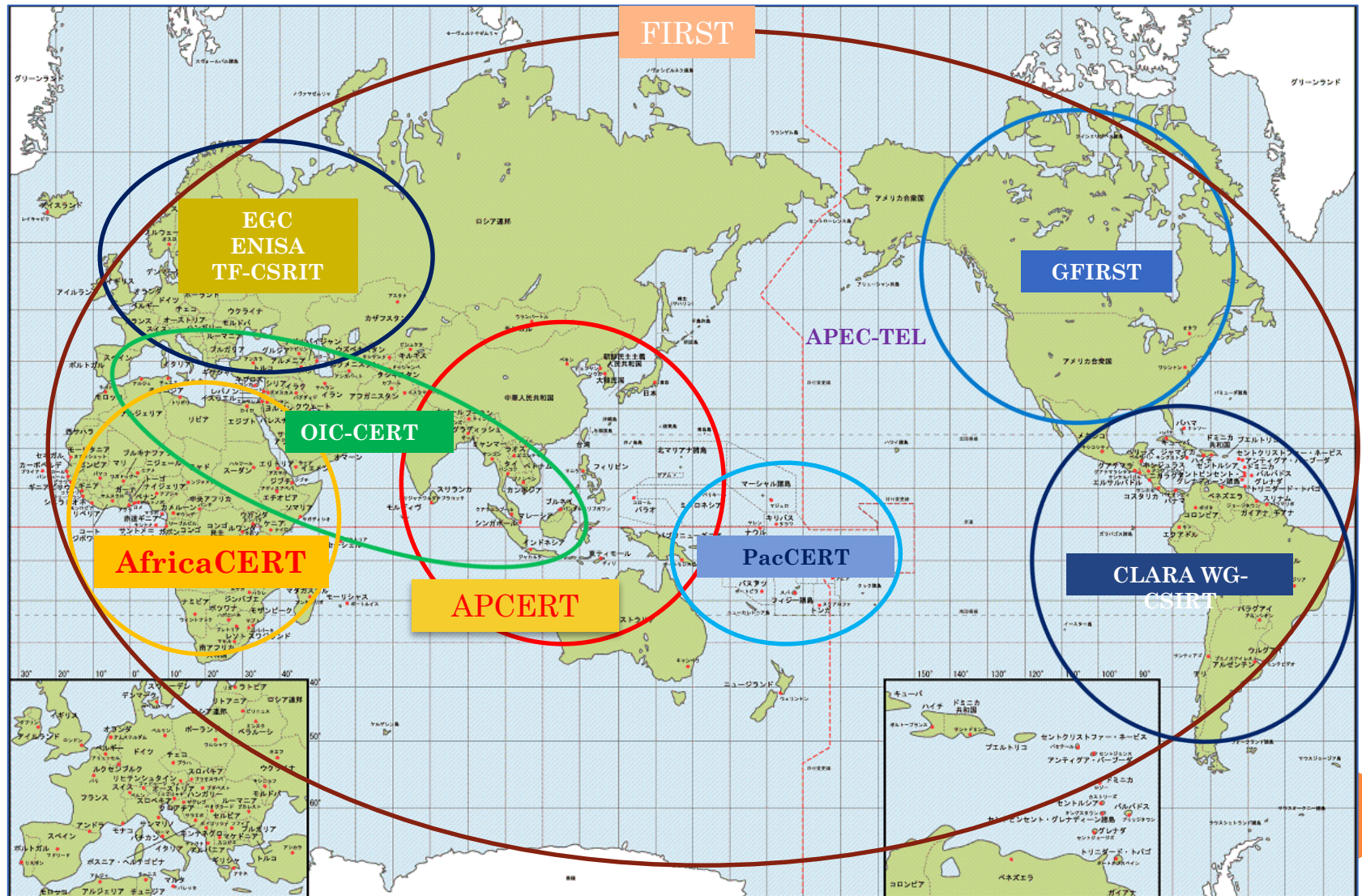
Au niveau Régional

- Réseaux CERT, CSIRT : AfricaCERT, APCERT, PacCERT etc.

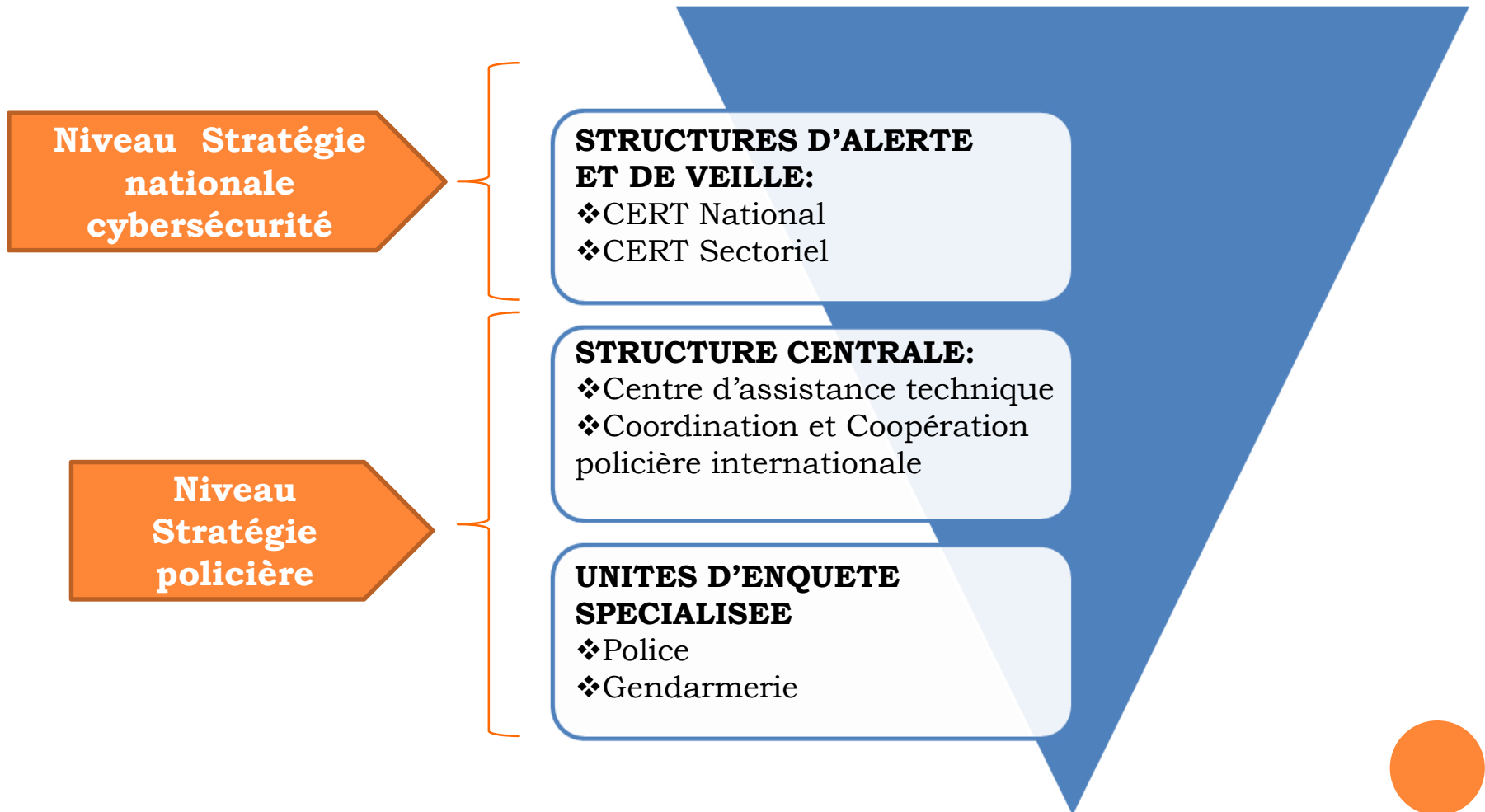
Au niveau National

- CSIRT et les Réseaux des UAGI
- Etat, les Infrastructures critiques
- La Gendarmerie, la Police

NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE



NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE



NECESSITE D'UNE REPONSE GLOBALE ET COORDONNEE

- ❖ Mutualiser les moyens et les compétences;
- ❖ Echanger les information en temps réel ;
- ❖ Assurer la veille en matière de cybersécurité et de lutte contre la cybercriminalité.

Ministère de l'Administration Territoriale et de la Sécurité



**Séminaire de formation appliquée de FRANCOPOL
sur la cybercriminalité**

OUAGADOUGOU du 25 février au 1^{er} mars 2013.























Calculons son évolution temporelle en utilisant l'équation de Schrödinger (2.36) et sa complexe conjuguée :

$$\begin{aligned}\frac{\partial}{\partial t}\rho(r,t) &= \psi^* \frac{\partial \psi}{\partial t} + \frac{\partial \psi^*}{\partial t} \psi \\ &= \frac{1}{i\hbar} \psi^* \left(-\frac{\hbar^2}{2m} \Delta \psi + V(r) \psi \right) - \frac{1}{i\hbar} \left(-\frac{\hbar^2}{2m} \Delta \psi^* + V(r) \psi^* \right) \psi \\ &= \frac{i\hbar}{2m} (\psi^* \Delta \psi - \psi \Delta \psi^*) \quad .\end{aligned}\tag{3.25}$$



POUR VOTRE AIMABLE ATTENTION !