CHAPITRE V : La Cybercriminalité : Principes, Typologie et Modes Opératoires.

I. INTRODUCTION

La criminalité se développe aujourd'hui sur un terrain moins risqué et plus fertile que celui du monde réel car l'anonymat y est pratiquement assuré pour qui sait s'y prendre et le dispositif policier s'il n'est pas inexistant est très insuffisant pour surveiller le milliard d'individus qui se retrouvent sur le net. Pourtant cet espace virtuel est devenu aussi indispensable à l'économie des entreprises et aux relations entre le citoyen et son administration que le téléphone et le courrier papier.

Le monde devient instable et dangereux. Les échanges se mondialisent et ne connaissent, sur la toile, pas de frontières. Dans ce monde virtuel où tout est à craindre, les amis de nos amis peuvent être nos pires ennemis et les clients de nos partenaires peuvent être nos concurrents. La montée du terrorisme et une situation économique très perturbée engendrent un impérieux besoin de sécurité.

Connaître les menaces qui pèsent sur les systèmes d'information, comprendre les mesures de sécurité à mettre en place et déjà un premier pas est franchi vers un monde Internet plus sûr, un monde où l'économie et la culture pourront se développer harmonieusement, malgré les pièges et les coups de boutoirs des hackers qui foisonnent sur la toile.

Les vulnérabilités et la maîtrise insuffisante des technologies du numérique leur confèrent un certain niveau d'insécurité. Cet état d'insécurité est largement exploité par les acteurs du monde criminel. De plus, chaque technologie est porteuse de potentialités criminelles et offre des opportunités pour réaliser des infractions. L'Internet n'échappe pas à cette règle et le monde criminel a investi le cyberespace.

II. Définitions et Notions de crime informatique et de cybercrime.

A) Le crime Informatique et le Cybercrime.

Infraction informatique

L'Organisation pour la Coopération et le Développement Economique (**OCDE**) a défini en 1983 **l'infraction informatique** comme étant tout comportement illégal, immoral ou non autorisé qui implique la transmission et/ou le traitement automatique de données.

Un crime informatique

Un crime informatique (*computer-related crime*) est un délit pour lequel un système informatique est l'objet du délit et/ou le moyen de le réaliser. C'est un crime lié aux technologies du numérique qui fait partie de la criminalité en col blanc.

Cybercrime (*cybercrime*)

Le cybercrime (*cybercrime*) est une forme du crime informatique qui fait appel aux technologies de l'Internet pour sa réalisation. Cela concerne tous les délits réalisés dans le cyberespace.

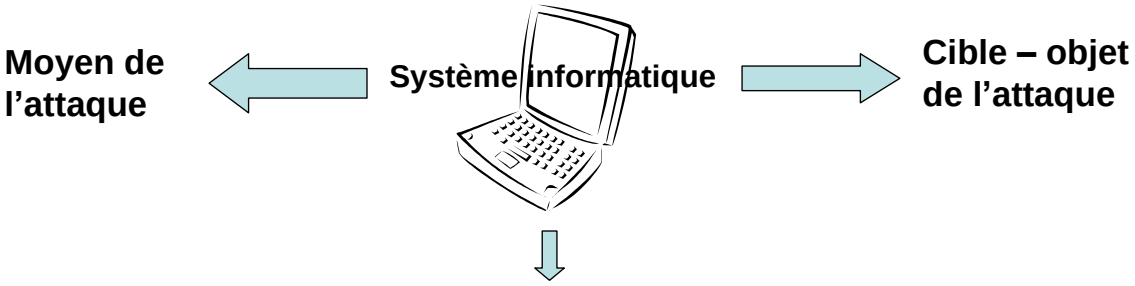
Cyberdélit

Un cyberdélit désigne toute activité mettant en jeu des ordinateurs ou des réseaux en tant qu'outil, cible ou lieu d'une infraction. Toute activité assistée par ordinateur qui est *illégale ou considérée comme illicite* par certaines parties et peut être menée *en utilisant les réseaux électroniques mondiaux*.

Le monde virtuel confère au crime la capacité à être automatisé, autorisant une réalisation à grande échelle (**cyberépidémie**), permettant d'être commis à distance *via* les réseaux (ubiquité du criminel, dans le temps et dans l'espace) et avec éventuellement des effets à retardement

Les technologies de l'Internet facilitent toute sorte d'infractions (vol, sabotage d'informations, atteintes au copyright, au droit d'auteur, à la violation du secret professionnel, de l'intimité numérique, de la

propriété intellectuelle, dissémination de contenus illégaux, attaques concurrentielles, espionnage industriel, atteinte aux droits des marques, diffusion de fausses informations, dénis de service, fraudes diverses, etc.).



•Criminalité en col blanc
•Délit commis à distance via des réseaux, caché derrière un écran •Ubiquité du criminel dans l'espace et dans le temps
•Savoir-faire criminel embarqué dans le logiciel
•Commission automatisée des délits, à grande échelle

Caractéristiques du crime informatique

B) Cybercriminalité : Notions de base et Types d'Infractions.

1. Définitions

Cybercriminalité : ensemble des infractions s'effectuant à travers le cyberspace 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 au Cameroun).***

La Cybercriminalité : « Ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication, ainsi que celles dont la commission est facilitée ou liée e à l'utilisation de ces technologies ». ***Convention de Budapest du 23 novembre 2001***

Selon **l'O.N.U.,** la « **Cybercriminalité** » doit recouvrir « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent », et dans une acception plus large « tout fait illégal commis au moyen d'un système ou d'un réseau informatique ou en relation avec un système informatique ».

Selon le ministère de l'Intérieur français, la **cybercriminalité** recouvre « l'ensemble des infractions pénales susceptibles d'être commises sur les réseaux de télécommunications en général et plus particulièrement sur les réseaux partageant le protocole **TCP-IP** , appelés communément l'Internet»

2. Les Types d'Infractions

La **cybercriminalité** regroupe trois types d'infractions :

- les infractions spécifiques aux technologies de l'information et de la communication : parmi ces infractions, on recense les atteintes aux systèmes de traitement automatisé de données, les traitements non autorisés de données personnelles (comme la cession illicite des informations personnelles), les infractions aux cartes bancaires, les chiffrements non autorisés ou non déclarés ou encore les interceptions ;
- les infractions liées aux technologies de l'information et de la communication : cette catégorie regroupe la pédopornographie, l'incitation au terrorisme et à la haine raciale sur internet, les atteintes aux personnes privées et non aux personnages publics, les atteintes aux biens ;
- les infractions facilitées par les technologies de l'information et de la communication, que sont les escroqueries en ligne, le blanchiment d'argent, la contrefaçon ou toute autre violation de propriété intellectuelle.

3. Les Objectifs de La Convention sur la cybercriminalité de Budapest

La Convention sur la cybercriminalité du **Conseil de l'Europe**, aussi connu sous le nom de **Convention de Budapest** est le seul instrument international juridiquement contraignant conçu expressément pour lutter contre la cybercriminalité, et qui sert de lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre pour la coopération internationale contre la cybercriminalité parmi les États Parties.

La **convention sur la cybercriminalité de 2001** poursuit trois objectifs déterminés :

- l'harmonisation des législations des États signataires ;
- la modernisation de ces législations, notamment en matière procédurale ;
- l'amélioration de la coopération internationale en matière d'extradition et d'entraide répressive.

a)

Le premier axe est l'harmonisation des législations nationales en ce qui concerne la définition des infractions répertoriées par la Convention. Il s'agit d'incriminer quatre séries d'infractions qui sont :

- les infractions informatiques : falsification et fraude informatique ;
- les infractions de contenu : la pornographie enfantine. Le protocole additionnel inclut la propagation via Internet d'idées racistes et xénophobes ;
- les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes : le partage non autorisé via Internet des œuvres protégées ;
- les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes : accès illégal, interception illégale, atteinte à l'intégrité des données ou des systèmes.

b)

Le deuxième axe, d'ordre procédural, définit les moyens d'enquêtes et de poursuites pénales les mieux adaptés à la mondialisation du réseau Internet. La Convention prévoit des règles pour garantir les droits des individus, mais aussi pour faciliter la conduite d'enquête. On peut citer les règles régissant :

- la conservation des données stockées,
- la conservation et la divulgation rapide des données relatives au trafic,
- la perquisition des systèmes informatiques,
- la saisie de données informatiques, la collecte en temps réel des données relatives au trafic,
- l'interception de données relatives au contenu.

c)

Le troisième axe concerne la mise en place d'un système rapide et efficace de coopération internationale. La Convention sur la cybercriminalité prévoit des formes d'entraide correspondant aux pouvoirs définis préalablement par la Convention. Ces conditions sont exigées afin que les autorités judiciaires et les services de police d'un État membre puissent agir pour le compte d'un autre État dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes ni de perquisitions transfrontalières. En outre, toute donnée obtenue devrait être rapidement communiqué à l'État intéressé.

C) Facteurs favorisant l'expression de la criminalité via l'Internet

1) Monde virtuel et dématérialisation

La dématérialisation des transactions, les facilités de communication associées aux solutions de chiffrement, de sténographie et d'anonymat, autorisent des liaisons entre criminels de différents pays sans contact physique, de manière flexible et sécurisée en toute impunité. Les fins malveillantes sont : usurpation d'identité, leurre, accès indus, exploitation frauduleuse de ressources, infection, détérioration, destruction, modification, divulgation, vol de données, chantage, extorsion, racket, déni de service, etc.

2) Mise en réseau des ressources

La généralisation de la mise en réseau des ressources informatiques et informationnelles, font qu'elles deviennent des cibles attrayantes pour la réalisation de crimes économiques via les nouvelles technologies. La disponibilité d'outils d'exploitation des failles et vulnérabilité des systèmes, de bibliothèques d'attaques et de logiciels qui capitalisent le savoir-faire criminel dans un programme, facilite la réalisation des attaques informatiques. Les fins malveillantes sont : L'usurpation d'identité électronique, les possibilités d'anonymat ou la prise de contrôle d'ordinateurs par exemple.

3) Disponibilité d'outils et existence de failles

La disponibilité d'outils d'exploitation des failles et vulnérabilité des systèmes, de bibliothèques d'attaques et de logiciels qui capitalisent le savoir-faire criminel dans un programme, facilite la réalisation des attaques informatiques.

4) Vulnérabilité et défaillance

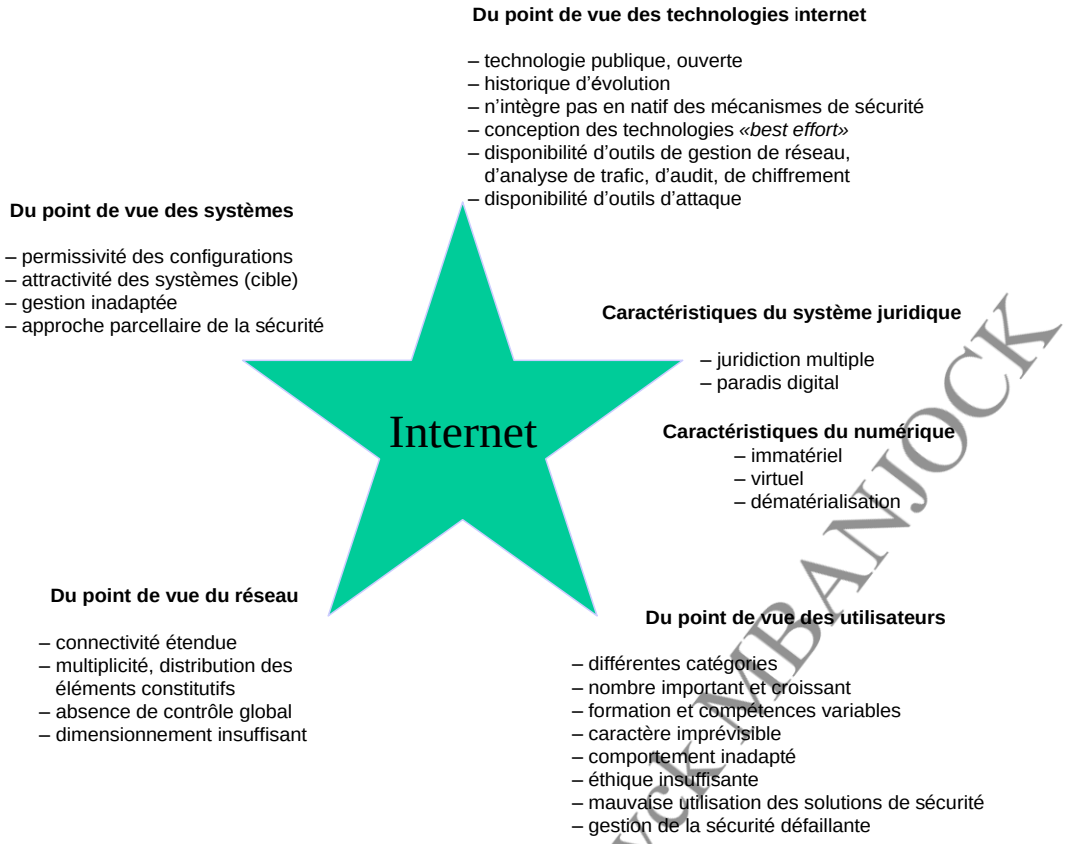
La criminalité tire partie des vulnérabilités et défaillances organisationnelles et techniques de l'Internet, de l'absence d'un cadre juridique harmonisé entre les Etats et d'un manque de coordination efficace des polices. Il peut s'agir : (blanchiment d'argent, chantage, extorsion, etc.) ou générer de nouveaux types de délits à partir des technologies du numérique: intrusion dans des systèmes, vol de temps processeur, vol de code source, de bases de données, etc.

5) Difficulté à identifier l'auteur d'un délit

Le crime informatique est un crime sophistiqué, réalisé le plus souvent au niveau international avec parfois un effet à retardement. Les traces laissées dans les systèmes sont immatérielles et difficiles à collecter et à sauvegarder. Il se pose alors la question de leurs saisies lors d'une perquisition informatique. Les questions suivantes, montrent à quel point la notion de preuve numérique est difficile à établir:

- comment identifier les données pertinentes?
- comment les localiser?
- comment les sauvegarder?
- comment constituer une preuve recevable auprès d'un tribunal?
- comment récupérer des fichiers effacés?
- comment prouver l'origine d'un message?

- comment remonter jusqu'à l'identité d'une personne sur la base uniquement d'une trace numérique du fait qu'il est difficile d'établir une correspondance certaine entre une information numérique et son auteur (dématérialisation) et de l'usurpation d'identité fréquente?
- quelle est la valeur d'une trace numérique en tant que preuve contribuant à établir la vérité auprès d'un tribunal (notion de preuve numérique) sachant que les supports de mémorisation sur lesquelles des traces ont été recueillies sont faillibles (les notions de date et d'heure sont variables d'un système informatique à l'autre et aisément modifiables).
- etc.



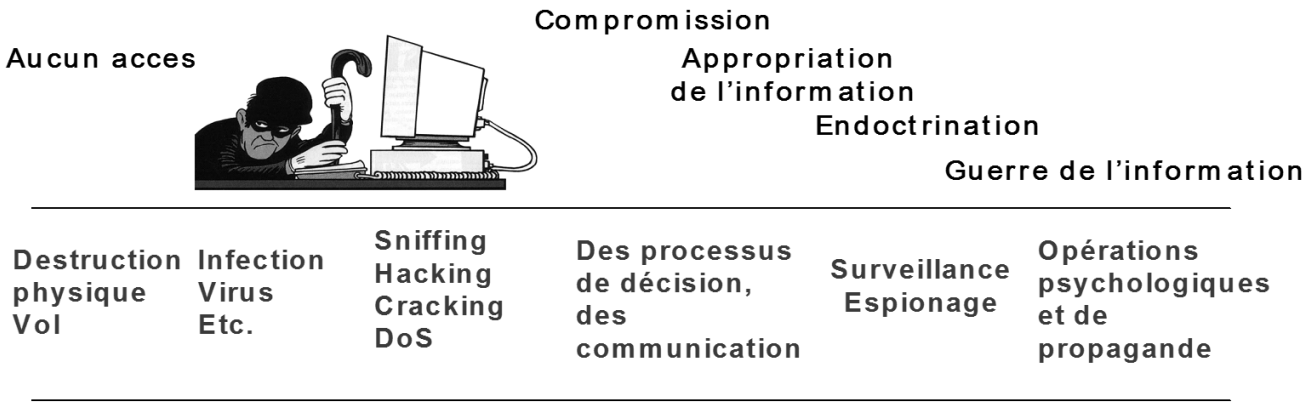
Principales caractéristiques du monde de l'Internet exploitées à des fins criminelles

6) Aterritorialité et paradis numériques

Le manque de régulation internationale et de contrôle, l'inefficacité de la coopération internationale en matière d'investigation et de poursuites judiciaires font que l'Internet offre une couche d'isolation protectrice aux criminels.

A l'heure actuelle, aucune réponse correcte tant sur le plan juridique que technique est apportée pour maîtriser les différents délits favorisés par l'Internet tels que:

- l'industrie parallèle et très organisée de la copie à la chaîne de logiciels, de films, de musique, etc., qui a pris dans le cyberespace une dimension sans précédent;
- les atteintes au copyright, droits d'auteur, la violation du secret professionnel, de l'intimité numérique ou de la propriété intellectuelle;
- les atteintes à la propriété, l'appropriation illégale de la propriété d'autrui, l'endommagement, la destruction de la propriété d'autrui ou l'immixtion dans la propriété d'autrui (notion de violation de domicile virtuel);
- la dissémination de contenus illégaux;
- attaques concurrentielles, espionnage industriel, atteinte aux droits des marques, diffusion de fausses informations, dénis de service commandités par des concurrents.



Crime sophistiqué
réalisé au niveau international
Effet à retardement
Trace immatérielle difficile à collecter
Anonymisation
Usurpation d'identité
Dématérialisation
Relais d'attaques
Multiples intermédiaires
Etc.

Coopération internationale?

Identification des malveillants?

Difficulté à identifier un malveillant

III. Les Cyberdélinquants

Sécuriser un système d'information nécessite de connaître contre qui l'on doit se protéger. De nos jours, on distingue deux grands types de cyberdélinquants à savoir : d'une part, les professionnels dont les activités sont directement rémunératrices et, d'autre part, les amateurs, généralement animés par un fort besoin de reconnaissance sociale.

A) Les Professionnels

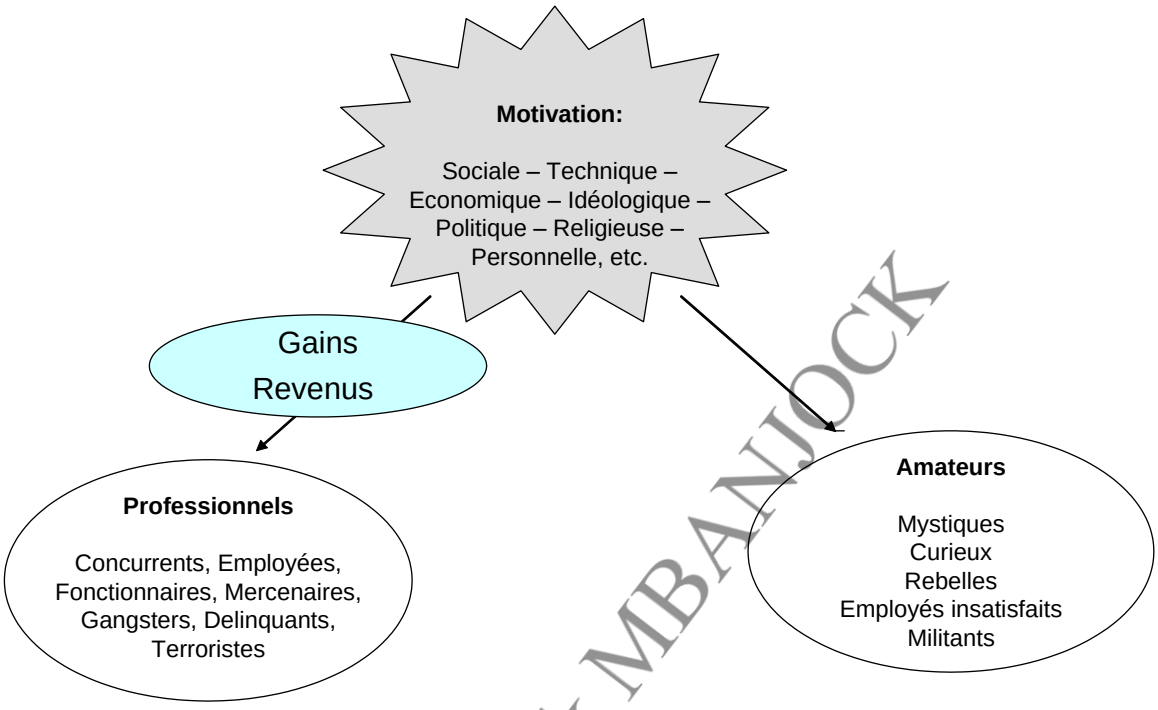
Les professionnels sont généralement:

- des concurrents directs de l'organisation visée;
- des fonctionnaires au service de leur Etat;
- des mercenaires (pouvant agir aussi bien pour le compte d'institutions privées que publiques);
- des truands de toutes sortes.

B) Les Amateurs

Parmi les amateurs, se reconnaissent:

- les techniciens, successeurs des premiers passionnés, ces hackers des premiers âges dont la motivation essentielle était le désir de maîtriser toujours mieux les technologies;
- les curieux;
- les immatures: souvent appelés «script-kiddies» ou «kiddiots».
- les psychopathes;
- les militants, mus par idéologie ou religion, qui sont d'ailleurs souvent à cheval entre amateurisme et professionnalisme).



IV. Les Programmes indésirables ou malveillants

1) Le Spam

Le ***spam*** est un envoi massif de messages électroniques non sollicités dont la finalité est à l'origine commerciale et publicitaire afin d'inciter les internautes à commander un produit ou un service.
Le phénomène de *spam* peut ressembler à une attaque par bombardement, inondation de messages (*e-mail bombing*) entraînant une surcharge inconsidérée des serveurs de messagerie, des boîtes à lettres des utilisateurs et des désagréments. Cela peut se réaliser par l'inscription de l'utilisateur à son insu à des listes de diffusion d'information (*list linkink*). Le *spam* est maintenant utilisé pour propager des programmes malveillants.

2) Les Programmes malveillants

D'après les principaux observateurs de la sécurité informatique que cela soit le **CERT** (*Computer Emergency Response Team), Le* **FBI**, le **CLUSIF** (Club de la Sécurité des Système d'Information Français), il s'agit des logiciels suivants:

- Les **téléchargeurs** et **implanteurs** (**downloaders**) qui permettent le téléchargement de données (accès à distance et chargement de programmes ou récupération de données);
- Les **keyloggers** qui sont des enregistreurs de frappe, renifleurs de clavier qui capturent les informations saisies au clavier par l'utilisateur. Il existe également des périphériques matériels (**keyloggers** matériels), indétectables par les logiciels qui enregistrent les données;
- Les **bot-robots** qui sont des programmes permettant la prise de contrôle à distance de systèmes afin de former un réseau d'attaques caché. De 25-50 nouveaux robots sont découverts chaque jour. Ils servent de relais de spamming, de phishing ou pour distribuer des adwares.
- Les **logiciels publicitaires** (***adware – advertising software***) qui permettent entre autres la personnalisation des démarches commerciales;
- Les **logiciels espions** (**spyware – spying software**) qui, comme leur nom l'indique, enregistrent des données à l'insu de l'utilisateur. (*Selon l'éditeur de logiciels Webroot INC. plus de 100 000 différents spywares sont présents sur le net et plus de 300 000 sites Internet hébergent de tels logiciels. Un PC connecté sur l'Internet possède en*

moyenne 28 spywares installés à l'insu de son utilisateur. Plus de 80% des ordinateurs d'une entreprise contiennent au moins un spyware. Ces programmes sont à l'origine de 70% des attaques.)

- les virus et les dérivés (vers, cheval de Troie, bombe logique)

Les **virus** sont des programmes malveillants introduits dans un système à l'insu des utilisateurs, qui possèdent la capacité de se dupliquer soit à l'identique, soit en se modifiant (virus polymorphe), de porter atteinte aux environnements dans lequel ils s'exécutent et de contaminer les autres avec lesquels ils sont en relation. Différents types de virus sont distingués en fonction de leur signature, de leur comportement, de leur type de reproduction, d'infection, de dysfonctionnements induits, etc.

Types de Virus	Caractéristiques
Vers	Les vers sont des programmes qui se diffusent à travers le réseau, le plus souvent indépendamment d'une intervention humaine et ont souvent comme finalité de consommer de manière excessive des ressources (mémoire, bande passante) portant atteinte ainsi au critère de disponibilité ou favorisant la prise de contrôle à distance des systèmes infectés.
Cheval de Troie	Les programmes malveillants qualifiés de chevaux de Troie (***Trojan horse***) sont introduits subrepticement, souvent sous couvert de programmes anodins ou d'aide, dans des systèmes pour en prendre le contrôle afin de réaliser le vol de temps processeur, l'altération, la modification, la destruction des données et programmes, des dysfonctionnements, des écoutes illicites, mais aussi pour réaliser d'autres malveillances et servir de relais à des attaques ultérieures.
Bombe logicielle	Les bombes logicielles (***logical bomb***) sont des virus qui s'activent lors de la réalisation d'évènements particuliers (date anniversaire par exemple) pour porter atteinte au système dans lequel il se trouve.

3) Les Tendances

De nos jours, les virus n'ont plus pour objectif principal la destruction massive et gratuite de données. Ils deviennent pragmatiques et sont orientés vers la recherche de gains. Leur finalité est et leur capital embarqué leur permet de réaliser des fraudes. Les virus deviennent des vecteurs de réalisation de la criminalité financière au service le plus souvent, de la criminalité organisée et constituent des moyens d'enrichissement considérable pour leur auteur.

V. Les Principaux délits favorisés via l'Internet

1) Escroquerie, espionnage et activités de renseignement, trafics divers, chantage

De manière générale, le service de mise en relation offert par le réseau Internet favorise l'ensemble des trafics possibles que cela soit relatif au trafic d'armes ou à celui d'êtres humains, aux escroqueries (atteintes contre des biens, atteintes à des systèmes et infrastructures informatiques, vol de données, atteintes au droit d'auteur, etc.).

Les manifestations les plus redoutables de ces délits sont :

- **Carding ;**
- **Skimming ;**
- **Phishing ;**
- **Escroqueries sur Internet ;**
- **Escroqueries à la téléphonie.**

a) Le carding : un marché mondialisé

Au sens général, il s'agit du piratage de cartes bancaires par diverses techniques matérielles, logicielles ou subversives aux fins d'obtenir et de revendre les données de cartes bancaires, de s'en servir pour effectuer des achats frauduleux, au préjudice du porteur légal.

3 étapes :

- Coding: piratage de données, Générateur automatique de numéros,
- Vending: revente des données, Achat et revente de numéros de cartes bancaires, pistes magnétiques, informations des titulaires,
- Cashing: échanges financiers, escroqueries et circuits de (blanchiment d'argent, Effectuer des achats réels (web, tels télévente, en vente, boutique……), Générer des transactions d'achats virtuels, Retrait d'argent et échanges financiers.

b) Cashing ou escroqueries et circuit de blanchiment

Ensemble des dispositifs pour récupérer l'argent des comptes porteurs, utiliser et blanchir les sommes transférées, et Utilisation de dispositifs financiers pour rémunérer les fournisseurs de données bancaires.

c) Le **skimming** : une criminalité à l'échelle européenne qui consiste au piratage des **DAB** et **DAC**, en passant par la création de numéros de carte bancaire parfaitement valides bien que ne correspondant à aucun compte réel.

2) Atteintes aux personnes

L'Internet permet à des communautés virtuelles clandestines, de se constituer autour de pratiques punies par la loi. Il peut s'agir de pornographie, de pédophilie, ou de ***snuff movies*** (films montrant des scènes de violence et de torture réalisées sur des victimes, pouvant conduire à la mise à mort des personnes maltraitées). Atteinte à la vie privée, à la représentation de la personne, au secret professionnel, aux droits de la personne résultant des fichiers ou traitements informatiques.

3) La Contrefaçon

Les infractions au code de la propriété intellectuelle peuvent être nombreuses: contrefaçon d'une œuvre de l'esprit (y compris logiciel), de dessin, d'un modèle, d'une marque, etc.

4) La Manipulation de l'information

La manipulation peut prendre diverses formes, comme par exemple la diffusion de documents internes d'une entreprise de manière à provoquer sa déstabilisation, envois de courriers électroniques appelant les destinataires à réaliser des dons monétaires sur des sites contrefaits, etc.

Crimes et délits contre les personnes – Atteintes à la personnalité – Atteinte à la vie privée – Atteinte à la représentation de la personne – Dénonciations calomnieuses – Atteinte au secret professionnel – Atteinte aux droits de la personne résultant des fichiers ou des traitements informatiques – Atteintes aux mineurs, etc.
Crimes et délits contre les biens – Escroquerie – Atteintes aux systèmes informatiques – Infraction de Presse
Provocation aux crimes et délits – Apologie des crimes contre l'humanité – Apologie et provocation au terrorisme – Provocation à la haine raciale – Négationisme – Diffamation – Injures
Infraction au code de la propriété intellectuelle – Contrefaçon d'une œuvre de l'esprit (y compris logiciel) Contrefaçon d'un dessin ou d'un modèle – Contrefaçon de marques – Participation à la tenue d'une maison de jeux de hasard (cybercasino)

VI. La Cybercriminalité au Cameroun

A) Les Aspects Théoriques

1) Cadre juridique.

Bien que le Cameroun ne soit pas signataire de la Convention de Budapest, le droit camerounais possède une loi spécifique à la cybercriminalité, la Loi n°2010/012 du 21 décembre 2010 relative à la cybersécurité et à la cybercriminalité.

Cette loi n°2010/012 complétée par la loi relative au droit d'auteur permet au droit camerounais de comprendre une partie des toutes incriminations informatiques présentes dans la Convention de Budapest (8/10).

La Convention de l'Union Africaine (UA) sur la Cybersécurité et la protection des données à caractère personnel a été adoptée. Le Cameroun n'a cependant pas encore ratifié la convention.

2) Moyens procéduraux.

Certains moyens procéduraux présents dans la Convention de Budapest trouvent un parallèle dans le droit camerounais permettant ainsi de prendre des mesures pour conserver les données de trafic ou les données stockées, intercepter des données, mettre sur écoute téléphoniques (4/6).

Forces judiciaires. Le Cameroun ne possède pas de cellule cybercriminalité. Il existe en revanche une **Agence Nationale des Technologies de l'Information et de la Communication** (**ANTIC**).

3) Coopération internationale.

Les dispositions relatives à la coopération internationale présentes dans la Convention de Budapest trouvent un parallèle dans le droit camerounais grâce à une loi relative à la cybersécurité et à la cybercrimialité.

Le Cameroun dispose d'accords bilatéraux relatifs à l'entraide en matière pénale et à l'extradition.

Le Cameroun est membre d'une organisation internationale ITU-IMPACT.

- INTERPOL
- BCN (Bureau Central National)
- **OCLCTIC** (Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication)

4) Stratégie nationale.

Le Cameroun ne s'est pas encore doté d'une stratégie de cybersécurité.

Le Cameroun possède également un **CERT** national

Le Cameroun n'a pas encore de forces armées et services non gouvernementaux relatives à la lutte contre la cybercriminalité.

5) Partenariat.

Le Cameroun n'a pas encore développé de partenariats public-privé pratique et régulier et automatisé.

A LA UNE

Lors du séminaire débit décembre 2016 sur l'Information et la sensibilisation à la cybersécurité, l'ANTIC réaffirme ses travaux : couvrir trois grands axes que sont : l'audit de sécurité, la veille sécuritaire, et la certification électronique au Cameroun.

B) Initiatives nationales, sous régionales et Chantiers en cours

1. **Centre d'Alerte et de Réponses aux Incidents Cybernétiques (CIRT)**
   Centre de Cyber Défense

✓ **Cyber défense/ Sécurité**

- **Sécurité des systèmes d'information et de communication**
  - Protection, anticipation, prévention
  - Réaction et réponses coordonnées

- **Assurer la sécurité d'un cyber espace prédéfini**
  - Centré sur les actifs d'un territoire et sur ses interdépendants avec son environnement avec la mise en œuvre de mesures défensives
- **Via un centre des opérations de Cyber sécurité**
  - Citoyens, entreprises, infrastructures vitales, administrations
  - Défense et souveraineté nationales.

✓ **Centre des opérations de cyber sécurité**

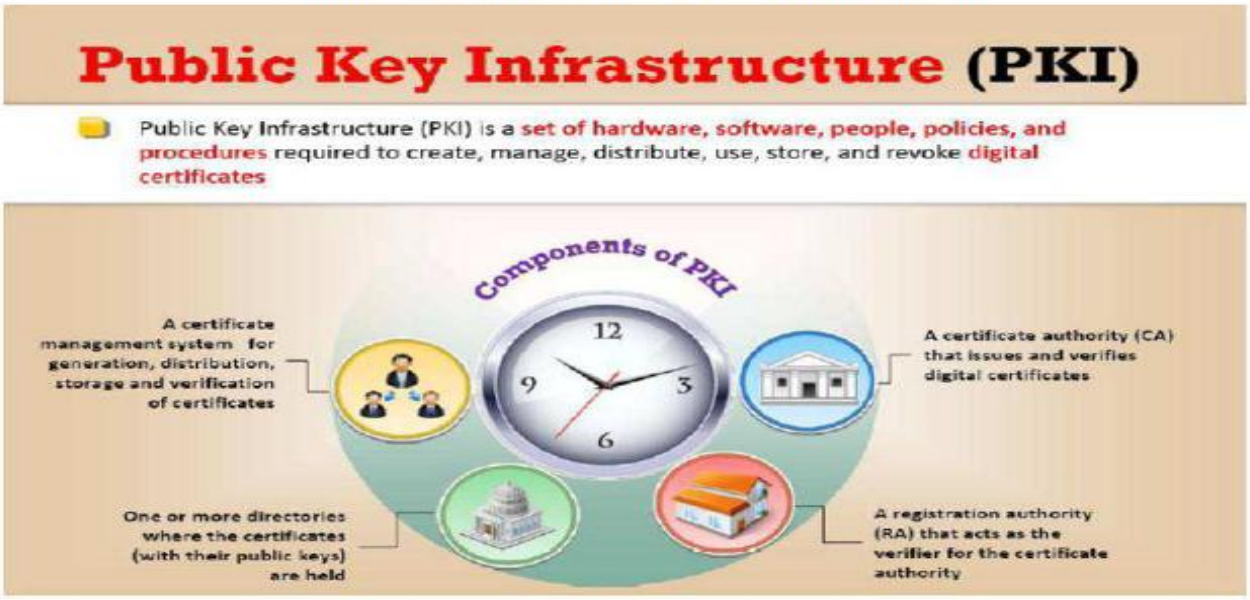
- **Un service de veille et de renseignement**
  - Domaines public et privé
  - Domaine défense
- **Un service de détection et d'alerte**
  - En cas d'évolution de la menace
  - En cas d'émergence de vulnérabilité impactant
  - En cas d'incident
- **Un service de coordination des réactions**
- **Un service de planification des réactions**
  - Assure la mise en œuvre des mesures de réponse aux attaques
  - Assure la mise en œuvre des mesures de réponse aux incidents
  - Elève le niveau de résilience par des exercices réguliers.

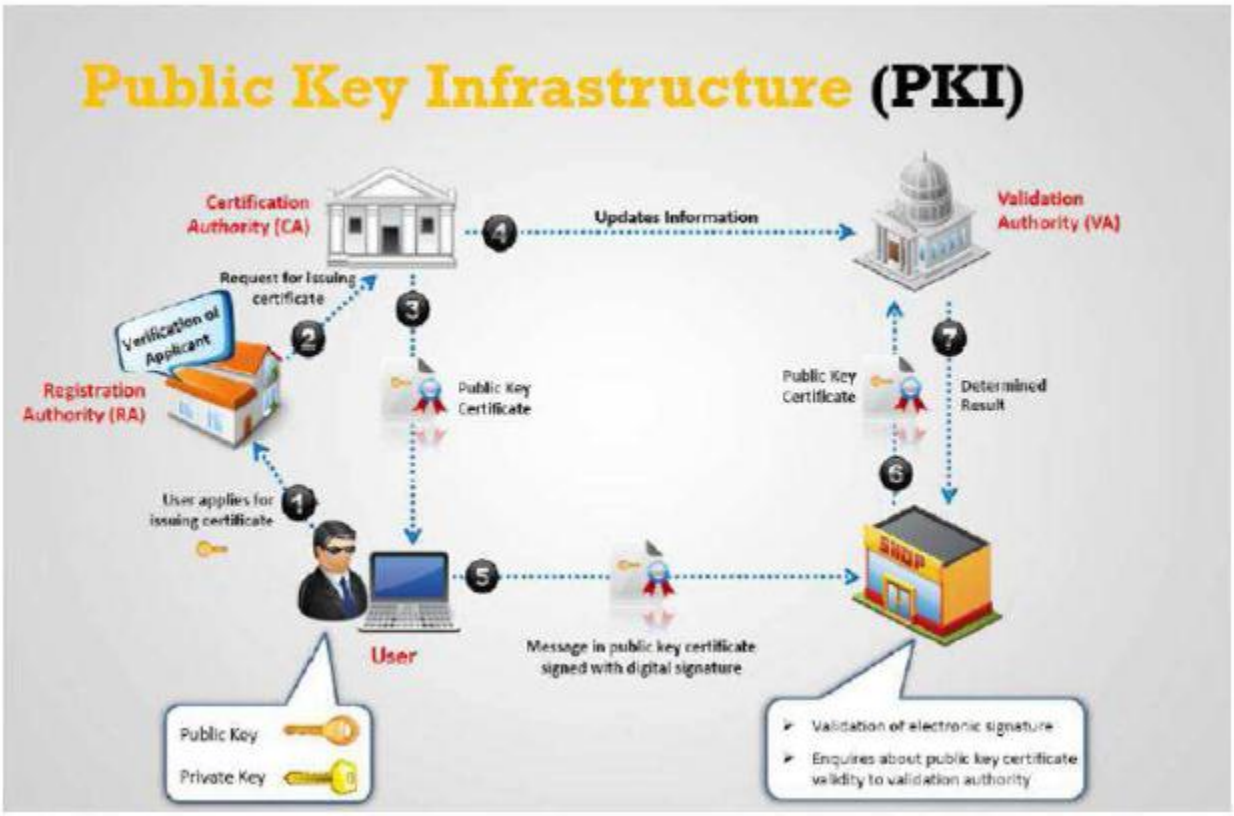
C) L'infrastructure nationale à clé publique (PKI)

Le Cameroun comme premier pays en Afrique Centrale a entrepris, depuis 2009, de mettre en place, avec le concours de la République de Corée, une plateforme de sécurité appelée **PKI (Public Key Infrastructure)** ou **Infrastructure à Clé Publique**, pour sécuriser les transactions gouvernementales en ligne.

Cette plateforme de sécurité permet, grâce aux services d'authentification, de non répudiation, d'intégrité et de confidentialité, de prémunir les données et les échanges électroniques gouvernementales d'attaques provenant de cybercriminels.

L'infrastructure nationale à clé publique (PKI)





RÔLE ET FONCTION DE LA PKI?

- Sécurisation des échanges électroniques dans les administrations, entreprises, organisations diverses ou entre ces différentes entités (correspondances, messages confidentiels divers) ;
- Sécurisation des actes administratifs (décrets, arrêtés et textes divers) ;
- Signature des contrats et conventions en ligne ;
- Sécurisation de pièces officielles (actes d'Etat civil, bulletin n°3, diplômes, permis de conduire, traitement salarial, examens et concours, etc.);
- Amélioration de la sécurité dans les réseaux privés virtuels (VPN);
- Offre de services en ligne (marchés public, impôt, douane, actes divers);
- Transactions en ligne (e-banking, e-commerce).

Décret N° 2012/1318/PM du 22 Mai 2012 fixant les conditions et les modalités d'octroi de l'autorisation d'exercice de l'activité de certification électronique.