Module 3 : LA CYBERCRIMINALITE ET LACYBER SECURITE

Définitions

Cybercriminalité : c'est l'ensemble des infractions s'effectuant à travers le cyber espace par des moyens autres que ceux habituellement mis en œuvre et de manière complémentaire à la criminalité classique.

Cyber sécurité : ensemble des 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 télécommunications, les SI et pour la protection de la vie privée des personnes.

Le piratage informatique :

C'est une introduction dans un système ou un réseau afin de prendre connaissance, de modifier ou de détruire les informations ; le piratage informatique est l'une des pratiques la plus utilisées par les cybercriminels. C'est aussi une atteinte contre les biens, les personnes et sert aux pirates à s'infiltrer illégalement afin de détourner un serveur pour surfer gratuitement, téléchargé les logiciels, musiques, vidéos, images, … de pirater les comptes bancaires. Pour cette pratique nous avons les acteurs exemple les hackers et les techniques exemples le phishing, le pharming, le harponage, le smishing…

Travail à faire : Enumérer 10 formes d'atteintes utilisées par les pirates pour s'infiltrer dans un SI ou dans un réseau de communication, définir chaque technique, l'illustrer et dire comment s'en protéger (protection légale et technique).

Introduction

Avec l'essor des TIC, on assiste à l'avènement des nouvelles infractions qui se réalisent ou qui sont favorisées par les TIC. La cybercriminalité encore appelée criminalité des technologies consiste à utiliser les systèmes et réseaux informatiques en général et l'Internet en particulier pour poser des actes criminels proscrits par les textes législatifs et règlementaires d'où la nécessité de sécuriser son système d'information ou son réseau de communication à l'aide

de divers moyens technique, organisationnel, juridique, financier, humain, procédural et autres moyens.

I- **Présentation générale de la cybercriminalité :**

Les utilisateurs passent ¾ de leur temps à surfer, à rechercher les informations, à communiquer c'est ainsi qu'ils deviennent la proie des cybercriminels qui ont pour but de se procurer un avantage illégal, de prouver leurs ingéniosités, de nuire à autrui. La grosse difficulté au Cameroun est d'identifier l'auteur du cyber crime, de le géo localiser car il peut se trouver n'importe où dans le monde.

La cybercriminalité peut prendre diverses formes et peut se produire à tout moment et n'importe où. Ici les cybercriminels utilisent un certain nombre de méthodes en fonction de leur ingéniosité et de leurs objectifs. L'ordinateur ou le matériel peut être l'agent de l'acte criminel, le facilitateur ou la cible. Les atteintes de la cybercriminalité sont de deux types :

- Les atteintes aux biens : (il s'agit entre autre de la fraude à la carte bancaire, la vente par petites annonces ou enchères d'objets volés ou contrefaits, l'encaissement d'un paiement sans livraison de la marchandise, la copie illégale de musique, film ou logiciel pour soi ou pour autrui).
- Les atteintes aux personnes : (il s'agit de l'atteinte à la vie privée, des propos incitant à la haine raciale, des recettes d'explosif, de la diffusion auprès d'enfants des photographies à caractère pornographique ou violant).

Dans les deux cas, les faits sont punis par la loi.

Les diverses manifestations de la cybercriminalité entrainent plusieurs conséquences exemple : la perte d'informations confidentielles ou non, l'infection par des virus de son système ou réseau de communication, l'impact sur la productivité avec des répercutions financières.

En Afrique on a longtemps considéré le phénomène de cybercriminalité comme un mythe qui existait dans les pays développés où la connectivité est plus importante et où les technologies sont beaucoup plus avancées, aujourd'hui on ne parle plus de nouvelles technologies en Afrique car on constate des avancées considérables en matière de TIC. On peut conclure en disant que les cybers citoyens africains sont devenus cybers vulnérables.

II- **Quelques données statistiques dans le monde :**

Avec la multiplicité des infractions il est recommandé de collecter des indices et des éléments de preuve. Nous illustrerons certains états statistiques dans le monde :

- un rapport publié en septembre 2011 par **Symantec**, société américaine spécialisée dans la sécurité informatique, dans ce rapport plus de 431 millions d'adultes ont été victimes des cybercriminels dans le monde en 2010, soit plus d'un million par jour. Les principaux types de cyber crimes étaient les logiciels malveillants,
- **Kaspersky,** éditeur reconnu pour les solutions de sécurité informatique contre toutes formes de menaces cybercriminelles, annonce dans un rapport annuel de 2009, portant sur le développement des menaces du cyberespace qu'il y a eu **73 619 767** attaques de réseau provenant des chevaux de Troie, logiciels conçus pour voler les données, tels que les mots de passe, les codes, licence, signature électronique,
- un rapport sur l'état de la fraude sur Internet, a été publié par le bureau fédéral d'investigation des Etats-Unis (FBI) en 2010, le bureau central des dépositions aurait enregistré plus de **300 000** plaintes,
- Selon l'ANTIC le Cameroun a subi 12800 attaques en 2017(escroquerie financière sur Internet, la fraude à la carte bancaire, l'usurpation d'identité) cette cybercriminalité a causé d'énormes conséquences économiques dans le pays 14 milliards de FCFA ont été injectés par l'Etat pour sécuriser son cyberespace entre 2013-2017 ; Malgré cela le phénomène s'est accentué avec l'avènement des réseaux sociaux,
- Dernière cyber attaque mondiale s'est produite en Mai 2017,
- En novembre 2016, un email sur 85 contenait des malwares, un email sur 2620 contenait des phishing,
- Au deuxième trimestre de l'année 2016 plus de 83% de Smartphones étaient infectés
- En 2016 toujours, 13,7 millions de personnes ont été confrontés par la cyber criminalité en France,
- En 2017 on relève 41% de taux de succès d'un ranconware,
- Les particuliers sont deux fois plus infectés que les professionnels.

TAF de recherche : Faux en informatique et fraude en informatique de part leur définition qui découle de l'autre

- Selon l'(UIT) L'Union Internationale des Télécommunications, le coût de la cybercriminalité est évalué à près de **1 000** milliards de dollars aux

Etats chaque année et estime à **650 000**, le nombre de systèmes informatiques infectés dans le monde.

- En Afrique, la cyberescroquerie s'est répandue. Les techniques les plus utilisées sont le « phishing » ou hameçonnage et le jeu de « qui perd gagne ».
- Dans un rapport publié en 2011, **McAfee**, une société de sécurité informatique, présentant l'extension « .cm » du Cameroun faisant partie des cinq noms de domaine les plus risqués de la planète (.cm, .com, .cn, .ws, .info), avec un taux de risque de **36,7%,** sur environ 27 millions de noms de domaines analysés.

A titre d'exemple, entre juin 2009 et juin 2010, Les cybercriminels ont piraté le site officiel du Premier ministère, en créant un site web frauduleux « **http://www.govcamonline.com/**» dont la page d'accueil portait les mêmes informations jusqu'aux appels d'offres lancé. C'est ainsi que de nombreuses personnes tant du Cameroun et des pays étrangers ce sont vues extorquées d'importantes ressources.

Bien d'autres sites web camerounais ont fait l'objet de cyber-attaque. (la douane camerounaise en 2008, notamment ;le Ministère des Domaines et des Affaires Foncières en 2008 ; l'Université de Yaoundé I en 2009 ; le quotidien la Nouvelle Expression en 2009 ; le quotidien national Cameroun Tribune en 2011 ;le site web du Parti des Démocrates Camerounais en 2011).

Selon une étude d'IBM menées auprès de 3000 entreprises dans le monde, le taux du cybercrime dépasse désormais celui des vols et des agressions physiques.

III- **Les techniques de sécurités du cyber espace (lutte contre la cybercriminalité) :**

(Convention : pacte, un accord de volonté conclu entre deux ou plusieurs parties et qui s'apparente à un contrat.

Directive :)

La lutte contre la cybercriminalité est une lutte permanente et les mesures mise en œuvre ne sont pas toujours suffisantes. Ce fléau étant mondial la CEDEAO (Communauté Economique des Etats de l'Afrique de l'Ouest) s'est dotée d'une directive portant sur la cybercriminalité ; l'union africaine a adopté une convention africaine (qui insiste sur la culture de cybersécurité), l'instrument international est la convention de Budapest (en Hongrie), cette convention européenne reste ouverte à tous les états y compris les pays non membres).

Au Cameroun, le MINPOSTEL est en charge de l'élaboration et de la mise en œuvre de la politique de sécurité des réseaux de communications électronique et des SI d'où la mise en place de certaines mesures.

a- <u>Les mesures légales</u> :

La loi n°2010/012 relative à la cyber sécurité et cybercriminalité a été élaboré pour pallier au problème de vide juridique. C'est ainsi que la loi n°2010 pense à encadrer les pratiques peu recommandables dans le cyber espace d'où la répression par certains articles (confère chapitre 2 du titre 3intitule des infractions et des sanctions) :

***L'atteinte à la vie privée**

sanctionné selon l'article 74 de la loi n°2010/012 du 21 décembre 2010 est punit d'un emprisonnement d'un à deux ans et d'une amende d'un à cinq millions de FCFA, quiconque porte atteinte à l'intimité de la vie privée d'autrui en fixant, enregistrant ou transmettant sans le consentement de leur auteur, les données électroniques ayant un caractère privé ou confidentiel. Sont également punies, les personnes qui collectent par des moyens illicites, des données nominatives d'une personne en vue de porter atteinte à son intimité et à sa considération.

*** La fraude à la carte bancaire**

sanctionné par l'article 73 de la loi n° 2010/012, Celui qui, par voie d'un système d'information, ou dans un réseau de communications contrefait, falsifie une carte de paiement, de crédit, ou de retrait, fait ou tente de faire usage d'une carte contrefaite ou falsifiée (l'intention vaut l'acte), encourt une peine d'emprisonnement de deux à dix ans, et ou une amende de 25 à 50 millions F.

***La disposition des images et des vidéos pornographiques enfantines**

sanctionné par l'article 76 de la même loi est punit de cinq à dix ans et d'une amende de cinq à dix millions F ou de l'une de ces deux peines seulement, celui qui confectionne, transporte, diffuse par voie de communications électroniques ou d'un système d'information, un message à caractère pornographique enfantine, ou de nature à porter gravement atteinte à la dignité d'un enfant. L'alinéa 2 de l'article81 définit la PE.

<u>Illustration par un cas</u> :

Si nous prenons le cas du Général français à la retraite Raymond GERMANO qui a comparu le 3 novembre 2009 pour avoir téléchargé les

images mettant en scène les enfants de 6 mois **à** 12 ans. L'affaire remonte à l'année 2006, les policiers autrichiens au cours d'une enquête se sont intéressés à un site de diffusion d'images pornographiques principalement pédophile, l'enquête a permis de déterminer les utilisateurs du site dont le Général, la trace de celui a été retrouvé grâce à l'adresse IP de son ordinateur. Il n'a d'ailleurs pas nié les faits et s'est dit prêt à se soumettre à un traitement. Son ordinateur a été saisi, près de trois milles photos ont été retrouvés dans son disque dur. Sa peine d'emprisonnement a été de 2 ans et amende de 30 milles euros.

b- <u>Les mesures pratiques</u> :

Bien qu'il n'existe pas de sécurité absolu, la loi protège et dissuade les individus à ne pas commettre les infractions, d'où l'assertion selon laquelle la loi est dissuasive avant d'être répressive. Tout de même les cybers citoyens doivent assurer un minimum de sécurité pratique sur leur réseau ou dans leur SI en paramétrant par exemple la confidentialité, en utilisant les mots de passe alphanumérique, en installant les logiciels de reconnaissance vocal, facial, digital, à rétine, par Bluetooth, … les cybers citoyens doivent également s'armer d'un guide de bonne pratique sécuritaire. Les parents trouveront aussi un intérêt à installer un logiciel de contrôle parental permettant de filtrer et de bloquer certaines chaines et sites indésirables. Exemple **logiciel log protect, logiciel open AN** filtrant les contenus adultes ou choquants. Les maîtres mots sont : la sensibilisation et la prudence.

Dans un monde concurrentiel et mondialisé, les services publiques ou privées qui traitent les informations (la banque qui doit fidéliser leurs clientèles) ont également un intérêt à protéger les informations afin que celle sensible ou non, confidentielle ou non, ne soient diffuser volontairement ou accidentellement. Chaque individu, cyber citoyen est un acteur direct ou indirect pour la bonne marche de la société et doit de ce fait signaler les infractions qui se produisent. En dehors de la signalisation, en cas d'acte cybercriminel les victimes peuvent déposer à la police ou à la gendarmerie leur plainte pour besoin d'enquête. Certaines agences telles que l'ART, l'ANTIC travaillent en collaboration avec MINPOSTEL en vue d'assurer pour le compte de l'état le contrôle et le suivi des activités technologiques. L'ANTIC a par exemple mis sur pied un centre d'alerte et de réponse aux incidences cybernétique (CIRT) fonctionnel 24/24 (222 09 91 64, alerts@antic.cm), nous avons aussi INTERPOL qui a fait de la lutte contre la cybercriminalité l'une de ses priorités en apportant son assistance à des pays membres en cas de cyber attaque.

<u>Conclusion</u>

Au vue de ce qui précède nous pouvons dire que le développement des TIC, indispensable au développement harmonieux et durable passe par l'implication de toutes les parties prenantes : le Gouvernement, le secteur parapublic, le secteur privé, les populations. Le phénomène de cybercriminalité emporte véritablement des conséquences car il constitue une véritable menace pour la sécurité des SI, des RC(Réseau de communication), des citoyens, il sera dans ce cas nécessaire de mettre en place les stratégies de prévention, de dissuasion et de répression à l'aide de divers moyens participant à la sécurisation du cyberespace.(par la protection qu'elles assurent au SI, au réseau, aux données à caractère personnelles).

<u>Module 4 :</u> **TIC et biens matériels et logiciels (**il s'agit de la GESTION DES RESSOURCES MATERIELLES ET LOGICIELLES**)**

Les technologies ont fait évoluer l'organisation de notre société car elles ont ouvert la voie à des modèles de société plus durable. La notion de développement durable (concept appliqué à la croissance économique prenant en compte les aspects environnementaux et sociaux pour les générations du présent et du futur) est la finalité de l'usage des technologies, il s'agit d'une approche globale de gestion des ressources matérielles, logicielles et humaines dont le but sera de satisfaire aux besoins et aux aspirations de l'être humain. Des lois et règlements définissent les droits et obligations des personnes utilisant les ressources informatiques. Tout utilisateur n'ayant pas respecté ces textes en vigueur pourra être poursuivis, car nul n'est censé ignorer la loi.

I. Le Droit d'usage des ressources informatiques

Ce droit fait référence à l'ensemble des ressources matérielles et logicielles.

a) L'usage du matériel

L'usage du matériel relève d'une charte d'utilisation, d'une notice, d'un règlement définissant les conditions de bonne utilisation des ressources informatiques, ces règles s'appliquent à tout utilisateur.

b) Le Logiciel et le droit d'auteur

L'auteur d'un logiciel peut autoriser, interdire, restreindre à l'utilisateur ses droits d'usage, la circonscription peut porter sur les points suivants:

- l'étude du code source ;
- la modification, copie, la redistribution, l'utilisation du logiciel ;
- relever les insuffisances et apporter des suggestions.

Le contrat de licence d'utilisation ou condition d'utilisation est un contrat qui lie l'auteur à l'utilisateur, ce contrat de licence définit les conditions d'usage du logiciel que l'auteur autorise. C'est une « cession de droits d'utilisation du logiciel » et non un « transfert de propriété du logiciel ». Les conditions d'utilisation d'un logiciel relèvent du droit d'auteur parce que la conception d'un logiciel est une création de l'esprit (Ensemble des prérogatives dont dispose un auteur (ou un groupe d'auteurs) sur les œuvres de l'esprit il se divise en deux branches :

- Le droit moral qui reconnait à l'auteur la paternité de l'œuvre et vise le respect de l'intégrité de l'œuvre ;
- Les droits patrimoniaux qui confèrent un monopole d'exploitation économique sur l'œuvre, pour une durée variable (selon le pays) au terme de laquelle l'œuvre entre dans le domaine public.)

II. Les atteintes/intrusions dans un système automatisé de données

Les atteintes au système de traitement automatisé de données sont considérés comme le non-respect des principes de confidentialité, d'intégrité et de disponibilité des données, ces atteintes sont sanctionnées en tant qu'atteinte contre les ressources informatiques. Condamner celui qui prend connaissance d'informations confidentielles ou non, revient à apporter la preuve de l'acte frauduleux de la personne.

On considère qu'il y a intrusion lorsqu'une personne réussit à obtenir un accès non autorisé dans un système, ie qu'en cas d'intrusion, une personne n'ayant pas le droit d'accès au SAD soit parvenu à s'octroyer les droits de l'administrateur.

Il existe plusieurs types d'atteintes ou intrusion, il s'agit de :

a) **Les intrusions simples** définit comme "*le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données* " ;

b) **Les intrusions avec dommages,** ici l'intrusion et le maintien frauduleux ont certaines conséquences c'est à dire lorsqu'il en résulte soit la suppression, la modification, la divulgation, le vol de données contenues dans le système, soit une altération du fonctionnement dudit système ;

c) **Les entraves volontaires aux systèmes et aux données s'y trouvant :** c'est le fait d'altérer le fonctionnement d'un système de traitement automatisé des données. Cette intrusion vise notamment l'introduction volontaire des programmes susceptible d'entrainer une perturbation du système tel que les virus. (logiciel malveillant conçu pour se propager sur d'autres ordinateurs dans le but de perturber le fonctionnement de l'ordinateur infecté).

III - Techniques de sécurité légale et réglementaire, physique et logicielle

La sécurité couvre plusieurs niveaux : le niveau physique, organisationnel, règlementaire, et autres. Bien qu'il n'existe pas de sécurité absolue, les textes législatifs et règlementaires protègent tout de même les individus et leurs biens.

La liste des moyens de protection d'un SAD est définie dans le titre II de la loi relative à la cybercriminalité et à la cybersécurité intitulé « de la cybersécurité», ces moyens étant loin d'être exhaustifs nous citerons entre autres certains moyens mis en place pour conserver, sécuriser et garantir la bonne marche d'un système ou d'un RC

a- la protection légale et réglementaire

Comment le droit camerounais réprime-t-il le fait de s'introduire illégalement, illicitement, frauduleusement dans un SAD?Aux yeux de la loi chacun des coupables qui aura accès de manière frauduleuse dans un système ou RC pourra être poursuivi au regard des dispositions de la loi relative à la C.C et à la C.S.

b- La protection physique ou matérielle

Cette protection vise à sécuriser les infrastructures matérielles :

La partie cuivrée de la carte mère (partie verte) doit se nettoyer avec un diluant, L'on s'engagera aussi à dépoussiérer, prévoir un système d'aération, utiliser des onduleurs, régulateurs de tension, assurer la réparation des erreurs de fonctionnement (maintenance corrective ou curative), à prévenir celles-ci par des vérifications périodiques, c'est-à-dire voir si le matériel fonctionnent bien (maintenance préventive) ou à assurer une maintenance évolutive (installation et mise à jour), installation d'un parafoudre, installation d'une prise de terre, protection anti incendie, protection anti inondation.

c- La protection logicielle

Cette protection porte sur :création d'image système (copie tout le contenu du système sur un support externe permet de refaire le système en utilisant l'image) ; l'installation des programmes anti-virus originaux (virus : logiciel malveillant conçu pour se propager à d'autres ordinateurs dans le but de perturber le fonctionnement de l'ordinateur infecté) ; l'installation de logiciel de reconnaissance vocale, faciale, à rétine, digitale, corporelle ;sous Windows 8 l'on peut procéder à la protection en paramétrant l'ajout de mot de passe image, mdp texte; (paramètre du PC, comptes, option de connexion, ajouter un MDP image, sélectionner l'image, dessiner le schéma) ;l'activation d'un filtre anti-spam (afin de se protéger des courriers intempestif) ; installation d'un anti spycam ; l'activation d'un pare-feu(configuration paramètre),l'installation d'un anti-spyware (spyware : logiciel malveillant que l'on installe dans un ordinateur dans le but de collecter et de transférer les informations très souvent sans que

l'utilisateur n'en ait connaissance) ; activation d'un anti-hameçonnage ((menu outils) arnaque de type bancaire) ; installation des IDS (système de détection d'intrusion), des IPS ;utilisation de la technologie de cryptographie ;paramétrage des droits en écriture et en lecture, utilisation de la technologie de captcha (protection des logiciel robot ie avoir la certitude que l'utilisateur n'est pas un robot) ; paramétrage du BIOS pour la sécurisation du système de démarrage ; protection des ports (USB, VGA, RJ45, HDM(connexion télé et laptop).

CONCLUSION

Chaque utilisateur est responsable des infractions qu'il commet par l'intermédiaire des moyens technologique, outre les sanctions civiles et pénales prévues par les textes delois et règlement, le non-respect des conditions d'utilisation prévues dans une charte d'utilisation, une notice ou autres expose le coupable à des sanctions disciplinaires.

TAF : def : contrat de licence d'utilisation, œuvre de l'esprit ; les différents types d'atteintes dans un STAD; les principes de sécurité dans un SI; l'importance des IDS, IPS.