HISTOIRE ET DYNAMIQUES DE LA CYBERCRIMINALITE ET DE LA CYBERSECURITE

UNIVERSITE DE DSCHANG
Prof. Guy Mvelle
Doyen de la Faculté des sciences juridiques et politiques
Université de Dschang
Juin-Juillet 2O26
guymvelle@gmail.com

INTRODUCTION

Objectif général du Cours

Il s'agit dans le cadre de ce travail, de faire une présentation et une analyse de l'évolution des cybermenaces dans le monde et au Cameroun d'une part et les efforts menés par les Etats et les organismes divers pour les prévenir, les gérer, et les combattre d'autre part. Il s'agit de permettre aux apprenants d'avoir une grande culture générale dans l'évolution des cybermenaces et des cyberattaques dans le monde en général, en Afrique et au Cameroun en particulier, et des avancées observées pour les neutraliser, les réduire à défaut de les éradiquer. Un cours nécessaire pour participer au débat relatif aux questions de la cybercriminalité et de la cybersécurité qui peut également devenir un outil au service des spécialistes de la gouvernance cybersécuritaire.

De façon spécifique, il s'agit de présenter et analyser les origines et les types de cyberattaques rencontrées dans le monde ; de présenter et analyser les politiques, normes et stratégies de prévention, de gestion et de lutte développées par les Etats, les acteurs interétatiques et les organismes privés.

1.Qu'est-ce que la cybercriminalité ? En quoi consiste-t-elle techniquement ? Qu'est-ce que la cybersécurité ?

- **La cybercriminalité** : « Actes qui affectent la confidentialité, l'intégrité, la disponibilité et la survivance des systèmes technologiques de l'information et de la communication, les données et les infrastructures réseau sous-jacentes » (art. 25 Conv. UA sur la cybersécurité et la protection des données personnelles, 2014).

- « Ensemble des infractions s'effectuant à travers le cyber espace par d'autres moyens que ceux habituellement mis en œuvre et de manière complémentaire à la criminalité classique » (Art. 4, loi du 21/12/2010 sur la cybersécurité et la cybercriminalité au CMR).

- Techniquement, il s'agit d'une activité intentionnelle visant à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité de ce système ou de l'information qu'il contient, ou en perturbant le monde numérique en général.

- **Une cybermenace** : Terme plus englobant et renvoyant à un certain degré de gravité à grande échelle qui fait allusion à **une activité intentionnelle** visant à compromettre la sécurité d'un système d'information en altérant la disponibilité, l'intégrité ou la confidentialité de ce système ou de l'information qu'il contient, ou en perturbant le monde numérique en général.
- **Une cyberattaque** : **Acte offensif** envers un dispositif informatique ou des données informatiques/ une offense indésirable consistant à voler, exposer, modifier, désactiver ou détruire des informations via un accès non autorisé aux systèmes informatiques ou aux données informatiques…
- **Une Cyberdéfense** : **Acte de prévention ou de lutte contre** une offense indésirable consistant à voler, exposer, modifier, désactiver ou détruire des informations dans un système d'information.

- **La cybersécurité :** 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 communication électroniques, les systèmes d'information et pour la protection de la vie privée des personnes (article 4, loi du 21 décembre 2010 sur la cybersécurité au Cameroun).

- **La sécurité numérique :** ensemble des mesures prises pour gérer le risque de sécurité numérique au service de la prospérité économique et sociale : opérations techniques, la prospérité, l'application du droit pénal, la sécurité nationale et internationale, etc. (OCDE, 2023)

2. **Quelles sont les motivations des cybercriminels ?**

- **Des motivations multiples liées à la cybercriminalité** : motivations politiques (espionnage, désinformation, sabotage avec destruction des infrastructures stratégiques ou critiques, etc.), motivations défensives (riposte à une première attaque, rendre l'appareil, neutraliser les effets d'une attaque, etc.), motivations économiques ou lucratives (appât du gain, escroquerie, positionnement par rapport à des concurrents économiques par le vol des secrets industriels et commerciaux, vol des bases de données clients, vol de savoir-faire ou discrédit à l'endroit des concurrents, etc.), exhibition technique des informaticiens (s'amuser, relever des défis techniques pour la beauté du geste, reverser les résultats dans la communauté, se vanter, etc.), motivations émotionnelles ou sentimentales (vengeance amoureuse), vengeances administratives ou institutionnelles après un licenciement, etc.

3. **Problématique générale du cours** : mieux comprendre comment l'on est arrivé à la cybercriminalité et à la cybersécurité, replacer les évènements dans une suite, une continuité qui leur donne sens, scruter le passé pour contribuer à penser l'avenir, interpréter les faits passés pour comprendre le présent et prévenir le futur, savoir d'où l'on vient pour prévoir d'où l'on va, rechercher les faits et les objets qui ont engendré la cybercriminalité et la cybersécurité : les machines, les connaissances scientifiques (algorithmes, les langages et les

informations), les conflits internationaux (la seconde guerre mondiale mais surtout la guerre froide, les conflits post-guerre froide, le conflits israélo-arabes, les rivalités américaines dans le monde), les faits sociaux (l'expansion de l'informatique et du numérique).

CHAPITRE 1

LES PREMIERS ACTES DE CYBERCRIMINALITÉ ET LEURS CAUSES

- **La guerre froide, la reconnaissance informatique et l'accélération des avancées technologiques**

  -La guerre froide : L'ensemble des conflits qui ont opposé les grandes puissances au lendemain de la seconde guerre mondiale jusqu'en 1991. Le camp américain composé des démocraties libérales faisait face à l'Union soviétique et aux démocraties dites populaires. La guerre était caractérisée de froide parce que malgré les vives tensions entre les deux blocs, il n'y eut jamais d'affrontement militaire direct. La confrontation se faisaient plutôt par des guerres interposées et par des combats idéologiques et culturels avec de fortes tensions diplomatiques entre belligérants. Les deux superpuissances (USA et URSS), tout en étant hostiles l'une à l'autre, évitaient de s'affronter directement, par crainte d'une escalade suicidaire. Par conséquent, le conflit Est/Ouest était dérivé dans trois directions : la course aux armements au centre, la propagande et la subversion dans les zones d'influence de l'adversaire, l'intervention chez les tiers (les non-alignés), et donc l'utilisation de tous les moyens d'espionnage dont l'informatique.

  - 1970 : CRYPTO AG : Premier vaste programme de cyber espionnage ; entreprise suisse spécialisée dans les télécommunications et la cryptographie, constructeur de dispositifs de chiffrement pour assurer la confidentialité des communications diplomatiques et militaires ; des appareils de cryptage truqués sont vendus à plus de 120 pays par cette société pour fournir des renseignements aux services secrets américains et ouest-allemands. En 2020 **CRYPTO AG,** désormais propriété de la CIA et du Bureau fédéral de renseignement (All), est mise en cause dans l'affaire des Cryptoleaks. Elle aurait permis à ses deux propriétaires de déchiffrer des messages codés de plusieurs dizaines de pays dans le monde. Son programme d'espionnage est appelé Opération Rubicon.

  -Accélérations des avancées technologiques : Création de nouveaux langages de programmation informatique, naissance des circuits intégrés (liaison de plusieurs transistors sans utiliser de fil électrique), passage de l'informatique du domaine militaire à la vie civile grâce à IMB qui collaborait avec le département de défense américain, début de l'enseignement de l'informatique dans les universités américaines, création des systèmes d'exploitation

(Wildows, Max Os, Linux), invention du micro-ordinateur en 1977 par Apple, invention du premier PC par IBM en 1981, etc.

-Ver de Morris (1988) : Premier ver informatique de l'histoire. L'étudiant américain Robert Tappan Morris lance à partir du MIT (Massachusetts Institute of Technology) un ver informatique qu'il distribue dans le monde entier via internet encore limité dans les milieux militaires, universitaires et les centres de recherche. Le ver se révèle très dangereux à cause de plusieurs erreurs de code et cause d'énormes pannes sur environ 6000 ordinateurs, soit environ 10% des machines connectés à travers le monde. Robert Morris est condamné à une peine de probation de 3 ans et à 10 000 dollars d'amendes en vertu de la *Computer Fraud and Abuse Act* de 1986. Le ver cause entre 10 et 100 millions de pertes dans le monde et est suivi par d'autres vers comme WannaCry ou Mirai.

- **Constat général :** La guerre froide, les besoins militaires, la reconnaissance de l'informatique et l'accélération des avancées ethnologiques constituent ainsi les facteurs ayant favorisé le détournement de l'informatique à des fins criminelles. Une criminalité qui est principalement étatique, même si intervient un évènement majeur impliquant un simple individu (Robert Tappan Morris) qui voulait peut-être simplement éprouver ses connaissances techniques sans réelle intention de nuire à grande échelle.
- **Conclusion :** Les motivations sont donc politiques : espionnage, désinformation, sabotage avec destruction des infrastructures stratégiques ou critiques, etc. Travail des unités spécialisées, en lien de près ou de loin avec des organisations militaires ou des services de renseignement. Leur démarche est généralement professionnelle, rigoureusement planifiée, ciblée et peut mettre en œuvre des outils sophistiqués.

CHAPITRE 2
L'INTENSIFICATION CONTEMPORAINE DE LA CYBERCRIMINALITE

1/ Les tensions post-guerre froide, conflits israélo-palestiniens, rivalités et expansions des grandes puissances, etc.

-Attaque des sites web de l'OTAN par des nationalistes serbes (1999) = politique et idéologique

- Multiples attaques de groupes iraniens : Ashiyane, Shabgard et Simorgh (**2003) =** nationaliste, idéologique et politique

- Hacking par les Israéliens du système de défense aérien de la Syrie, préalablement à une série de bombardements **(2007)**

- Cyberattaque contre l'Estonie : attaques massives en déni de service (DDoS) paralysant des banques, des médias, des sites gouvernementaux et autres services publics menées en **représailles au déplacement d'un monument à la gloire de l'Armée rouge du centre-ville vers la périphérie de Talinn (2008=** idéologique et politique

- Attaque de l'Iranian Cyber Army contre Twitter **(2009) =** nationaliste, politique et idéologique.

-Attaque Stuxnet (Américains et Israéliens) afin de ralentir secrètement le programme nucléaire iranien : destruction d'un million de centrifugeuses (AIEA, **2010)** = Motivations défensives, politiques, etc.

- Détournement par la Chine de 15% des routes mondiales d'Internet pendant 18 mn (*traffic hijacking*, **2010) =** Technique, politique et anti-impérialiste.

2/ Expansion de l'informatique et du numérique et diffusion de la cybercriminalité dans la société.

-Accessibilité presque par tous de l'informatique et du numérique sans grande barrière financière ou compétences techniques majeures (accessibilité financière et matérielle)

-Amélioration générale de la connectivité dans le monde

-Accroissement des capacités de stockage, de traitement et de partage des données

-Pénétration de l'ordinateur dans tous les milieux socio-professionnels et dans tous les systèmes techniques, financiers, commerciaux, informatiques et administratifs.

-Accès du grand public à internet, etc.

-Faits majeurs : Attaque de plusieurs pays par des logiciels de rançon : Maroc, Algérie, Tunisie, Egypte, Sénégal, Ouganda, Sud-Soudan, Côte d'Ivoire, Kenya, Namibie, Zimbabwe, Madagascar…(**2017)**

- Constat alarmant de l'UIT sur la vulnérabilité de la presque totalité des pays africains, excepté Ile Maurice, Kenya et Rwanda (**2018)**

- Soupçon d'espionnage du siège de l'Union africaine supposément par la Chine (**2012- 2017**)

- Camair-Co victime d'une piraterie de 500 billets d'avion (**2011)**

- 7 sites web d'administrations publiques victimes d'attaques de type web d'effacement (modification non sollicitée de la présentation d'un site Web),(**2015-2017**)

- 34 sites gouvernementaux attaqués par des programmes malveillants

- Plusieurs centaines de cas d'usurpations d'identités dont celles de 182 membres du gouvernement

- Environ 4 milliards de pertes économiques liées au *scamming* (escroquerie ou cyber arnaque, fraude 419)

- **Conséquences : Selon l'OCDE,** les pertes directes liées aux cybers incidents déclarés s'élevaient en 2020 à un total de près de 28 milliards USD dans le monde et des milliards de donnés ont été volées ou compromises. Les coûts directs et indirects liés à ces incidents sont estimés sensiblement de 1 à 10% du PIB mondial.
- Selon **l'Association italienne pour la sécurité informatique (CLUSIT)** en 2021 le coût total de la cybercriminalité a dépassé 6000 milliards de dollars. D'après une autre étude réalisée par **Mc Afee** en 2020, la cybercriminalité a couté plus de 1000 milliards de dollars à l'économie mondiale. En 2021 coût médian d'une attaque informatique en France était de 15300 euros (10 millions de FCFA), une augmentation de 29% par rapport à 2020.

- Au Cameroun, les données publiées par l'ANTIC révèlent qu'en 2021, le Cameroun a cumulé 12 milliards de FCFA de pertes financières dues à la cybercriminalité (coûts des enquêtes techniques, les notifications aux clients de l'intrusion, la mise en conformité règlementaire, les honoraires d'Avocat et les frais de justice, la sécurisation des données client après incident, les relations publiques, la mise à jour et l'amélioration des dispositifs de sécurité, la baisse du chiffre d'affaires liée à la perte des contrats clients, la dépréciation de la valeur de l'entreprise ou de la marque, la perte de la propriété intellectuelle, la perte de confiance des clients, etc.).

3/ Les Conséquences

- **Techniquement,** les différentes attaques et menaces numériques présentent des dangers sur toutes les trois couches du cyberespace que sont la couche physique ou matérielle, la couche logique et la couche cognitive.
- Ces attaques techniques ou matérielles concernent de multiples dispositifs : systèmes de contrôle d'accès, appareils de réseau, systèmes de contrôle industriel, systèmes de surveillance… En dehors de l'intégration de portes dérobées (ou backdoor), ces attaques peuvent être utilisées pour de l'écoute clandestine, la génération d'erreurs entraînant l'arrêt d'une machine, le contournement des systèmes d'authentification informatique…
- Selon le site Techniques de l'Ingénieur (TI), les attaques visant le hardware ont d'abord été imaginées pour le vol de données bancaires sur les puces des cartes bleues Ces approches sont à présent appliquées aux téléphones portables, dont les circuits sont mal protégés. Avec l'Internet des objets, la situation est encore pire où les appareils sont à la fois omniprésents et très peu, voire pas du tout, sécurisés. Tous les appareils électroniques (ordinateurs, réseaux de communication, capteurs…) intégrant des processeurs (partie de l'ordinateur qui interprète et exécute les instructions) sont exposés. Il suffit qu'un composant physique soit compromis pour impacter les différentes couches de cybersécurité d'un système.
- **Au plan administratif :** Atteinte à la confidentialité des documents administratifs, compromission de l'efficacité de l'action publique, atteinte à la sureté et à la sécurité de l'Etat qui devient de plus en plus en proie aux menaces sécuritaires protéiformes, etc.
- **Au plan social :** exposition au chantage social (harcèlement numérique), atteinte à la réputation individuelle, atteinte à la vie privée, stress, risques et cas de suicides avérés, etc.
- **Au plan économique :** préjudice commercial (vol des données des clients, plan de développement de l'entreprise dévoilé, secrets de fabrication dévoilés, etc.), pertes financières sèches, etc.
- **Au plan politique national :** atteinte à la souveraineté de l'Etat, risque de conflits entre l'Etat et les groupes divers, etc.
- **Au plan de la politique internationale** : Risque d'une course au cyber armement, risque d'une cyberguerre, bouleversement de la politique internationale par la dissémination des moyens numériques, une perturbation du système international, déstabilisation des relations internationales et une reconfiguration géopolitique, création de nouvelles alliance numérique, etc.

4/ Les motivations

Les motivations ne sont plus seulement politiques, elles deviennent à la fois économiques et sociales, c'est-à-dire touchent à toutes les préoccupations sociales. Au plan économique, les attaques sont motivées essentiellement par l'argent que les attaquants cherchent à en dérober. Dans certains cas, ils cherchent à se positionner par rapport à des concurrents économiques, en leur volant leurs secrets industriels et commerciaux, leurs bases de clients, leur savoir-faire, en les décrédibilisant. Ce sont des mafias, des mercenaires, des cybercriminels, ou plus généralement des concurrents peu scrupuleux. Ils arnaquent et rançonnent. Ils utilisent couramment les cryptomonnaies qu'ils minent pour s'enrichir en se servant de ressources dont ils ont détourné frauduleusement l'utilisation, ou dont ils tirent parti pour rendre leurs flux financiers discrets voire anonymes.

Au plan social, on peut avoir des motivations émotionnelles ou sentimentales : Les attaquants sont ici un salarié fâché contre son employeur, ou un amoureux jaloux, éconduit ou trompé. Ils cherchent par exemple à se venger ou à obtenir des informations pouvant humilier le partenaire contre lequel on est fâché.

Au plan défensif, une attaque cyber peut être menée en riposte à une première attaque. Plusieurs cas de figures peuvent se présenter : « rendre la pareille » à l'attaquant original, en rentrant dans le jeu risqué de l'escalade du conflit ; neutraliser les effets d'une attaque dont on serait la victime. Ces démarches de riposte, dans la mesure où elles pourraient paraître légitimes, soulèvent de nombreuses questions politiques, légales et techniques.

5/ Constat général 2 : Les motivations demeurent politiques mais progressivement avec la diffusion de l'informatique et du numérique sur l'ensemble de la société, les motivations deviennent d'abord économiques ensuite sociales. Les régions d'origine des premières attaques majeures demeurent l'Occident (USA, Europe de l'ouest, Europe de l'Est, etc), l'Asie (Iran, Chine, etc.) et se sont répandues désormais dans tous les pays d'Afrique.

CHAPITRE 3

LA CYBERSECURITE ET SES REPONSES A LA CYBERCRIMINALITE

(1)

Les réponses politiques et juridiques

- **Les réponses onusiennes**

  -Maintien de la paix et la sécurité internationale : permettre numériquement la construction et le maintien d'une forme de paix, de sécurité et de stabilité stratégique du cyberespace.

  -Dès 1998, présentation d'un projet de résolution porté par la Fédération de Russie et intitulé « Les progrès de la téléinformatique dans le contexte de la sécurité internationale » qui va lancer la machine onusienne, en inscrivant pour la première fois ce point à l'ordre du jour de la session ordinaire de l'AG des Nations unies. Par la suite,

et ce jusqu'en 2016 inclus, la représentation russe présentera tous les ans un projet de résolution visant à poursuivre cette séquence de travail.
-Convention des Nations unies contre la cybercriminalité (24 décembre 2024) pour harmoniser les législations, faciliter les enquêtes conjointes et améliorer l'extradition des cybercriminels à l'échelle internationale
-Groupe de travail non limité de l'AGNU pour débattre des règles de comportement responsable et prévenir les conflits utilisant les TIC entre puissances mondiales
-Le Centre international de calcul des Nations Unies (CICNU) fournit des solutions Common Secure pour la gouvernance, la supervision et la réponse aux menaces pour ses 90 partenaires onusiens

---

CHAPITRE 4

LA CYBERSECURITE ET SES REPONSES A LA CYBERCRIMINALITE

(2)

Les réponses administratives et techniques

1/ Les réponses administratives

-Création des départements et des unités de sécurité des systèmes d'information dans les administrations avec cellules de veille.

-Sensibilisation des personnels et employés sur les mesures à prendre pour la sécurité des données et des systèmes d'information dans les administrations

-Formation et renforcement permanent des capacités des personnels

-Mise en place des meilleures conditions de travail des personnels et des employés

- Mise en place de la sécurité physique des employés…

2/ Les réponses techniques

Lorsqu'il s'agit de protéger la couche physique et la couche logique, il existe de grands types de protections informatiques :

-**Protection du réseau** : sécurité entre les différents appareils situés sur le même réseau. Dans ce cas, la protection logicielle et la protection matérielle sont toutes deux importantes. Il faut empêcher que des personnes non autorisées agissent sur le système de façon malveillante : connaître le système d'exploitation, réduire l'accès au réseau, réduire le nombre de points d'entrée (ports), définir une politique de sécurité interne (mot de passe, etc.), déployer des utilitaires de sécurité…

Les meilleures pratiques en matière de protection des logiciels consistent à s'assurer que les solutions de protection logicielle restent pertinentes et fonctionnent à votre avantage : Maintenir les logiciels à jour et corrigés. Les services et outils de protection logicielle peuvent aider les utilisateurs de logiciels à rester sur la bonne voie

en ce qui concerne la maintenance et l'inventaire d'un large choix de programmes logiciels.

-Protection des points de terminaison : les ordinateurs portables, les téléphones, les ordinateurs, les tablettes, etc. doivent être sécurisés (là encore, tant au niveau des logiciels que du matériel) afin d'éviter que des utilisateurs indésirables ne s'infiltrent. Cela implique souvent diverses méthodes de chiffrement, de contrôle des utilisateurs et, bien sûr, de protection des logiciels.

-Sécurité d'Internet : ou cybersécurité elle concerne le transit et l'utilisation de l'information. Les attaques de cybersécurité se produisent lorsque des informations sont interceptées. C'est pourquoi plusieurs couches de chiffrement et d'authentification sont généralement utilisées pour stopper ces attaques. **Protection du cloud** : réduire les risques liés à la protection des logiciels dans le cloud. Il s'agit de sécuriser les transferts de données et les dispositifs sur le même réseau.

-Le principe du moindre privilège : donner aux utilisateurs de logiciels un accès minimal aux programmes afin qu'ils puissent faire leur travail. Ne pas donner accès à des fonctionnalités, des droits d'accès et des contrôles que les employés n'ont pas besoin d'utiliser. Par cette politique on réduit le risque d'attaques en veillant à ce que personne ne modifie accidentellement les droits d'accès par erreur ou n'ait accès à des informations dont il n'a pas besoin. Il faut par ailleurs réévaluer les privilèges lorsque les employés changent de poste, terminent des projets et, bien sûr, quittent l'entreprise.

-Automatisation des tâches de protection logicielle : Dans l'impossibilité de suivre manuellement le large éventail de tâches à effectuer régulièrement, il faut procéder à l'automatisation. Les services informatiques devraient automatiser les tâches régulières qui sont importantes pour les logiciels de protection informatique, telles que les configurations de sécurité, l'analyse des modifications apportées aux pare-feu, etc. Pour automatiser, les entreprises doivent investir dans les bons outils et solutions de protection logicielle.

-La formation des employés : Prévoir une journée par trimestre pour examiner les risques liés à la protection des logiciels, les raisons pour lesquelles ces informations sont importantes et ce que les employés peuvent faire pour assurer leur propre sécurité et celle de l'entreprise ou l'organisme. Il est également important d'apprendre aux employés à reconnaître les signes d'attaques de sécurité, de tentatives d'hameçonnage, etc.

Dans la formation l'on peut établir un plan de protection logiciel : Si quelque chose se passe mal, comment allez-vous réagir ? Comment allez-vous détecter une attaque et vous assurer que vous subissez le moins de dommages possible en conséquence ?

Se documenter, surveiller et mesurer : Mettre par écrit toutes les politiques de protection logicielle afin que tous les membres du personnel y aient accès et comprennent parfaitement les processus concernés (Ne pas oublier de les montrer aux nouveaux employés !).

Conclusion générale

Phénomène qui émerge en Europe occidentale et se dissémine dans toutes les parties de la planète dans un contexte de guerre et de rivalités plus générale entre les grandes puissances et en fonction du taux de pénétration d'Internet et d'utilisation des NTIC…la cybercriminalité a d'abord été étatique avant de se muer en actes individuels, collectifs et non-étatiques. Les personnes ou les groupes qui agissent à l'intérieur de l'Etat ou à travers les frontières prospèrent non seulement à cause de la fragilité des systèmes juridiques et administratifs existants, mais aussi grâce à la diffusion de l'informatique et de l'internet sur l'ensemble de la société. Les réponses étatiques existent (droit, justice, technique, etc.), mais elles ne sont pas suffisantes. En attendant leur amélioration la société doit travailler à une plus grande sensibilisation des populations au phénomène de la cybercriminalité dont la lutte doit être holistique. Le droit, la justice, l'économie, la psychologie, la sociologie, l'histoire, la technique, la science politique doivent tous contribuer à la compréhension et à la lutte contre la cybercriminalité. L'histoire en nous retraçant les origines du phénomène, nous permet d'interroger les pratiques et les auteurs qui peuvent mieux lutter contre la cybercriminalité. L'informatique et internet ayant été d'abord des outils à l'usage des armées ne doivent-ils pas revenir dans leur giron pour qu'ils soient mieux contrôlé ?

QUESTIONS AUX ETUDIANTS

3. Quelles sont les causes (techniques, sociales, économiques et politiques) de la cybercriminalité ?

- Faible degré de sophistication des systèmes d'information et des dispositifs techniques de protection ;
- Marginalisation sociale, rancunes émotionnelles et affectives, exhibition technique, etc.
- Recherche du gains, escroqueries diverses et détournements de deniers publics, etc.
- Repressions politiques

4. Quels sont les objectifs ou motivations des cybercriminels ?

- Les motivations politiques

Ces motivations servent ici à ce qui s'apparente à une « cause nationale ». Les attaquants sous le couvert des Etats sont amenés à espionner d'autres États, et à leur dérober leurs secrets, tels que des stratégies diplomatiques dans le cadre de négociations internationales. Ils cherchent à les déstabiliser, en s'attaquant par exemple à la crédibilité de leurs processus électoraux. Ils cherchent encore à les agresser en attaquant leurs infrastructures critiques nationales. Ce sont souvent des unités spécialisées, en lien de près ou de loin avec des organisations militaires ou des

services de renseignement. Leur démarche est généralement professionnelle, rigoureusement planifiée, ciblée et peut mettre en œuvre des outils sophistiqués.

- **Les motivations lucratives et compétitives**

Ici, les attaques sont motivées essentiellement par l'argent que les attaquants cherchent à en dérober. Dans certains cas, ils cherchent à se positionner par rapport à des concurrents économiques, en leur volant leurs secrets industriels et commerciaux, leurs bases de clients, leur savoir-faire, en les décrédibilisant. Ce sont des mafias, des mercenaires, des cybercriminels, ou plus généralement des concurrents peu scrupuleux. Ils arnaquent et rançonnent. Ils utilisent couramment les cryptomonnaies qu'ils minent pour s'enrichir en se servant de ressources dont ils ont détourné frauduleusement l'utilisation, ou dont ils tirent parti pour rendre leurs flux financiers discrets voire anonymes.

- **Les motivations Emotionnelles ou sentimentales**

Les attaquants sont ici un salarié fâché contre son employeur, ou un amoureux jaloux, éconduit ou trompé. Ils cherchent par exemple à se venger ou à obtenir des informations pouvant humilier le partenaire contre lequel on est fâché.

- **Les motivations Ludiques ou récréatives**

Il s'agit de s'amuser, de relever des défis techniques, pour la beauté du geste, pour en reverser les résultats dans la communauté à des fins d'amélioration ou encore, pour les plus égocentriques, pour se vanter.

- **Les motivations Défensives**

Une attaque cyber peut être menée en riposte à une première attaque. Plusieurs cas de figures peuvent se présenter : « rendre la pareille » à l'attaquant original, en rentrant dans le jeu risqué de l'escalade du conflit ; neutraliser les effets d'une attaque dont on serait la victime. Ces démarches de riposte, dans la mesure où elles pourraient paraître légitimes, soulèvent de nombreuses questions politiques, légales et techniques.

5. Quelle est la différence entre une cybermenace et une cyberattaque ?

6.Quelles sont les différentes formes de cyberattaques ?

- Hameçonnage, attaque par intercepteur, écoute électronique par réseau wifi, mystification, attaque hors sol, cassage de mot de pass, attaque par force brute, bourrage d'identifiant, attaque par dictionnaire, Déni de service, attaque par inondation, attaque par arrêt de service, Déni de service distribué, Harponnage, exploit et trousse d'exploit, injection de code, exploit sur web, attaque par téléchargement furtif, piratage psychologique, détournement de formulaire, détournement de domaine, compromission de courriel d'affaires, typosquattage, minage clandestin, attaque par embuscade, porte dérobée, reconnaissance, etc.

7. Quelles sont les conséquences (techniques, sociales, économiques et politiques) de la cybercriminalité ?

Techniquement, les différentes attaques et menaces numériques présentent des dangers sur toutes les trois couches du cyberespace que sont la couche physique ou matérielle, la couche logique et la couche cognitive.

La couche physique ou couche inférieure comprend l'infrastructure matérielle qui est à la base de l'internet et qui est composé des câbles de fibre optique, les routeurs, les serveurs, la technologie cellulaire, les satellites, les ordinateurs personnels, smartphones, tablettes, etc. **C'EST LE HARDWARE.**

Cette couche se compose de l'ensemble des périphériques d'accès et des infrastructures nécessaires à leur fonctionnement chez les fournisseurs de connexion, les systèmes de transmission, les relais (satellites), ainsi que les grands nœuds d'interconnexions des réseaux, gérés par des grossistes, les câbles sous-marins, les satellites, et les fermes de données où résident les informations.

La couche logique ou syntaxique qui comprend les services protocoles, programmes, applications, etc. et qui permet d'assurer la transmission des données entre deux points du réseau et donc de faire voyager l'information jusqu'à son destinataire. C'est le software= les logiciels qui permette à notre ordinateur de fonctionner et assurent le traitement des données. On distingue généralement le logiciel de base et le logiciel d'application. Partie immatérielle ou partie intelligente de l'ordinateur.

iii) La couche sémantique ou cognitive ou couche supérieure qui est l'espace de l'information, des réseaux sociaux, des discussions et des échanges instantanés dans le monde, les contenus que nous diffusons au quotidien à travers nos ordinateurs, nos smartphones, etc.

- **Exemples :** En 2018 des usines chinoises avaient implanté des puces de surveillance et de contrôle du réseau sur des cartes mères fabriquées pour Supermicro. Avant cela des défaillances de composants avaient été détectées chez des entreprises de défense telles que Raytheon, BAE, Northrop Grumman et Lockheed. La National Security Agency a aussi demandé aux fabricants américains d'implanter une porte dérobée dans les produits exportés.
- De nombreux processeurs partagent des zones de mémoire cachées, où ils peuvent laisser des informations qui deviennent alors vulnérables. La solution contre les attaques du wardware réside sur de nouvelles architectures qui permettent d'isoler physiquement les informations critiques. Cela a un coût et seuls les entreprises bancaires et organismes militaires se permettent ces solutions.
- Selon le site Techniques de l'Ingénieur (TI), les attaques visant le hardware ont d'abord été imaginées pour le vol de données bancaires sur les puces des cartes bleues**.** Ces approches sont à présent appliquées aux téléphones portables, dont

les circuits sont mal protégés. Avec l'Internet des objets, la situation est encore pire où les appareils sont à la fois omniprésents et très peu, voire pas du tout, sécurisés.

- Tous les appareils électroniques (ordinateurs, réseaux de communication, capteurs…) intégrant des processeurs (partie de l'ordinateur qui interprète et exécute les instructions) sont exposés. Il suffit qu'un composant physique soit compromis pour impacter les différentes couches de cybersécurité d'un système.