THÈME I/ LA CYBERCRIMINALITÉ

Introduction

La démocratisation de l'informatique et la globalisation des réseaux ont favorisé le développement du cybercrime. Les nouvelles technologies sont utilisées par des hackers pour attaquer la sécurité des systèmes informatiques et les droits d'autrui **(ex : téléchargement illégal, contrefaçon, atteinte aux données personnelles).**

La Cybercriminalité

Définition

La cybercriminalité est la troisième grande menace mondiale après les armes chimiques, bactériologiques et nucléaires. C'est une criminalité située dans le « cyberespace », un espace virtuel. Selon l'ONU (**Organisation des Nations Unies**) , elle désigne tout comportement illégal via des opérations électroniques visant la sécurité des systèmes informatiques et des données.

Les attaques cybercriminelles consistent en des actions menées par des cybercriminels à l'aide d'ordinateurs contre d'autres systèmes pour voler des données personnelles ou autres.

Cybercrime vs Crime informatique

- Crime informatique : les systèmes et réseaux sont la cible unique.
- Cybercrime : utilisation d'ordinateurs ou réseaux pour commettre des crimes traditionnels (ex : fraude, intrusion).
- Cyberespace : lieu favorable au crime grâce à l'anonymat.

Types d'infractions

1. Infractions spécifiques aux TIC : atteintes aux systèmes, données personnelles, cartes bancaires.
2. Infractions liées aux TIC : pédopornographie, incitation à la haine, atteintes aux personnes privées.
3. Infractions facilitées par les TIC : escroqueries en ligne, blanchiment, contrefaçon.

Cybercrime et intelligence artificielle (IA)

L'IA, développée depuis les années 1950, imite l'intelligence humaine via des algorithmes. Elle permet d'analyser rapidement de grandes données.

Utilisations de l'IA dans la lutte contre la criminalité

- Analyse vidéo et données pour prédire et résoudre des crimes (police prédictive).s

- Reconnaissance faciale et vocale pour identifier criminels et transcrire interrogatoires.
- Analyse des réseaux sociaux pour détecter profils suspects et activités illicites.
- Surveillance via caméras IA pour identifier véhicules et suspects.
- Prédiction du risque de récidive chez les délinquants.

Risques liés à l'IA

L'IA augmente la productivité et la sophistication des cybercriminels. Des IA génératives comme WormGPT sont utilisées à des fins criminelles. L'accès à ces technologies facilite la cybercriminalité, même pour des acteurs peu qualifiés.

Question I : Apparition et développement du phénomène

- Le piratage a commencé dans les années 1970 avec les « Phreakers » qui manipulaient les téléphones pour appels gratuits.
- En 1990, l'opération Sundevil du FBI a saisi ordinateurs et disquettes liés à des fraudes.
- La première loi anti-cybercrime américaine date de 1986 (Computer Fraud and Abuse Act).
- Aujourd'hui, le cybercrime touche aussi bien le web public que le Dark Web.
- Les objets connectés (smartphones, caméras, consoles) sont des portes d'entrée pour les pirates.
- Exemple : en 2017, 29 millions de comptes Facebook piratés, exposant noms, emails, numéros de téléphone, et autres données personnelles.

Question II : Cybercriminalité et conséquences économiques

- Le cybercrime coûte chaque année des milliards de dollars aux entreprises et particuliers.
- La contrefaçon et le piratage via Internet coûtent plus de 100 milliards de dollars par an, mettant en danger la santé publique et le développement économique.
- OMS : **(Organisation Mondiale de la Santé)**.plus de 10 % des médicaments sur le marché mondial sont contrefaits, 25 % dans les pays en développement.
- Coût mondial de la cybercriminalité estimé à 1 trillion de dollars en 2019, avec une hausse liée à la COVID-19.
- Les formes les plus coûteuses pour les entreprises sont : espionnage économique, criminalité financière, ransomwares.

- Pour les particuliers, les pertes financières sont souvent moindres mais les impacts sociaux sont importants.

Question III : Les différentes formes de la cybercriminalité

A. Formes du cybercrime

1. Crimes visant réseaux ou appareils : piratage, intrusion.
2. Crimes utilisant ces dispositifs pour commettre d'autres crimes : virus, phishing, cyberharcèlement.

Le **phishing** est une **arnaque en ligne** où des pirates imitent des sites ou e-mails officiels pour **voler des informations personnelles**.

10 catégories principales (selon F. Colantonio) :

1. Vol de services télécom (phreaking).
2. Espionnage des télécommunications.
3. Crimes classiques facilités (blanchiment, pédopornographie, vol d'identité, harcèlement).
4. Vandalisme (attaques gratuites ou protestataires).
5. Ventes et investissements frauduleux (spéculation, usurpation).
6. Extorsions de fonds (chantage, ransomwares).
7. Vol d'argent par usurpation d'identité financière (phishing, pharming).
8. Diffusion de contenus immoraux ou dangereux (pornographie, racisme, apologie du terrorisme).
9. Violation de la propriété intellectuelle (piratage, contrefaçon).
10. Escroqueries et piratage (collecte illicite de données, manipulation psychologique).

B. Profils des cybercriminels

- **Hackers** : spécialistes en informatique, avec diverses motivations (curiosité, gain, nuisance).
- **Hacktivistes** : activistes divulguant des informations confidentielles pour des causes sociales, politiques ou religieuses (ex : Anonymous, WikiLeaks).

C. Techniques utilisées

- **Spyware** : logiciels espions volant des informations à l'insu de l'utilisateur (keyloggers, rootkits, adware).

- **Ransomware** : logiciel malveillant bloquant les données d'une victime et demandant une rançon en cryptomonnaie.

Le Dark Web et les Data Brokers

- Le Dark Web est une partie cachée d'internet, accessible via des logiciels comme Tor, utilisée pour des activités illégales (vente de données, cyberattaques, trafic).
- Le Dark Web est intraçable, rendant difficile la localisation des cybercriminels.
- Les Data Brokers collectent et vendent des données personnelles issues de sources en ligne, créant des profils détaillés vendus à des entreprises diverses.

Question VI : Dispositif législatif et réglementaire

Problèmes législatifs

- Difficultés liées aux lacunes législatives et à la stricte interprétation du droit pénal.
- Distinction entre lieu public et privé à l'ère du numérique.
- Nouveaux crimes comme l'apologie du terrorisme et espionnage électronique.
- Nouveaux moyens de preuve électroniques (signatures, QR codes, vidéos).

Protection des données personnelles

- Loi tunisienne n° 2004-63 sur la protection des données personnelles, adhésion à la convention 108 de 2017.
- Droits des personnes : information, accès, opposition, droit à l'oubli.
- Sanctions administratives et pénales en cas de violation.
- Obligation pour les responsables de traitement d'assurer la sécurité des données.

Lutte internationale

- Convention de Budapest (2001) : harmonisation des législations, modernisation des procédures, coopération internationale.
- Organismes internationaux : INTERPOL, EUROPOL, EUROJUST.

Lutte nationale

- Instances tunisiennes : INPDCP, ATI, ANSI.
- Décret-loi n° 2022-54 relatif à la lutte contre les infractions liées aux systèmes d'information.

- Pouvoirs des autorités : saisie, interception, collecte de preuves électroniques.
- Sanctions pénales pour accès illégal, interception, modification de données, fraude, falsification, diffusion de fausses informations.

Question IV : Mesures de protection et de lutte

Au niveau des utilisateurs

- Sensibilisation aux risques du cyberespace et à la valeur économique des données personnelles.
- Utilisation d'outils de protection comme les pare-feu.
- Contrôle accru sur ses données via des outils comme le "digital labor".

Au niveau des entreprises

- Simplification des politiques de confidentialité (langage clair, infographies).
- Concepts de **Privacy By Design** (protection intégrée dès la conception) et **Privacy By Default** (paramètres de sécurité par défaut).
- Sécurisation des postes de travail, serveurs, sites web (pare-feu, antivirus, mises à jour).
- Prévention, détection et réaction face aux cyberattaques.
- Techniques comme l'anonymisation et la pseudonymisation des données.

Protection des mineurs sur Internet

- Les mineurs sont exposés à des contenus violents, cyberintimidation, cyberchantage, jeux dangereux.
- Internet crée une dépendance et des troubles physiques chez les jeunes.
- Risques liés à la pédopornographie et exploitation sexuelle.
- Statistiques montrent un usage précoce et avancé d'Internet par les adolescents.
- Cadre juridique : Constitution tunisienne, Code de la protection de l'enfant, lois sur la protection des données.
- Mesures techniques : logiciels de contrôle parental, blocage des sites dangereux.
- Équilibre nécessaire entre protection et liberté d'expression.