COMITÉ : Légal

QUESTION : Législation sur la cybersécurité/cybercriminalité.

MEMBRES DE L'ÉTAT-MAJOR : Matthaios Giannaros

POSITIONS : Vice-Président

Table des matières :

Introduction personnelle :

Chers délégués, Je m’appelle Matthaios Giannaros, j’ai 16 ans, et je suis élève au LFHED. En tant que vice-président du Comité Légal, sous la présidence de Irida Kapatai, j’ai l’honneur de vous présenter ce sujet essentiel: la législation sur la cybersécurité et la cybercriminalité.

À l’ère du numérique, la cybersécurité est un enjeu majeur pour les États, les entreprises et les citoyens. Les cyberattaques se multiplient, menaçant la protection des données personnelles, la stabilité des infrastructures et la souveraineté des nations. Face à ces défis, il est primordial de trouver un équilibre entre sécurité et libertés individuelles, tout en encourageant une coopération internationale efficace pour lutter contre la cybercriminalité.

J’espère qu’à travers cette conférence, vous trouverez ce sujet aussi captivant que moi et que vous tirerez pleinement profit de cette expérience enrichissante du MUN. Si vous avez besoin d’aide pour votre préparation, n’hésitez pas à me contacter.

Introduction:

La cybercriminalité est née avec l'avènement d'Internet et des technologies numériques dans les années 1990. À ses débuts, elle se limitait à des activités relativement simples, comme le piratage informatique ou les escroqueries par phishing (arnaques en ligne qui cherchent à tromper une personne pour lui voler des informations sensibles comme ses mots de passe, numéros de carte bancaire, ou codes d’accès). Cependant, avec l'évolution rapide des technologies, la cybercriminalité est devenue plus sophistiquée et organisée. Aujourd'hui, elle englobe un large éventail d'activités malveillantes, telles que le vol de données, les rançongiciels, le piratage de systèmes gouvernementaux et même le cyberterrorisme. Notre dépendance croissante aux appareils électroniques et à Internet a amplifié les risques, faisant de la cybersécurité un enjeu mondial majeur. De nos jours, la cybersécurité concerne aussi bien les gouvernements que les entreprises et les citoyens. Chaque jour, des millions de cyberattaques sont recensées, mettant en danger des données personnelles, des infrastructures essentielles (comme les réseaux électriques, les systèmes de santé et les services financiers) et la stabilité économique (par exemple, en perturbant les chaînes d'approvisionnement ou en causant des pertes financières directes). Avec l’essor du numérique, la cybercriminalité est devenue plus sophistiquée et difficile à combattre. Les cyberattaques peuvent prendre différentes formes, comme le vol d’informations, les rançongiciels ou le piratage de systèmes gouvernementaux. Par exemple, en 2017, l’attaque WannaCry a paralysé des hôpitaux, des entreprises et des institutions publiques dans plus de 150 pays, montrant à quel point nos sociétés sont vulnérables.

Les conséquences de ces attaques peuvent être graves, entraînant des pertes financières, une érosion de la confiance dans les systèmes numériques et même des violations des droits humains. La protection des données est cruciale car les fuites d'informations personnelles peuvent exposer des individus à des risques d'usurpation d'identité, de harcèlement ou de discrimination. Par exemple, la divulgation non autorisée de données médicales peut compromettre la vie privée et la dignité des personnes. De plus, les cyberattaques contre des infrastructures critiques, comme les

hôpitaux, peuvent mettre des vies en danger, violant ainsi le droit fondamental à la sécurité et à la santé.
Afin de mieux protéger les utilisateurs, plusieurs pays ont mis en place des lois, comme le RGPD en Europe ou le Cloud Act aux États-Unis.

Cependant, la cybercriminalité ne s'arrête pas aux frontières, ce qui rend la coopération internationale essentielle. Étant donné que la cybersécurité est un enjeu majeur pour la protection des données et des infrastructures, il est nécessaire d'agir ensemble au sein des Nations Unies pour renforcer la législation et assurer un cyberespace plus sûr. Cette collaboration est indispensable pour prévenir les violations des droits humains, protéger les économies nationales et garantir la stabilité mondiale.

Définition des termes clés

Cybersécurité : Ensemble des mesures prises pour protéger les systèmes informatiques, les réseaux et les données contre les attaques malveillantes. Elle vise à garantir la confidentialité, l'intégrité et la disponibilité des informations.

Cybercriminalité : Infractions commises à l'aide d'outils numériques, comme le vol de données, la fraude en ligne, le piratage de systèmes ou la diffusion de logiciels malveillants.

Piratage informatique (Hacking) : Accès non autorisé à un système informatique pour voler, modifier ou détruire des données. Certains hackers sont criminels, d'autres (appelés "hackers éthiques") aident à améliorer la sécurité.

Rançongiciel (Ransomware) : Logiciel malveillant qui bloque l'accès aux fichiers d'un utilisateur et exige une rançon pour les débloquer. Ex : l'attaque WannaCry en 2017 a touché plus de 300 000 ordinateurs dans 150 pays.

Données personnelles : Informations permettant d'identifier une personne, comme son nom, adresse, numéro de téléphone, adresse IP ou historique de navigation. Leur protection est un enjeu clé en cybersécurité.

RGPD (Règlement Général sur la Protection des Données) : Loi européenne adoptée en 2018 pour protéger les données personnelles des citoyens. Elle impose aux entreprises et organisations de respecter des règles strictes sur l'utilisation et la sécurisation des données, sous peine de sanctions importantes.

Cyberterrorisme : Utilisation des technologies numériques pour mener des attaques visant à semer la peur, perturber des infrastructures essentielles ou influencer des décisions politiques.

Protection des données : Ensemble des lois et réglementations visant à encadrer l'utilisation et la sécurisation des informations personnelles. Le RGPD en Europe est un exemple de cadre légal mis en place pour cela.

Ingénierie sociale : Technique de manipulation psychologique utilisée par les cybercriminels pour inciter une personne à révéler des informations confidentielles (ex : arnaques par email, faux appels téléphoniques).

Coopération internationale en cybersécurité : Collaboration entre différents pays et organisations pour lutter contre la cybercriminalité, partager des informations et établir des réglementations communes.

Cloud Act (Clarifying Lawful Overseas Use of Data Act) : Loi adoptée par les États-Unis en 2018, permettant aux autorités américaines d'accéder aux données stockées sur des serveurs à l'étranger si elles appartiennent à une entreprise américaine (comme Microsoft, Google ou Apple). Cette loi pose des questions sur la souveraineté numérique et la protection des données personnelles, car elle peut entrer en conflit avec des réglementations comme le RGPD en Europe.

Cyberespace : Espace virtuel créé par l'ensemble des réseaux informatiques, où les informations circulent à travers Internet et d'autres infrastructures numériques. Il n'a pas de frontières physiques, ce qui rend sa gouvernance et sa sécurité complexes. Le cyberespace est utilisé pour la communication, l'économie, la politique et même les conflits, d'où l'importance d'une régulation internationale.

Cyberattaque
Action malveillante visant un système informatique dans le but de l'endommager, de le perturber, de voler des données ou de prendre le contrôle à distance. Elle peut être menée par des individus, des groupes ou des États.

Maliciel (Malware)
Logiciel malveillant conçu pour infiltrer, endommager ou perturber un système informatique, souvent sans le consentement de l'utilisateur. Exemples : virus, chevaux de Troie, ransomware.

Phishing (Hameçonnage)
Technique de cyberattaque visant à tromper un utilisateur afin qu'il fournisse des informations confidentielles (mots de passe, numéros de carte bancaire, etc.) en se faisant passer pour une entité de confiance.

Violation de données (Data breach)
Accès, divulgation ou vol non autorisé de données personnelles ou confidentielles stockées sur un système ou un réseau.

Infrastructure critique
Systèmes et actifs essentiels au bon fonctionnement d'un pays, tels que les réseaux d'énergie, les hôpitaux, les services financiers, qui sont particulièrement vulnérables aux cyberattaques.

Loi sur la cybersécurité
Ensemble de règles ou de régulations nationales ou internationales visant à encadrer la sécurité numérique et à sanctionner les actes de cybercriminalité.

Attribution des attaques
Processus technique et juridique permettant d'identifier l'auteur d'une cyberattaque, ce qui reste complexe en raison de l'anonymat et de la déterritorialisation d'Internet.

Responsabilité des États dans le cyberespace
Principe du droit international selon lequel un État peut être tenu responsable s'il commet ou soutient une cyberattaque qui viole les normes internationales.

Convention de Budapest
Premier traité international visant à lutter contre la cybercriminalité, adopté en 2001 par le Conseil de l'Europe. Il fixe des standards juridiques pour la coopération internationale et la criminalisation de certains actes.

Souveraineté numérique
Capacité d'un État à contrôler ses infrastructures numériques, ses données et à faire respecter ses lois dans le cyberespace.

Interpol Cybercrime Directorate
Branche d'INTERPOL chargée de coordonner la lutte internationale contre la cybercriminalité en facilitant la coopération policière entre les États membres.

Aperçu général :

La cybersécurité et la cybercriminalité sont des enjeux majeurs à l'ère du numérique. Avec l'explosion des technologies de l'information et de la communication, les cyberattaques se multiplient, menaçant la sécurité des données, la stabilité des infrastructures critiques et la souveraineté des nations.
Cybersécurité

La cybersécurité désigne l'ensemble des mesures prises pour protéger les systèmes informatiques, les réseaux et les données contre les accès non autorisés, le vol ou les dommages. Elle englobe un large éventail de pratiques, de technologies et de politiques visant à garantir la confidentialité, l'intégrité et la disponibilité des informations. Les domaines clés incluent :

- **Protection des données personnelles** : Assurer que les informations sensibles, telles que les numéros de sécurité sociale, les coordonnées bancaires et les dossiers médicaux, sont protégées contre les violations.
- **Sécurisation des infrastructures critiques** : Protéger les services essentiels comme les réseaux électriques, les systèmes de transport et les établissements de santé contre les cyberattaques.
- **Prévention de la fraude financière** : Mettre en place des mesures pour empêcher les escroqueries en ligne, le vol d'identité et les transactions non autorisées.

L'importance de la cybersécurité a augmenté de manière exponentielle avec la transformation numérique, le cloud computing et l'Internet des objets (IoT). Cependant, à mesure que la technologie évolue, les méthodes utilisées par les cybercriminels se sophistiquent, faisant de la cybersécurité un domaine en constante évolution.

Les causes de la cybercriminalité

La cybercriminalité est un phénomène en pleine croissance. Plusieurs raisons expliquent pourquoi elle se développe aussi vite.

1. L’argent : la principale motivation

Beaucoup de cybercriminels agissent pour gagner de l’argent facilement. Ils utilisent différentes méthodes pour voler ou escroquer les gens. Par exemple, certains utilisent des rançongiciels : ils bloquent l’accès à un ordinateur ou à des fichiers importants, puis demandent de l’argent pour les débloquer.

D’autres font du phishing (ou hameçonnage), en envoyant de faux e-mails qui ressemblent à ceux de vraies entreprises. Leur but est de pousser les gens à donner leurs mots de passe ou leurs informations bancaires.

Enfin, certaines personnes vendent des données personnelles volées sur des sites illégaux comme le dark web, un espace d'Internet difficile à surveiller.

2. Les raisons politiques ou idéologiques

Certaines cyberattaques ne sont pas faites pour de l'argent, mais pour des raisons politiques. Par exemple, des États utilisent l'informatique pour espionner d'autres pays, voler des informations confidentielles, ou même perturber des élections.

Il existe aussi des groupes comme Anonymous qui attaquent des sites ou des entreprises pour défendre des idées ou des causes. Ces groupes se considèrent souvent comme des "justiciers" du web.

3. Le progrès de la technologie

Les nouvelles technologies comme l'intelligence artificielle, la 5G ou les objets connectés créent de nouvelles opportunités… mais aussi de nouveaux dangers. Par exemple, un frigo connecté mal protégé peut être utilisé pour mener une attaque informatique.

Les cybercriminels profitent souvent du manque de sécurité de ces nouvelles technologies, car les fabricants n'ont pas toujours le temps ou les moyens de tout protéger.

4. Le manque de connaissances en cybersécurité

Beaucoup de gens ne savent pas comment se protéger sur Internet. Ils utilisent des mots de passe faciles, ne mettent pas à jour leurs logiciels ou cliquent sur des liens suspects. Ces erreurs rendent leur ordinateur vulnérable.

Dans les entreprises, de nombreux employés ne sont pas bien formés, ce qui peut causer de graves problèmes si un pirate réussit à entrer dans le système.

5. Un monde connecté et sans frontières

Internet est mondial, ce qui veut dire que les criminels peuvent agir depuis n'importe quel pays. Grâce à des outils comme les VPN ou des cryptomonnaies, ils peuvent rester anonymes et difficiles à retrouver.

Cela rend la justice compliquée : même si on découvre qui est responsable d'une attaque, il est parfois impossible de l'arrêter car il vit dans un pays où il n'est pas puni.

6. L'intelligence artificielle : une nouvelle arme

Avec les progrès rapides de l'intelligence artificielle (IA), de nouveaux risques apparaissent. Par exemple, des cybercriminels peuvent utiliser des IA pour créer de faux messages, imiter des voix ou traduire automatiquement des textes dans plusieurs langues pour toucher plus de victimes.

L'IA peut aussi aider les pirates à automatiser leurs attaques, à tester des millions de mots de passe en quelques minutes, ou à identifier plus facilement les failles de sécurité.

Les conséquences de la cybercriminalité

La cybercriminalité a de nombreuses conséquences, qui touchent aussi bien les particuliers que les entreprises ou les gouvernements.

1. Des pertes d'argent importantes

Les entreprises qui subissent une cyberattaque doivent réparer les dégâts, protéger leurs clients, ou même payer des rançons. Cela peut leur coûter des millions, voire des milliards d'euros. Les petites entreprises sont souvent les plus touchées car elles sont moins bien protégées.

Les particuliers aussi peuvent perdre de l'argent à cause de fraudes bancaires ou de vols de données.

2. La vie privée est en danger

Quand des données personnelles sont volées (comme des adresses, des mots de passe, des dossiers médicaux), cela peut causer de gros problèmes. Les gens peuvent se faire voler leur identité, ou être harcelés.

Certaines personnes perdent confiance dans les services numériques et évitent de les utiliser, surtout si elles ont déjà été victimes.

3. Les services essentiels peuvent être bloqués

Des attaques peuvent bloquer des hôpitaux, des transports, ou même des réseaux électriques. Cela peut avoir des conséquences graves, par exemple si un hôpital ne peut plus soigner ses patients à cause d'une panne informatique.

Ce genre d'attaque montre que la cybercriminalité peut mettre des vies en danger.

4. Moins de confiance dans les outils numériques

Quand les cyberattaques se multiplient, les gens deviennent plus méfiants. Ils hésitent à acheter en ligne, à utiliser des applications ou à faire confiance aux services publics. Cela peut freiner le progrès, car la société a besoin du numérique pour avancer.

5. Un danger pour la sécurité nationale

Enfin, certaines cyberattaques visent directement les gouvernements ou les militaires. Elles peuvent voler des informations secrètes, désorganiser un pays, ou même l'influencer politiquement.

Certains experts pensent que les guerres de demain se feront aussi sur Internet, avec des attaques informatiques contre les pays ennemis.

6. L'exposition des jeunes à des contenus dangereux

Internet peut aussi exposer les jeunes à des contenus violents, illégaux ou dangereux :

- accès facile à la drogue,
- marchés noirs sur le dark web,
- groupes incitant à la violence ou à la criminalité.

Cela peut pousser certains adolescents à s'enfermer dans des milieux à risque ou à adopter des comportements délinquants, surtout s'ils se sentent isolés ou vulnérables.

Étude de cas : Scattered Spider

Même si la cybersécurité s'est améliorée ces dernières années, un groupe de cybercriminels appelé Scattered Spider a réussi à mener certaines des attaques les plus marquantes en 2023 et 2024.
Ce groupe cible surtout de grandes entreprises dans des secteurs comme l'aviation, les télécommunications ou les casinos.
Ils utilisent une méthode appelée ingénierie sociale : ils manipulent des employés pour obtenir leurs identifiants.

Témoignage de Mandiant (Google), octobre 2023

« Scattered Spider est l'un des groupes les plus habiles que nous ayons observés. Il se fait passer pour des employés, trompe les systèmes de sécurité et reste caché pendant plusieurs jours. » https://www.wired.com/story/scattered-spider-most-imminent-threat/

En septembre 2023, MGM Resorts, une chaîne de casinos aux États-Unis, a été attaquée. En quelques heures, les pirates ont bloqué les systèmes d'enregistrement, les cartes des chambres, les machines à sous et les sites web.
Résultat : plus de 100 millions de dollars de pertes et des milliers de clients impactés.
Les hackers ont réussi à accéder aux systèmes simplement en appelant un employé et en se faisant passer pour un technicien.

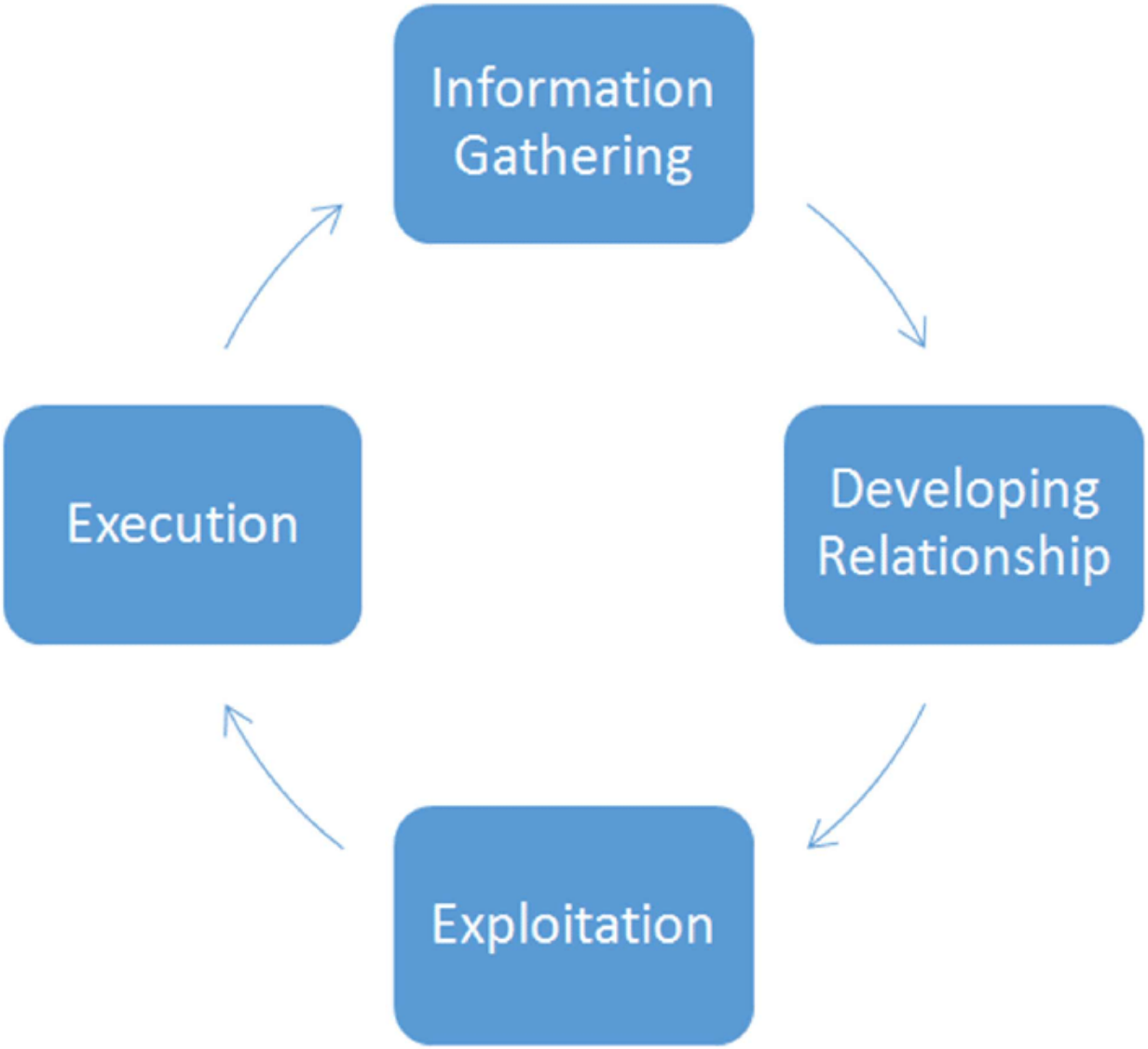
Scattered Spider est composé de jeunes hackers, souvent moins de 20 ans, originaires surtout des États-Unis et du Royaume-Uni.
Ils ne travaillent pas pour un gouvernement mais pour l'argent. Ils utilisent des rançongiciels, c'est-à-dire qu'ils bloquent les systèmes et demandent une somme d'argent pour les débloquer.

Malgré les investissements, l'ingénierie sociale reste très efficace, car elle repose sur la tromperie, pas sur la technique.
Il n'y a pas encore de coopération internationale efficace, ce qui rend ces groupes difficiles à arrêter.

L'Union européenne, les États-Unis et Interpol proposent des formations pour aider les employés à repérer ce type de manipulation.
Des entreprises comme Google et Microsoft demandent la création d'une coalition mondiale, mais elle n'a pas encore vu le jour.

Scattered Spider montre que même les grandes entreprises ne sont pas à l'abri.
La cybercriminalité évolue vite, et les efforts actuels ne suffisent pas encore à protéger les données ou empêcher ce type d'attaque.

Cycle d’une attaque d’ingénierie sociale



https://www.researchgate.net/profile/Hassan-Chizari/publication/307606034/figure/fig1/AS:402846190194688@1473057424163/Social-Engineering-Attack-Cycle.png

- **Collecte d’informations**
  Les attaquants cherchent des données sur leurs victimes (sur LinkedIn, réseaux, etc.).
- **Construction du prétexte**
  Ils se font passer pour une entité légitime : support IT, collègue, prestataire...
- **Exploitation**
  L’attaquant trompe la cible pour obtenir des informations sensibles, accès ou mots de passe.

- **Rétention/Persistance**
  Une fois l'accès obtenu, il installe des logiciels (malwares/backdoors) pour rester longtemps présent.
- **Exfiltration ou attaque**
  Il peut voler des données, installer un ransomware, ou provoquer une interruption des services.

Cette logique en cinq étapes permet de comprendre comment un simple appel ou un e-mail piégé peut déboucher sur un blocage total d'une entreprise

Etude de cas : Cyberattaque contre l'hôpital de Corbeil-Essonnes (France)

En août 2022, l'hôpital Sud Francilien, situé à Corbeil-Essonnes près de Paris, a été victime d'une attaque informatique par rançongiciel (ransomware). Ce type d'attaque consiste à bloquer tous les systèmes informatiques d'un établissement, puis à demander une rançon en échange de la clé pour les débloquer.

- Plusieurs services d'urgence ont dû fermer, obligeant les ambulances à rediriger les patients vers d'autres hôpitaux.
- Les opérations non urgentes ont été annulées.
- Les dossiers médicaux numériques ont été rendus inaccessibles, ce qui a compliqué le suivi des traitements.
- Les pirates ont réclamé 10 millions de dollars, et ont menacé de publier des données médicales sensibles en ligne si l'hôpital ne payait pas.

Finalement, l'hôpital a refusé de payer, comme le recommande l'Agence nationale de la sécurité des systèmes d'information (ANSSI), mais des données ont été diffusées sur le dark web. Cela a soulevé de fortes inquiétudes pour la vie privée des patients.

Comme dans beaucoup d'hôpitaux publics, le système informatique de Corbeil-Essonnes était ancien et mal protégé. Le manque d'investissement dans la cybersécurité a laissé des failles faciles à exploiter pour les cybercriminels.

- Le gouvernement français a annoncé un plan de cybersécurité pour les hôpitaux, avec 20 millions d'euros débloqués pour renforcer leurs défenses numériques.
- Interpol a signalé une hausse de 150 % des attaques sur les hôpitaux dans le monde entre 2020 et 2023.
- Les hôpitaux sont devenus des cibles privilégiées : ils contiennent des données très sensibles et ne peuvent pas se permettre de fonctionner sans leurs systèmes informatiques.

Cette affaire met en lumière la vulnérabilité des services publics face aux attaques informatiques. Alors que l'on pense souvent que seules les grandes entreprises ou les gouvernements sont visés, les hôpitaux, les écoles, et même les mairies peuvent devenir des cibles. L'absence de protection suffisante peut avoir des conséquences graves sur la santé et la sécurité des citoyens.

Pays et organisations concernés

Pays développés (États-Unis, pays de l'Union européenne, etc.) :

- États-Unis : Ciblés fréquemment par des cyberattaques (rançongiciels, espionnage, etc.), les États-Unis ont mis en place des stratégies nationales fortes via le Department of Homeland Security (DHS) et la Cybersecurity and Infrastructure Security Agency (CISA). Le pays mène également des opérations cyber offensives et a imposé des sanctions à des pays comme la Russie et la Corée du Nord pour des attaques informatiques.

- Union européenne : A adopté l'EU Cybersecurity Act et a renforcé la coopération entre États membres grâce à l'Agence de l'Union européenne pour la cybersécurité (ENISA). Europol joue aussi un rôle clé à travers son European Cybercrime Centre (EC3).

Pays du BRICS :

- Russie : Souvent accusée d'être à l'origine de cyberattaques visant d'autres pays (élections, infrastructures critiques). Elle nie toute implication officielle. La Russie développe aussi ses propres capacités de cyberdéfense et de surveillance.
- Chine : Accusée d'espionnage cybernétique à grande échelle, en particulier contre les États-Unis et les entreprises occidentales. La Chine a également mis en place une législation renforcée sur la cybersécurité pour contrôler l'espace numérique.
- Inde : Victime croissante de cybercriminalité, notamment financière. Le gouvernement a lancé une politique nationale de cybersécurité et développe ses capacités de protection numérique.
- Brésil et Afrique du Sud : Moins actifs sur la scène cyber internationale, mais confrontés à une hausse des attaques ciblant les citoyens et les infrastructures.

Pays en conflit ou instables :

- Ukraine : Victime de nombreuses cyberattaques russes, surtout depuis l'annexion de la Crimée en 2014 et plus intensément depuis l'invasion de 2022. Elle a reçu un soutien cybernétique de l'OTAN et de pays occidentaux.
- Iran : Acteur actif dans le cyberespace avec des groupes liés à l'État accusés de campagnes contre Israël, les États-Unis et d'autres pays du Golfe.
- Corée du Nord : Utilise des cyberattaques à des fins économiques et militaires. Le groupe Lazarus est soupçonné d'être responsable de nombreuses attaques internationales.

Organisations internationales :

- ONU : À travers l'UIT (Union internationale des télécommunications), l'ONU tente d'établir des normes globales en matière de cybersécurité. Elle organise aussi des forums intergouvernementaux.
- OTAN : Renforce les capacités de cyberdéfense de ses membres, considère le cyberespace comme un domaine d'opération militaire.
- Interpol : Coordonne des actions contre la cybercriminalité transnationale, notamment via le Global Complex for Innovation basé à Singapour.

Développements récents

2013	Création du European Cybercrime Centre (EC3) par Europol.
2016	Cyberattaque contre les élections américaines, attribuée à la Russie.
2017	Propagation mondiale du rançongiciel WannaCry, lié à la Corée du Nord.
2018	Lancement du Cybersecurity Act par l'Union européenne.
2020	Augmentation massive des cyberattaques pendant la pandémie de COVID-19.
2021	Attaque de Colonial Pipeline aux États-Unis : crise énergétique régionale.
2022	Cyberattaques massives contre l'Ukraine avant et après l'invasion russe.

2023	Signature du Global Cybersecurity Cooperation Agreement entre pays du G7.
2024	Lancement par l'ONU d'un programme mondial de formation en cybersécurité.

Implication des Nations Unies

Convention des Nations Unies contre la criminalité transnationale organisée

La Convention des Nations Unies contre la criminalité transnationale organisée, adoptée en 2000, vise à prévenir et à combattre toutes formes de criminalité organisée à dimension internationale. Bien qu'elle ne traite pas exclusivement de la cybercriminalité, elle constitue une base juridique essentielle pour la coopération entre États face aux crimes transfrontaliers, y compris ceux commis dans le cyberespace. L'article 2(b) permet d'inclure la cybercriminalité parmi les « crimes graves », ce qui facilite la mise en œuvre de mécanismes de coopération judiciaire.

Le Conseil économique et social a, à plusieurs reprises, encouragé les États membres à intégrer les infractions liées aux technologies de l'information comme crimes graves, afin de renforcer les capacités nationales de poursuite et de permettre des actions concertées à l'échelle internationale.

UNODC (Office des Nations Unies contre la drogue et le crime)

L'UNODC coordonne le Programme mondial sur la cybercriminalité, qui vise à renforcer les capacités judiciaires et policières des pays en développement dans la lutte contre les crimes en ligne. En 2019, ce programme a permis la mise en place de formations spécialisées dans plusieurs régions du monde, notamment en Afrique et en Asie du Sud-Est, sur les techniques d'enquête numérique, la collecte de preuves électroniques et la coopération transfrontalière.

Lors du 14e Congrès des Nations Unies pour la prévention du crime en 2021, l'UNODC a souligné l'augmentation alarmante de la cybercriminalité pendant la pandémie de COVID-19 et a appelé à une réponse mondiale coordonnée. Il a également encouragé l'harmonisation des législations nationales en matière de cybercriminalité pour faciliter l'entraide judiciaire entre pays.

Union internationale des télécommunications (UIT)

L’UIT est l’agence spécialisée des Nations Unies responsable des technologies de l’information et de la communication. Elle a lancé le Global Cybersecurity Agenda (GCA), une initiative qui soutient les États membres dans l’élaboration de stratégies nationales de cybersécurité, la protection des infrastructures critiques, et la promotion de la coopération internationale.

L’UIT a aussi mis en place un Indice mondial de cybersécurité (GCI) qui mesure les engagements des pays en matière de cybersécurité dans cinq domaines : juridique, technique, organisationnel, renforcement des capacités, et coopération.

Comité ad hoc pour une convention internationale sur la cybercriminalité

En 2022, l’Assemblée générale des Nations Unies a mis en place un comité ad hoc intergouvernemental chargé de rédiger une convention internationale globale sur la lutte contre l’utilisation des technologies de l’information à des fins criminelles. Ce comité regroupe des représentants de tous les États membres et s’inscrit dans une volonté de créer un cadre juridique universel face à l’évolution rapide des cybermenaces.

Les négociations sont en cours et portent notamment sur la définition des infractions, les mécanismes de coopération, la protection des droits de l’homme en ligne, et la souveraineté numérique. Cette future convention est considérée comme un tournant dans la gouvernance mondiale de la cybersécurité.

Solutions déjà mises en place

- Nombreuses lois nationales ont été instaurées pour encadrer la cybersécurité et punir les actes de cybercriminalité. Par exemple, le *Computer Fraud and Abuse Act* aux États-Unis (1986) ou encore le *Cybercrime Act* en Australie (2001) criminalisent différents types d’infractions numériques.
- La Convention de Budapest (2001), adoptée par le Conseil de l’Europe et ratifiée par plus de 65 pays, est le premier traité international juridiquement contraignant en matière de cybercriminalité. Elle harmonise les législations nationales, facilite la coopération internationale et fournit un cadre d’enquête pour les crimes numériques.
- Des agences spécialisées ont été créées pour faire face aux menaces numériques, telles qu'Europol avec son *European Cybercrime Centre (EC3)* ou encore l'Agence de l’Union européenne pour la cybersécurité (ENISA), qui soutient les États membres dans la prévention des cyberattaques.
- Des partenariats public-privé ont été développés, notamment entre les gouvernements, les entreprises technologiques et les ONG pour partager les

informations sur les menaces, renforcer les infrastructures critiques, et sensibiliser le public, comme le *Global Forum on Cyber Expertise (GFCE)*.

Solutions possibles

Malgré les efforts existants, la coopération internationale reste limitée et les cybermenaces évoluent rapidement. Plusieurs solutions peuvent être envisagées :

- Renforcer la coopération internationale, notamment par la création de traités universels mis à jour régulièrement et ratifiés par un plus grand nombre d'États membres, afin d'harmoniser les définitions juridiques des cybercrimes et les procédures d'enquête.
- Encourager la création de systèmes de réponse rapide aux cyberattaques, via des cellules de crise communes entre États ou des centres de surveillance régionaux capables de détecter et contrer les menaces numériques en temps réel.
- Promouvoir l'éducation numérique dans les systèmes scolaires et les formations professionnelles afin de sensibiliser les citoyens, les fonctionnaires et les entreprises aux bonnes pratiques de cybersécurité.
- Créer un cadre juridique spécifique pour l'intelligence artificielle (IA) dans le domaine cyber, afin d'éviter son usage abusif pour des cyberattaques automatisées et encadrer la responsabilité des acteurs utilisant ces technologies.
- Imposer des standards de sécurité obligatoires aux entreprises privées, notamment celles qui gèrent des infrastructures critiques (énergie, santé, finance), pour assurer une meilleure résilience face aux cybermenaces.

Bibliographie

Council of Europe (2014). *Budapest Convention and Related Standards*. [online] Council of Europe. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

Europol (2019). *European Cybercrime Centre - EC3*. [online] Europol. Available at: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Enisa (2016). *ENISA*. [online] Europa.eu. Available at: https://www.enisa.europa.eu/.

Morgan, S. (2020). *Global cybercrime damages predicted to reach $6 trillion annually by 2021*. [online] Cybercrime Magazine. Available at: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/.

OECD. *The Protection of Critical Infrastructure in the Digital Age*. 2019. https://www.oecd.org/gov/risk/protection-critical-infrastructure-digital-age.htm

Global Forum on Cyber Expertise (GFCE). *About Us*. https://www.thegfce.org/about-us/

United Nations. *Combating Cybercrime*. United Nations Office on Drugs and Crime (UNODC). https://www.unodc.org/unodc/en/cybercrime/index.html

ITU. *Global Cybersecurity Index (GCI)*. International Telecommunication Union. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Kaspersky. *Types of Cybercrime*. https://www.kaspersky.com/resource-center/threats/what-is-cybercrime

Nations Unies. *Cybercrime and international peace and security*. Disarmament and International Security Committee (DISEC), UNGA, 2021. https://www.un.org/disarmament/topics/informationsecurity/ (Accessed: May 20, 2025).

Chertoff, Michael, and Clarke, Richard. *Cybersecurity: The International Legal Framework*. Council on Foreign Relations, 2020. https://www.cfr.org/report/cybersecurity-international-legal-framework (Accessed: May 20, 2025).

Carnegie Endowment for International Peace. *International Strategy to Better Protect the Financial System Against Cyber Threats*. 2021. https://carnegieendowment.org/2021/03/25/international-strategy-to-better-protect-financial-system-against-cyber-threats-pub-84185