**IA & Cybersécurité (CS)**

## 

## Introduction :

(photo : Titre + noms)

Mesdames et messieurs, bonjour ! Aujourd'hui, nous allons plonger dans l'univers fascinant de la cybersécurité et de l'intelligence artificielle.

On va découvrir également le monde des pirates (photo : Jack Sparrow), mais pas ceux-là ! plutôt ceux la (photo : anonymous), donc je vous assure que vous n’avez pas besoin de perroquet ou d’une jambe en bois, juste un peu de curiosité et un sens d’humour.

## Histoire

1. Evolution des ordinateurs et le “rôle dans la société”

(photo : premier ordinateur)

Tout d’abord je vais vous parler un peu de l’histoire.

Au tout début, les ordinateurs étaient d'énormes machines qui occupaient toute une salle. Ils étaient principalement utilisés par des institutions de recherche et des gouvernements pour effectuer des calculs scientifiques complexes. Mais au fil du temps, les ordinateurs ont beaucoup évolué.

(photo : Alan Turing ) (photo : alan turing premier ordinateur)

En 1936, le célèbre Alan Turing invente le premier calculateur programmable , qui était l'ancêtre de nos ordinateurs. Son but était de résoudre "tous" les problèmes de calcul. À partir de ce moment-là, un nouveau modèle apparaît tous les 5 à 10 ans, de plus en plus puissant et performant.

(photo : l'Apple II, le Commodore 64 et le ZX81)

Puis, dans les années 70 et 80, les ordinateurs personnels ont commencé à envahir nos vies. Des machines incroyables comme l'Apple II, le Commodore 64 et le ZX81 sont apparues. Ils étaient les rockstars de l'informatique, avec leurs graphismes pixelisés.

Grâce aux progrès technologiques, les ordinateurs sont devenus de plus en plus puissants, plus petits et moins chers.

(photo : l'Internet et mêmes)

Et comment ne pas mentionner Internet. C'est grâce à Internet que nous pouvons désormais créer et partager les mêmes.

1. Apparition des pirates informatiques et nécessité de mesures de cybersécurité

Cependant, l'émergence d'Internet a également entraîné la prolifération des pirates informatiques et des cyberattaques.

Ces menaces ont rendu nécessaire la mise en place de mesures de cybersécurité robustes pour protéger nos systèmes, nos données et notre vie privée.

Les pirates informatiques exploitent les vulnérabilités des systèmes informatiques pour accéder illégalement à des informations sensibles, causer des dommages ou perturber les opérations.

Comme les vrais pirates, nos pirates informatiques possèdent également des armes, qu’on appel les MALWARES, on peut les classer en plusieurs catégories :

* (photo : Ransomwares) Ransomwares : chiffrent les données de l'appareil infecté, rendant ainsi les données illisibles et inaccessibles aux utilisateurs. Ils prennent en quelque sorte en otage vos données pour ensuite demander une forte rançon afin de les déchiffrer.
* (photo : Spywares) Spywares : ou logiciels espions, ont pour but de collecter des données vous concernant, telles que les mots de passe, les informations sur les paiements, les messages personnels, etc. Les spywares fouillent et recueillent des informations vous concernant.
* (photo : Virus) Les virus : ce sont des programmes conçus pour s'auto-reproduire en infectant d'autres programmes et ainsi se propager d'un appareil à un autre. Une fois introduits, les virus essaient de supprimer, altérer ou endommager les fichiers de l'ordinateur en injectant le code viral.
* (photo : vers informatiques)Les vers : sont également un type de virus qui n'affecte pas les fichiers ou les données. Leur objectif initial est de se répandre en exploitant une vulnérabilité, puis de se répliquer continuellement. Cela surcharge l'espace de stockage de l'ordinateur et sollicite énormément le processeur, ce qui ralentit considérablement l'ordinateur.
* (photo : Cheval de Troie marrant) Le cheval de Troie : c'est un programme malveillant qui se fait passer pour un programme légitime. Lorsque l'utilisateur exécute le programme légitime, le programme malveillant caché est lancé. Le programme caché peut, par exemple, héberger une porte dérobée (backdoor), ce qui permet aux cybercriminels de prendre le contrôle de l'appareil à distance pour voler toutes les informations personnelles et confidentielles (mots de passe, informations bancaires, informations sur la vie privée, etc.). En prenant le contrôle de l'appareil, ils peuvent également installer d'autres malwares dont nous avons parlé précédemment.

Il faut comprendre que les cybercriminels n'utilisent pas ces malwares individuellement, mais ils combinent souvent plusieurs types de malwares pour rendre leurs attaques vraiment redoutables.

Dans la partie sur la cybersécurité, vous allez découvrir comment vous protéger de la plupart des malwares. (photo : messages urgents d’arnaque) Les malwares demandent souvent à l'utilisateur d'ouvrir un document sous forme de fichier .exe, .zip, Word, Excel, PDF, par e-mail, SMS, ou via une clé USB. Les messages sont souvent de type "URGENT", "facture en retard", "cette application est incroyable !" ou "votre colis est arrivé".

Les fameux hacks...

À votre avis, quand a eu lieu le premier "hack" officiel ? Eh bien, c'était entre 1834 et 1836, lorsque deux hommes d'affaires bordelais ont détourné l'usage du réseau de télégraphe optique pour obtenir des informations bancaires en primeur. Ce piratage du télégraphe peut être considéré comme l'un des premiers cas de piratage.

(Quelques exemples de hacks dans l’histoire)

Mais les véritables piratages informatiques tels que nous les connaissons aujourd'hui ont commencé dans les années 1980.

En 1988, le ver Morris a marqué l'un des premiers grands incidents de piratage à grande échelle. Écrit par Robert Tappan Morris, ce ver a décidé de partir en tournée mondiale sur les ordinateurs connectés à Internet, des milliers d'ordinateurs ont été infectés, provoquant d'importantes perturbations. Cet incident a conduit à la création de la première loi sur la cybercriminalité aux États-Unis.

Pendant la période des fêtes de fin d'année en 2013, la chaîne de magasins américaine Target a été victime d'une attaque qui a compromis les données de paiement de plus de 40 millions de clients. Les pirates ont exploité une faille de sécurité dans le système de point de vente de l'entreprise.

WannaCry : En mai 2017, le ransomware WannaCry a infecté des centaines de milliers d'ordinateurs dans le monde entier en exploitant une vulnérabilité dans le système d'exploitation Windows. Il a paralysé de nombreux services et institutions, notamment des hôpitaux, des entreprises et des organisations gouvernementales.

Face à ces menaces croissantes, il est devenu essentiel de mettre en place des mesures de cybersécurité, je laisse Marwan, notre spécialiste en cybersécurité pour vous parler de son domaine favori.

(photo : Histoire CS)x2

(photo : Fonction de CS)

(photo : CS) x2

**2. La cybersécurité : (image cybersécurité)**

Définition de la cybersécurité :

Pour faire le plus condensé possible, la cybersécurité, **c’est l'ensemble des lois, politiques, outils, dispositifs, concepts et mécanismes de sécurité, méthodes de gestion des risques, actions, formations, bonnes pratiques et technologies** qui peuvent être utilisés pour protéger les personnes et les actifs informatiques matériels et immatériels.

C’est dans la deuxième moitié du 20e siècle qu’est née la cybersécurité. En plus des précédents exemples mentionnés à propos des virus informatiques, le fameux ver Morris doit son origine à des expérimentations effectuées dès 1971, par **Robert Thomas,** du MIT (Massachusset Institut of Technology). Ce dernier a découvert (en partie accidentellement), qu’il était possible pour un programme informatique de se déplacer sur un réseau, en créant le **virus informatique Creeper**. (Photo ver informatique)

Cette observation a suscité un intérêt important puisqu’elle démontrait qu’une attaque était possible via le réseau Internet dont c’était les débuts.

De cet incident naîtra la première loi sur la cybercriminalité mais surtout la cybersécurité.

**Si la cybersécurité a d’abord concerné essentiellement les individus et les entreprises, utilisateurs d’Internet, elle a très vite englobé un aspect protection d’un banditisme organisé, voire de menaces géopolitiques.**

Aujourd’hui, le piratage informatique s’est en effet institutionnalisé avec des États qui l’utilisent pour des attaques des communications adverses, des sécurités ou des économies de pays rivaux ou ennemis.

C’est d’ailleurs pour cela que vous entendez de plus en plus souvent parler d’aspects militaires et informatiques, comme un tout.

Et désormais des organismes internationaux civils et militaires, comme l’UE, l’ONU, Forum de Davos ou l’OTAN, se saisissent du problème. (Logos de différents organismes internationaux)

Depuis les **années 2010, l’UIT** (l’Union Internationale des Télécommunications a créé l’indice GCI (**indice de corruption globale**) qui évalue l'engagement des pays en faveur de la cybersécurité au regard de cinq axes stratégiques (juridique, technique, organisation, prise de conscience et savoir-faire, coopération internationale). (Logos UIT)

C’est cette multiplication de menaces mais aussi la complexification de celles-ci qui a ouvert la porte à l’IA dans la cybersécurité, parce qu’elle offre une réactivité et la possibilité d’une charge de travail qui ne sont plus réalisables par l’humain seul.

Selon **Pierre Barnabé (Responsable de la division Big Data & Cybersecurity du groupe Atos – ESN française parmi le top 10 mondial), les trois piliers de la cybersécurité seraient** **« Anticipation, innovation, collaboration ». (photo Pierre Barnabé)**

## Et l’IA dans tout ça ? (photo IA)

* **L'intelligence artificielle (IA)** est conçue pour donner aux ordinateurs la pleine capacité de réponse de l'esprit humain. Cette science englobe de nombreuses autres technologies, à l'instar du Machine Learning et du Deep Learning.
* **Le Machine Learning (ML)** utilise les schémas comportementaux existants pour prendre des décisions à partir des données et des conclusions antérieures. L'intervention humaine est toujours requise pour implémenter des modifications. Le Machine Learning est probablement la discipline de cybersécurité basée sur l'IA la plus pertinente à ce jour.
* **Le Deep Learning (DL)** fonctionne de la même manière que le ML. Il prend des décisions à partir de schémas antérieurs, mais effectue des ajustements de manière autonome. Dans le domaine de la cybersécurité, le Deep Learning relève du Machine Learning, sur lequel nous nous concentrerons davantage ici.

**L’un des premiers rôles de l’IA dans la Cybersécurité sera un travail de tri** : les SOC (Security Operation Centers)(Photo de SOC) doivent traiter des milliers d’incidents. Une charge de travail trop importante pour qu’un seul humain soit efficace.

L’IA peut intervenir ici pour effectuer un premier travail de tri, qui sera vérifié ensuite par les experts pour les cas avérés ou pour les « faux positifs ».

Les SOC peuvent ainsi bénéficier d’une automatisation dans le tri des alertes grâce au Robotic Process Automation (RPA) qui analyse des données en les comparant à des listes noires et autres bases de données de logiciels malveillants.

Pour que l’IA puisse passer à l’étape supérieure et faire un tri plus précis, les RPA sont alors dotés du Machine Learning et apprennent de leurs erreurs pour réduire encore plus le risque de « faux positifs ».

### **L'erreur humaine dans la configuration**

L'erreur humaine représente une grande partie des faiblesses de la cybersécurité. Par exemple, une configuration système appropriée peut être incroyablement difficile à gérer, même avec d'importantes équipes informatiques impliquées. Dans la course à l'innovation constante, la sécurité informatique est devenue plus hiérarchisée que jamais. Des outils adaptés peuvent aider les équipes à identifier et à atténuer les problèmes survenant lorsque les systèmes réseau sont remplacés, modifiés et mis à jour.

Pensez à la façon dont les dernières infrastructures Internet comme le cloud computing peuvent prendre le dessus par rapport aux anciennes structures locales. Le département informatique doit garantir la compatibilité des systèmes d'entreprise pour les protéger. Les processus manuels d'évaluation de la sécurité des configurations épuisent les équipes, qui jonglent avec les mises à jour interminables et les tâches de support quotidiennes ordinaires. Grâce à une automatisation intelligente et adaptative, les équipes peuvent bénéficier de conseils opportuns sur les derniers problèmes détectés. Elles peuvent prendre conseil sur les options de traitement, voire disposer de systèmes pour régler automatiquement les paramètres si nécessaire.

Mais l’IA peut aussi avoir un “côté obscur” car c’est aussi un outil des hackers pour rendre plus performantes leurs attaques. (photo IA cyberattaque)  
  
Quelques exemples:  
  
 - ChatGPT: elle sera essentiellement utilisée pour des petites actions permettant, par exemple, d’obtenir des traductions et des rédactions plus crédibles de mails de hameçonnage, confirmer une ligne de code entrant dans un programme plus complexe.  
Mais il est clair que ce n’est pas ChatGPT qui moulinera tout le travail de A à Z.  
Il s’agît dans ce cas d’un outil complémentaire pour des hackers “en herbe”.

* Sinon, tous les systèmes d’IA et de ML et DL évoqués plus haut dans le cadre de la cybersécurité sont utilisables par des individus plus aguerris pour tester des combinaisons d’attaques, des mots de passe, des failles ou erreurs.

Là encore, l’utilité de l’IA se vérifie pour travailler avec un grand nombre de combinaisons, dans un temps réduit avant une éventuelle détection.

## 3 Facteur humain :

(photo : Social Engineering)

Je vais ensuite vous parler du facteur humain et plus précisément de l'ingénierie sociale.

Il est souvent présumé que la plupart des cyberattaques se déroulent en ligne, mais il convient de souligner que les plus grandes attaques informatiques ont été rendues possibles grâce à l'ingénierie sociale, un terme utilisé pour décrire cette pratique.

Maintenant que nous avons évoqué l'importance du facteur humain dans les cyberattaques, laissez-moi vous parler plus en détail de l'ingénierie sociale, également appelée "Social Engineering".

(photo : chaine de vulnérabilité)

Dans le piratage, il existe un concept appelé la chaîne de vulnérabilité, composée de 6 maillons : la conception, la fabrication, l'installation, la configuration, l'exploitation et bien sûr le facteur humain.

Le pirate dispose d'un outil spécifique pour s'attaquer à ce dernier maillon, c'est l'ingénierie sociale.

L'ingénierie sociale est un ensemble de méthodes et de techniques permettant à une personne d'obtenir l'accès à un système ou à des données confidentielles en influençant ou en manipulant les individus.

Première étape : la collecte de données

(photo : collecte de données / data mining)

1. Cette étape consiste à analyser en profondeur la cible et son contexte. La première recherche concerne l'analyse des sources ouvertes, notamment le site officiel de la cible, ses clients, ses partenaires et ses fournisseurs. Ensuite, les réseaux sociaux tels que Facebook, Twitter, Instagram, YouTube, LinkedIn, les forums, les listes de discussions, les groupes Discord, WhatsApp, etc., sont explorés.

(photo : outils data mining)

1. Ensuite, le pirate informatique utilisera des outils moins connus, tels que des moteurs spécialisés dans le datamining (collecte de données), pour récupérer des noms d'utilisateurs spécifiques, des adresses e-mail compromises, et il peut même accéder au dark web. Il existe des centaines de sources pour effectuer ce type de recherches.

(photo : Réseaux sociaux data mining, fake accout)

1. Une autre méthode consiste à obtenir des informations personnelles qui sont visibles uniquement par les amis et les proches de la cible. Par exemple, en créant un faux compte LinkedIn ou Facebook et en entrant en contact avec la cible.

(photo : Spy conferences)

1. Le pirate peut également tenter de découvrir dans quelle salle de conférence auront lieu des réunions confidentielles, dans le but d'espionner ces réunions.

(photo : Trashing)

1. Il existe également des approches plus physiques, comme le "Trashing", qui consiste à fouiller les poubelles de l'entreprise ou de la personne ciblée pour récupérer des informations.
2. Le pirate peut également essayer d'obtenir un rendez-vous commercial, car les gens sont souvent enclins à fournir des informations lorsqu'ils pensent qu'une transaction commerciale est en jeu. De même, lors d'un entretien d'embauche, le pirate peut tenter de collecter des informations sensibles.

(photo : hacker call)

Il est vrai qu'il existe de nombreux autres moyens de collecter des informations.

Le concept même de l'ingénierie sociale repose sur un paradigme relativement simple : "Il est dans la nature humaine de croire nos semblables, en particulier lorsqu'ils formulent des demandes qui nous paraissent raisonnables".

(photo : paradigme ingenerie sociale)

Comme je l'ai mentionné précédemment, le pirate informatique cherchera les maillons les plus faibles de la chaîne de vulnérabilité.

L'objectif de l'attaquant est d'établir la confiance. La démarche doit paraître ordinaire pour ne pas éveiller les soupçons, et il doit parfaitement maîtriser le langage et le jargon propres à la cible, qui peuvent varier en fonction du domaine d'activité (informatique, finance, recherche, etc.).

Il peut utiliser des phrases telles que "Laissez-moi vous aider", car nous avons souvent tendance à accepter l'aide de quelqu'un qui se propose.

Il peut prétendre être votre supérieur, car la hiérarchie au sein des grandes organisations est rarement remise en question. Par exemple, en disant : "Bonjour, ici la direction générale. Je vous appelle simplement pour vous informer que vous serez prochainement contacté dans le cadre d'une affaire sensible par le lieutenant de police Christophe Riviere. Je vous demande de lui apporter votre entière collaboration. Merci."

En résumé, c'est un domaine très vaste, et il est important de comprendre que le pirate informatique analyse tous ces comportements "prévisibles" afin de les exploiter.

Exemples

Je vais maintenant vous montrer deux extraits qui illustrent un peu tout ce que je viens de mentionner :

[BEST MOVIE SCENE EVER For "Social engineering" - Who Am I](https://youtu.be/xiSYI7zdF5I?t=84)

[Mr Robot - Social Engineering](https://www.youtube.com/watch?v=s9jwOVGWWuk)

Je vais conclure ce paragraphe en abordant un principe qui est au cœur du film "Who Am I" : "No system is safe" ou "aucun système n'est sûr".

Cela signifie qu'aucune protection n'est infaillible face aux cyberattaques. Même les systèmes les plus robustes peuvent être compromis. Cette réalité met en évidence l'importance de rester constamment vigilant et de prendre des mesures de sécurité appropriées pour protéger nos informations, nos systèmes et notre vie privée.

## 

## 

## Conclusion :

1. Récapitulation des points clés abordés dans la présentation

**Loin du clin d'œil cinématographique du début, nous avons pu voir que hacking et cybersécurité sont des mondes complexes, opposés mais aussi basés sur des mêmes logiques, de l’univers informatique  
Un besoin constant d’innover et d’être réactif permet de marquer des points face à l’adversaire, quel qu’il soit.**

1. Souligner l'importance croissante de l'IA dans la cybersécurité

**Si les débuts de ces deux univers ont été modestes, à la taille des possibilités informatiques de l’époque, l’accroissement des puissances, des réseaux et des données font rentrer un nouvel acteur dans cette lutte: l’IA.  
Au départ du bon côté de la “barrière” en apportant à la cybersécurité la possibilité de gérer des situations toujours plus complexes et volumineuses, les hackeurs y ont également trouvé une alliée potentielle.  
Le coup d’avance sera donc toujours à celui qui saura le mieux anticiper, innover et réagir avec un tel outil.**

(photo : conclusion)

—---------------------------------------------------------------------------------------------------------------------

Entrepôt des idées:

* Pour comprendre ce que l’IA devrait faire, on doit d’abord comprendre ce que l’humain fait.
* Job : cybersecurity analys (détecte et élimine les menaces de CS dans les entreprises / développe les stratégies préventives / monitor networking for potential vulnerabilities / conduct regular security audits / éduquer les employés d’avoir les meilleures pratiques / investigate security breaches a,d incidents / veille informatique pour savoir les dernières technologies et trends)
* Qualités de cybersecurity analys : strong analytical and critical thinking abilities pour pouvoir prendre des bonnes décisions rapidement et prendre des meilleurs actions / faire attention aux details / excellent communication skills / savoir apprendre rapidement (s’adapter rapidement aux nouvelles technologies) / strong ethical foundation
* Job : ethical hacker or white hat hacker : son travail est d’identifier les failles dans les computer system et les sites (l’IA a encore du mal à les remplacer car l’IA a encore besoin d’une personne derrière pour la guider et être effective / compréhension de business et le contexte technique / communiquer les recommandations.
* Cependant dans un futur proche, on risque d’avoir des IA de 2 côtés : IA qui est entraîné pour attaquer et IA entraîné pour défendre, l’humain n’aura pas le temps de réagir dans une telle bataille. Reste compliqué à évaluer car l’IA peut évoluer très rapidement.

Améliorer la présentation



**Humour** :

* Commencer la présentation par une blague sur cybersécurité / hackeurs (vanne, anecdote, meme…)
* support visuel drôle
* un jeu (de vote avec les réponses et résultats drôles (ex : réponse “pas de bol, vous vous êtes fait hack))

**Originalité** :

* Faire notre présentation sous forme d’une histoire fictive avec des personnages (on peut les appeler Marwan et Kirill pour fun)
* Easteregg : code secret à assembler au cours de la présentation et au dernier slide demander d’entrer le code secret.