- **Groupe 1 : Zélie, Jeanne, Chloé, Manon**

Mesdames, Messieurs.

Les menaces d'internet sont de plus en plus fréquentes, l'armée subit environ deux cyber attaques par jour en France, sur des bases de données, des expertises techniques et même un hôpital militaire.

Ces attaques peuvent être orchestrée depuis n'importe où et par n'importe qui. Très faciles à réaliser, il est très difficile d'identifier formellement le véritable attaquant, qui agit souvent sous couvert de relais involontaires ou d'intermédiaires.

Pour résoudre ce problème, l'État français s'est dotée d'une stratégie nationale pour la sécurité du numérique. Elle met en avant cinq lignes d'action :

Garantir la souveraineté nationale

Apporter une réponse forte contre les actes de cyber malveillance

Informer le grand public

Faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises

Et renforcer la voix de la France à l'international

La cyberdéfense rassemble la cybersûreté, la cybersécurité, la cyberagression (lutte informative offensive) et la cyberrésilience (lutte informative défensive).

Le cadre de la cyberdéfense dépasse la simple sécurité informatique dans la mesure où elle a des conséquences directes sur la sécurité nationale et vient donc intéresser les différents organismes de défense d'un pays. Avec la lutte informatique défensive (LID) et la lutte informatique offensive d'attaquer des ensembles de réseaux et d'ordinateurs qui contrôlent un pays.

Avec des degrés d'importances plus ou moins grands, ces réseaux et leurs systèmes de contrôle baptisés SCADAS peuvent permettre de contrôler les systèmes suivants : surveillance de processus industriels ;

- transport de produits chimiques ;
- système municipaux d'approvisionnement en eau ;
- commande de la production d'énergie électrique ;
- distribution électrique ;
- canalisation de gaz et de pétrole ;
- recherche et études scientifiques et industrielles

En 2016 une première directive a été adoptée en matière de cybersécurité, elle est entrée en vigueur le 9 mai 2017 afin d'intensifier en coopération entre les Etats-Membres de L'UE.

Elle prevoit l'obligation pour chaque pays membres de désigner une ou plusieurs autorités nationales et de se doter d'une stratégie.

Lors du printemps 2017, deux attaques massives ont eu lieu :

En mai il y a eu WannaCry qui a touché des usines et des hopitaux au Royaume-Unis et (Not) Petya en juin qui est parti d'Ukraine avant de toucher le reste du monde et a provoqué plus d'un milliard d'euros de dégâts.

En France, il y a eu une attaques contre le ministère des Armées francaise, afin d'éviter une nouvelle attaque, j'ai donc mis en place la L.I.O (lutte informatique offensive) qui permait a la France de recruter 1000 personnes qui integrerons le comcyber afin de réduire les cyber attaques, qui ont lieu environ deux fois par jour.

- **Groupe 2 : Sacha, Lubin, Océane, Adèle**

Bonjour aujourd'hui dans un monde qui entre dans une nouvel air , l'air du numérique , il faut savoir se protéger.ainsi le role que joue la cyberdéfense n'a jamais été aussi important .Mais la cyberdéfense ,c'est avant tout un moyen de protéger la cybersécurité contre les cyberattaques via différentes installations.Les cyberattaques , les attaques numériques ont quintuplé en 5 ans en 2016 c'est 80 % des infrastructures numériques européennes qui ont été visée , et on parle d'un déficit de plus de 400 milliards d'euros c'est pourquoi nous devons développé différents systèmes de sécurité pour préserver la cyber sécurité

Le comcyber c'est un commandement de cyberattaquants qui travaille pour le ministère de l'armée qui sont chargés de s'occuper de la cyberdéfense.La cyberdéfense française comporte 3000 militaires informaticiens spécialisés en sécurité systèmes et réseaux.Le principe était la lutte informatique défensive(LID).Analyser et détecter toutes tentatives d'intrusion dans les systémes d'information ou de matériels connéctés. En juillet 2017 le FBI et europôl ont réussi a démentelé Alphabay at Hansa qui sont deux grandes puissances du darkweb.

- **Groupe 3 : Paul, Maxime, Maxime, Clément**

Mesdames Messieurs bonjour.

Je sais qu'il y a de plus en plus de pirate informatique pouvant s’en prendre à des sites web mais heureusement pour lutter contre cela il y a des moyens de défense. Le problème c'est qu'ils sont plus ou moins sophistiqué et par conséquent plus ou moins facile à pénétrer.

Mais même avec des gros moyens de cyberdéfense les hackers les plus doués arrivent quand même a s'infiltrer et à passer les pares feux comme chez Altran et Airbus qui se sont fait piratés en 2019. Certains sont même engagé par des pays pour espionner d'autres états ce sont des mercenaires. Comme la dit le président de la commission européenne monsieur Jean-Claude Juncker : "les cyberattaques sont parfois plus dangereuses pour la stabilité des démocraties et des économies que les fusils et les chars".

Les cyberattaque sont les nouvelles menaces qui pèsent sur le monde.

- **Groupe 4 : Pierre, Ilian, Téo, Erwan**

Mesdames et monsieur le chef d'état et de gouvernement d'état

Je vais vous parler de la cyberdéfense.

La cyberdéfense est un ensemble de moyen physique et virtuels mis en place par un pays dans de le but de lutter contre la Cyberattaque. La cyberattaque consiste à protéger des donnés informatique

Il existe plusieurs types de cyberattaque comme le piratage informatique par des hackers ou encore l'espionnage d'un pays par un autre.

Il existe aussi : l'utilisation criminelle d'internet (cybercriminalité), y compris à des fins terroristes, la propagation de fausses informations ou manipulations à grande échelle, l'espionnage à visée politique ou économique, les attaques contre les infrastructures critiques (transport, énergie, communication…) à des fins de sabotage.

Récemment l'entreprise Aebi Schmidt a était visée par une attaque informatique ayant paralysée ses systèmes internes. L'entreprise était spécialisée dans le matériaux hivernal et aéroportuaire.

On estime que le Monde a perdu 400 milliards d'euros a cause des cyberattaques.

Pour éviter cela la France et l'Union Européenne utilise l'arme informatique (virus, pare-feu, ...

Le vecteur numérique reste enfin "au coeur de la stratégie de communication djihadiste", à "des fins de propagande, d'influence ou de déstabilisation".

Premier succès majeur d'une action commune du FBI et d'Europol : deux des plus gros marchés criminels du darkweb, Alphabay et Hansa, ont été démantelés en juillet 2017, preuve de l'efficacité des actions coordonnées.

- **Groupe 5 : Marceau, Raphaël, Kelvyn, Cyril**

Mesdames, messieurs,

Depuis plusieurs années, un nouveau danger s'est installer dans le monde : la Cybercriminalité.

Le cybercriminel, le plus connu a comme nom "hacker", il utilise des lignes de code afin d'arrivé a contrôler site webs, application, ou directement l'appareil concerné. Il peut aussi détourner des données ou des informations, comme le virus Wannacry, appartenant à la NSA a été volé par shadow Brokers en mai 2017.

Il existe également des espions au services de leur pays, ils ont pour missions de recueillir des informations sur d'autres Etats afin d'éviter des guerres informatiques.

Heureusement, Les pays ont développer ce qu'il appelle de la "cyberdéfense" pour éviter ses attaques. Cette cybersécurité repose sur 5 lignes d'actions :

- Garantir la souveraineté national,

- Apporter une réponse forte contre les actes de cyber malveillances,

- Informer le grand public contre les dangers,

- Faire de la sécurité un avantage concurrentiel pour les entreprises françaises,

- Renforcer la voix de la France à l'international.

Des moyens très importants sont mis a disposition pour l'armée (plus de 1 milliards d'euros). Cette armées, le Comcyber, constitué de plus de 3000 combattants numériques luttent tous les jours pour nous protéger. L'espace informatique du ministère est surveillé 24h/24 et 7j/7.

Dans le cadre de LIO, l'armée française à décidée de tirer parti des vulnérabilités adverse durant les phases de crises, cette nouvelle doctrine a 3 objectifs:

- évaluation des capacités adverses : recueille ou extraction d'informations,

- réduction voire neutralisation des capacités adverses, perturbations temporaires ou création de dommages majeure dans les capacités militaires adverses,

- modification des perceptions ou de la capacité d'analyse de l'adversaire : altération discrète de données ou systèmes, exploitation d'informations dérobées au sein du système d'information militaire de l'adversaire.

Mais cette doctrine est risquée, car la France risque des conflits avec d'autres nations pour espionnage.

Pour éviter cela, l'Union Européenne met en place une autonomie stratégique basée sur trois axes principaux :

- L'Axe technologique : soutient de recherches et des développements de pointes afin de favoriser le déploiement de technologies et de services numériques

- L'Axe réglementaire : il y a des réglementations qui sont mises en place pour protéger les citoyens et entreprises et les Etats membres de la cybercriminalité. Ces réglementations sont conformes a nos valeurs communes.

- Et l'Axe capacitaire : tentative de mettre en place un outils de partage d'informations techniques sur les menaces, afin d'anticiper et répondre rapidement à une cyber attaque.

De plus nous pouvons aussi citer l'ANSSI (Agence nationale de la sécurité des systèmes d'information), véritable pompier du cyberespace, chargé de prévention, vous protège aussi.

Merci de votre attention