

LA CYBER SOCIÉTÉ:

PLAN:

- **FACILITÉS**
- Communication
- Réseaux sociaux
- Moins d'utilisation du papier
- **DANGERS:**
- cyber-terrorisme
- cyber-violence
- cyber-criminalité
- comportements (sécurité + travail)
- **CYBERNAUTES:**
- 3ème revolution
- importance de l'enseignement
- LiFi

2.1 A COMMENT LA TECHNOLOGIE FACILITE LA VIE QUOTIDIENNE?

Grâce à l'Internet la vie des gens a changé complètement dans tous les secteurs. Par exemple, l'internet a facilité notre vie énormément parce que la communication est devenue vraiment rapide et immédiate. Ça a nous permis de pouvoir communiquer très facilement avec tout le monde à n'importe quel moment ou emplacement. Il faut qu'on souligne que sans l'internet nous n'aurions pas des réseaux sociaux que presque tout le monde utilise fréquemment chaque jour. Ces réseaux ont absolument changé notre style de vie car à partir de son apparition nous sommes habitués à les utiliser. Ils ont plein d'avantages comme qu'on peut retrouver des vieux amis et faire des nouveaux amis, cela nous fournit avec des nouvelles dans tout le monde et il nous tient informés, et c'est une manière d'avoir de la sécurité si quelque chose passe. Toutefois, il y a des inconvénients aussi, comme par exemple que avec cela on reste devant des écrans beaucoup plus temps et ça endommage nos yeux et nous fait perdre du temps. De plus, un autre inconvénient est que les réseaux sociaux créent beaucoup d'addiction, donc il faut qu'on en fasse une utilisation modérée. Surtout n'oublions pas que grâce à l'internet on a des livres online, donc il y a moins de livres physiques et on utilise moins de papier. Si on utilise moins de papier on sauvera beaucoup d'arbres.

INCLUDE STATS + MORE INFO FROM TEXT

2.2 A QUELS DANGERS LA CYBER-SOCIÉTÉ POSE-T-ELLE?

Cyber Violence:

- Un collégien sur cinq a été la cible d'insultes ou d'humiliations par SMS ou sur Internet.
- Parmi les élèves de collège, 14% ont reçu au moins un SMS ou une notification sur les réseaux sociaux contenant un surnom méchant ou une brimade, soit une hausse de 5% par rapport à une enquête de 2011.
- La proportion monte à 19% en prenant en compte happy slapping et la publication de photos méchantes.
- Le phénomène touche plus de filles que des garçons.
- Les élèves concernés de 6ème ont été 15% contre 20% en 3ème.
- Ces micro agressions sortent dehors des murs du collège.

- Les victimes déclarent souvent avoir subi d'autres incidents, tels que vols d'objets personnels, des bousculades, des mises à l'écart. Un collégien sur vingt a déclaré au moins trois faits de cyber-violence, ce qui s'apparente à du harcèlement.
- Ceux qui en parlent s'adressent à leurs amis (33%), ou à leurs parents (29%) plutôt qu'aux enseignants (16%).
- Néanmoins, le phénomène n'empêche pas 93% des élèves de se sentir bien dans leur collège.
- 8% de cas de cyber-violence sont rapportés à la police.

Comportement: Sécurité

Bons	Mauvais
Créer des mots de passe complexes	Utiliser des mots de passe simple
Changer régulièrement les mots de passe	Prendre contact avec des personnes inconnues
Installer des outils de protection	Cliquer sur les liens contenus dans les courriels inattendus.
Télécharger un logiciel de sécurité.	
Scanner les fichiers joints aux messages avant les ouvrir	

- Il faut qu'on
- Il faudrait que les gens
- C'est fondamental qu'on
- C'est essentiel qu'on
- C'est primordial qu'on
- C'est impératif qu'on
- Il vaut mieux que
- Les profs d'informatique insistent pour qu'on

Travail (déconnexion)

En période de vacances, selon le journaliste Julien Duponchel, les Français n'arrivent "*pas vraiment*" à couper le cordon avec leur employeur. 69% des actifs interrogés sur leur lieu de vacances disent consulter leurs mails professionnels tous les jours et rester joignables à tout moment. Un actif sur deux déclare rester connecté pour s'assurer qu'il n'y a aucun problème en son absence.

Depuis le 1er janvier 2017, un nouvel article a été ajouté au Code du travail : le droit à la déconnexion. Concrètement, les entreprises de plus de 50 salariés doivent mettre en place une charte pour définir les horaires précis d'utilisation des outils numériques et elles doivent surtout obliger leurs salariés à se déconnecter en arrêtant par exemple de les solliciter en dehors de leur temps de travail.

2.2 B QUELS DANGERS LA CYBER-SOCIÉTÉ POSE-T-ELLE?

Cyberterrorisme, la guerre de l'information:

En 1993, l'internet n'était pas un sujet important pour le public. Mais il y avait une futurologue, Alvin Toffler, qui avait déjà prédit qu'il y aurait des attaques cybernautes. Depuis lors, la notion de cyber-terrorisme ne cesse de diviser les experts. Les uns, alertent régulièrement sur le risque d'un < Pearl Harbour électronique >, les autres leur rappellent qu'aucun acte de cyber-terrorisme n'a encore été recensé.

Virgine Vacca, de la Campagne européenne d'intelligence stratégique, rappelle que le "Digital Pearl Harbour" a démontré que pour simuler une cyber-attaque d'envergure, les pirates devraient consacrer quelque 200 millions de dollars et disposer de cinq ans pour mener à bien l'offensive, donc c'est vraiment improbable que un Pear Harbour électronique arrivera.

Si les terroristes se servent d'Internet, c'est pour y véhiculer leur propagande, au travers de sites Web, de forums et de vidéos qui visent avant tout à recruter de nouveaux adeptes, et à asseoir leur notoriété. Ce qu'on veut dire est que si les terroristes veulent attaquer, ils ne le feront pas par Internet.

Le Cyber-terrorisme: l'utilisation d'Internet pour commettre des actes violents qui entraînent ou menacent de causer des pertes de vie ou des lésions corporelles importantes, afin de réaliser des gains politiques par l'intimidation.

Le Cyber-guerre: implique l'utilisation de l'espace de combat et le ciblage des ordinateurs et des réseaux dans la guerre.

- Les attaques proviennent normalement de petites groupes normalement adolescents, mais aucun dégât n'a été causé par les cyberattaques jusqu'à présent
- Ils n'ont pas causé de dommages physiques ou économiques significatifs et encore moins de dommages humains.
- Il y a 14 ans, il y a eu "l'explosion" du web. Cependant, depuis lors, les terroristes préfèrent toujours tuer de vraies personnes en utilisant des bombes et en les effrayant en utilisant les médias plutôt que de créer des dommages hypothétiques via Internet.
- Les experts pensent que pour le moment la cyber-guerre est plus un problème que le cyber-terrorisme
- En 2007, l'Estonie a été l'un des premiers pays à faire l'objet d'une cyber-attaque: les gens soupçonnent que la Russie était à l'origine de cette attaque; depuis lors, l'OTAN (NATO) a créé deux centres de cyber-défense, l'un à Bruxelles et l'autre à Tallinn, la capitale de l'Estonie
- En 1991, la première guerre du Golfe avait montré à quel point la maîtrise de l'information, et de ses technologies, contribue à asseoir la suprématie d'une armée.

2.3 A QUI SONT LES CYBERNAUTES?

Grâce à internet, l'éducation et l'enseignement s'a modifié énormément. Comme l'internet nous donnent toute l'information on besoin rapidement on n'a pas la nécessité d'aller à la bibliothèque pour avoir de l'information. Il faut qu'on souligne que l'internet est une énorme part de notre vie et nous regardons de l'information que il nous donne tout le temps, donc on peut dire que il influence grandement nos opinions et réactions sur certains sujets. D'un autre côté comme l'internet encourage l'utilisation des appareils technologiques il encourage aussi l'abandon de l'écriture. Et cela est vraiment mauvais parce que l'internet est en train de créer une société qui n'est pas attirée par les livres et par l'écriture.

INCLUDE STATS + MORE INFO FROM TEXT

2.3 B QUI SONT LES CYBERNAUTES?

Hier

Minitel: Avant l'Internet

- Lancé en 1982, Minitel était une innovation française qui permettait d'accéder à des services en ligne.
- Les plus populaires étaient: l'annuaire téléphonique, vente en ligne, les sites de rencontre
- Minitel a été fermé le 30 juin 2012 car ses services faisaient maintenant tous partie d'internet
- 2011: les internautes déclaraient avoir en moyenne 13.6 comptes différentes. Ils se répartissaient en 4.6 comptes pour les achats en ligne, 3.0 pour les comptes de messagerie, 2.1 pour l'e-administration, 1.7 pour les profils de réseaux sociaux, 0.9 par les comptes bancaires, 0.7 pour les messageries instantanées et 0.7 pour les forums.
- Aujourd'hui débrancher est le nouveau luxe alors que dans le passé c'était la capacité à être "brancher" qui donnait du prestige
- Aujourd'hui poser son téléphone bien en évidence n'est plus un attribut de richesse, mais au contraire, des personnes instaurent et souhaitent une journée sans portable, sans ordinateur ou sans internet.

Aujourd'hui

La France est en train de rater la troisième révolution industrielle.

Il faut que nous nous rendions compte que l'internet est un espace matériel. Par exemple, Google possède des millions de serveurs dans le monde entier, regroupés dans des "data centres". Pour assurer son approvisionnement énergétique, Google rachète des centrales hydro-électriques. Google et Facebook possèdent leurs propres câbles transatlantiques et leur noeuds de communication. Mais la France n'a pas ça. Leurs activités commerciales dépendent avant tout de leurs infrastructures matérielles.

Aujourd'hui, le contrôle des points d'échange d'internet est aussi importante que l'était, au 19ème et au 20ème siècles, le contrôle du canal de Suez. L'économie mondiale, la culture mondiale, la politique mondiale sont organisées autour d'internet. Plus aucun pays ne peut se couper d'internet, il subirait une catastrophe économique.

Dans le monde du cyberspace, la France était bien placée mais a perdu son pouvoir et elle n'a pas une réelle présence dans cette industrie. Malgré cela, la France a les compétences nécessaires et si la France ne réagit pas elle ne pourra faire concurrence aux géants américains d'internet. Si la France ne devient pas plus importante dans le monde d'Internet, il y a une menace et une crainte que la même chose qui est arrivée à la Chine au 20ème et elle risque de perdre son importance dans le monde.

Demain

Le LiFi: (le futur de la cyber-société)

Une nouvelle technologie pourrait remplacer le WiFi. Il s'agit du LiFi (light fidelity), un système de communication sans fil basée sur l'utilisation de la lumière LED. Ce projet a été présenté au 6ème Forum économique de Zermatt.

Alors que le WiFi utilise les ondes radio électromagnétiques, le LiFi utilise la lumière LED, pour transmettre des données internet. Son principal avantage est la vitesse de transmission des données qui pourrait résoudre les problèmes de saturation des réseaux.

Comme il existe 17 milliards de "points d'illumination" dans le monde, adopter le LiFi permettrait de tripler l'accessibilité à internet, par exemple dans l'Afrique.

Il a déjà été testé en France essentiellement et dans différents lieux, comme des hôpitaux, le métro et des magasins notamment. La marque Lidl par exemple, a décidé d'implanter cette technologie dans tous ses magasins. Et il y a des autres pays qui s'intéresse aussi.

La prochaine réunion va être à Paris en Février 2018.

1. La vitesse est rapide.
2. La sécurité est formidable, parce que c'est seulement vous et votre lumière que se connecte donc aucune personne ne peut se mettre dans votre LiFi et l'utiliser.
3. Les données ne passent pas par des serveurs comme google, ou par des satellites, il passe par la lumière publique. Donc c'est le propriétaire de la lumière publique qui contrôle l'information, ça veut dire le citoyen.