

CRÉE POUR

Les Cyberattaques

Alicia Sargueux

Lucie Peyrat

Dossier de Veille BUT InfoNum

1ère Année

PARTIE 1

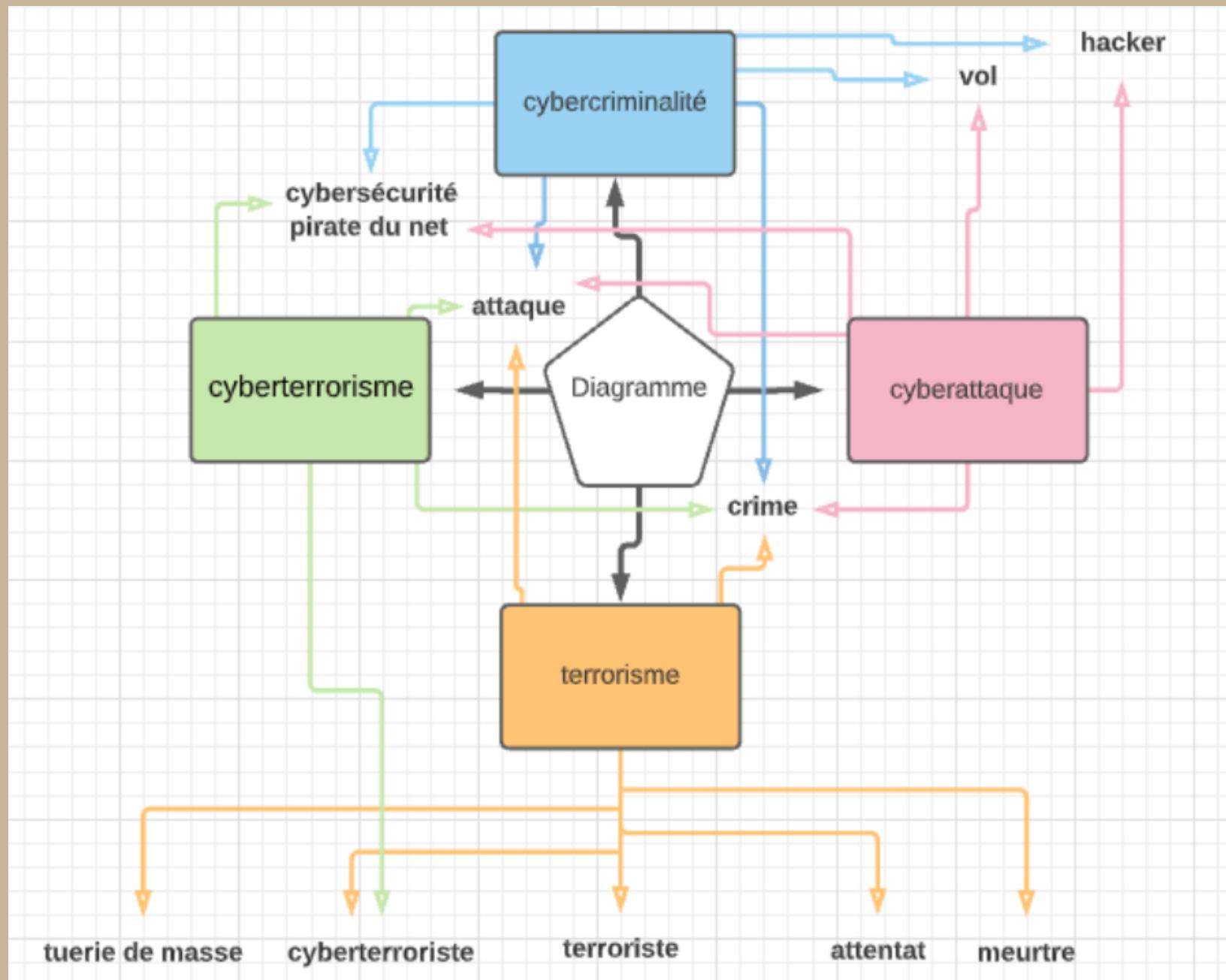
Le choix du sujet

Dans le cadre du cours de veille de Madame d'Hennezel, nous devions choisir car c'est un sujet d'actualité et effectuer un travail de veille informationnelle. D'après internet, la veille informationnelle est un processus de surveillance, paramétrable et automatisé, qui permet à ses utilisateurs d'être informés des publications les plus récentes quant à leurs domaines de recherche ou à leurs centres d'intérêt. Nous avons choisi le sujet "La place du cyberterrorisme dans le terrorisme" Nous avons choisi ce sujet car c'est il est d'actualité même si on entend beaucoup plus parler du terrorisme que du cyberterrorisme. Nous avons donc trouvé intéressant de se renseigner sur le cyberterrorisme et voir quelle place il a. Et nous voulions pour cela nous baser sur la problématique "Quelle est la place du cyberterrorisme dans le terrorisme ?". Mais avec un travail plus approfondi nous avons préféré choisir la problématique "**La place des cyberattaques dans notre vie quotidienne**". Car notre démarche de veille a apporté des liens beaucoup plus intéressants sur les cyberattaques et non le terrorisme ou le cyberterrorisme.

Démarche de veille

Pour pouvoir effectuer un travail de veille sur ce sujet, il faut d'abord lister des mots clés. L'objectif est de cibler des aspects concrets du sujet afin de trouver ce qui ressort le plus pour synthétiser. Après l'avoir fait, nous avons créé des alertes sur les mots "cybercriminalité", "cyberterrorisme", "cyberattaques" et "terrorisme" avec l'outil de veille "Google Alerts".

Suite à cette recherche, et grâce à un autre outil de veille qui est lucidchart, nous avons créé un diagramme se basant sur nos quatre mots "cybercriminalité, cyberattaque, cyberterrorisme et terrorisme".



Pour réaliser ce diagramme nous avons tout d'abord réfléchi aux mots clés. Ensuite nous avons organisé quatre grandes parties : le terrorisme, le cyberterrorisme, les cyberattaques et la cybercriminalité. A partir de celles-ci, nous avons associé différents mots clés. Certains se retrouvent évidemment dans plusieurs parties.

On y a lié le reste des mots afin de voir où il se reliaient et ceux qui ressortaient le plus afin de créer des nouvelles alertes. Ce schéma nous a été très utile pour la mise en place de Google Alerts. En effet, on a pu créer nos alertes en fonction des parties puis en fonction des mots auxquels elles étaient associées afin d'avoir des alertes associant deux mots. Par exemple, on a mis cyberattaque ET crime, cybercriminalité ET hackers et ainsi de suite.

Tableau mots clés

Mot-clef	Date de la mise en place de l'alerte	Moteur de recherche utilisé
cybercriminalité	18/11/2021	Google Alerte
cyberattaque	18/11/2021	Google Alerte
cyberterrorisme	18/11/2021	Google Alerte
terrorisme	18/11/2021	Google Alerte
terrorisme ET tuerie de masse	18/11/2021	Google Alerte
terrorisme ET terroriste	18/11/2021	Google Alerte
terrorisme ET meurtre	18/11/2021	Google Alerte
terrorisme ET cyberterroriste	18/11/2021	Google Alerte
terrorisme ET attentat	18/11/2021	Google Alerte
cyberterrorisme ET pirate du net	18/11/2021	Google Alerte
cyberterrorisme ET <u>cyberterroriste</u>	18/11/2021	Google Alerte
cyberterrorisme ET cybersécurité	18/11/2021	Google Alerte
cyberterrorisme ET crime	18/11/2021	Google Alerte
cyberterrorisme ET attaque	18/11/2021	Google Alerte

Nous avons remarqué que certains mots clé donnaient des résultats négatifs. Les alertes associées étaient inexistantes ou alors non pertinentes pour notre sujet, comme par exemple le mot terrorisme (d'où le changement de problématique). Nous avons donc classé ces mots dans un tableau, par ordre chronologique, et précisé le moteur de recherche que nous avons utilisé. Nous avons ensuite mis au point un code couleur, les mots clé surlignés en vert sont les mots qui nous ont donné un résultat positif et ceux en rouge sont ceux qui n'ont donné aucun résultat ou qui n'étaient pas pertinents pour nous, que nous n'avons donc pas utilisé.

cybercriminalité ET cybersécurité	18/11/2021	Google Alerte
cybercriminalité ET crime	18/11/2021	Google Alerte
cybercriminalité ET attaque	18/11/2021	Google Alerte
cyberattaque ET vol	18/11/2021	Google Alerte
cyberattaque ET pirate du net	18/11/2021	Google Alerte
cyberattaque ET hacker	18/11/2021	Google Alerte
cyberattaque ET cybersécurité	18/11/2021	Google Alerte
cyberattaque ET crime	18/11/2021	Google Alerte
cyberattaque ET attaque	18/11/2021	Google Alerte
cyberguerre	01/03/2022	Google Alerte et Google recherche avancée

 : résultats positifs

 : résultats négatifs

Nous avons ensuite trié tous les liens donnés par les alertes et avons sélectionné les plus pertinents, nous y avons ajouté une synthèse afin de dresser notre plan répondant à la problématique.

Tableau gestion de source

Titre de l'article	Liens et date	Mots clés utilisés	Moteur de recherche	Fiabilité de la source	Format/Information
Cyberattaque, fuite de données, panne mondiale... Les gros ratés des géants de la technologie en 2021	https://www.ouest-france.fr/leditiondusoir/2021-12-29/cyberattaque-fuite-de-donnees-panne-mondiale-les-gros-rates-des-geants-de-la-technologie-en-2021-b6634516-179f-4b7f-b6e3-7ef710472362 29/12/2021	cyberattaque	Qwant	fiable	article sur l'édition du soir
Une déferlante de cyberattaques en France	https://www.lefigaro.fr/actualite-france/une-deferlante-de-cyberattaques-en-france-20211124 24/11/2021	cyberattaque	Qwant	fiable	article sur le figaro
Attentat contre « Charlie Hebdo » : des éléments confidentiels ont fuité	https://www.lepoint.fr/justice/attentat-contre-charlie-hebdo-des-elements-confidentiels-ont-fuite-24-11-2021-2453659_2386.php 24/11/2021	cyberattaque et hacker	Qwant	fiable	article sur lepoint.fr
Attentat de Charlie Hebdo : des hackers tentent d'extorquer de l'argent à des avocats de victimes	https://www.leparisien.fr/high-tech/attentat-de-charlie-hebdo-des-hackers-tentent-dextorquer-des-avocats-de-victimes-24-11-2021-7NGHVRDISBAKDHUECKSEFQ5ELY.php 24/11/2021	cyberattaque et hacker	Qwant	fiable	article sur le Parisien
Engager des pirates en ligne, c'est désormais un jeu d'enfant	https://www.fredzone.org/engager-des-pirates-en-ligne-cest-desormais-un-jeu-denfant 24/11/2021	cyberattaque et hacker	Qwant	fiable	article sur FZN
Cybercriminalité : 4 chiffres sur l'explosion des rançongiciels en France	https://www.algerie360.com/hausse-de-cybercriminalite-la-justice-monte-au-creneau/ https://www.lesechos.fr/tech-medias/hightech/cybercriminalite-4-chiffres-sur-lexplosion-des-rancongiciels-en-france-1366709 24/11/2021	cybercriminalité	Qwant	fiable	article sur les echos

Titre de l'article	Liens et date	Mots clés utilisés	Moteur de recherche	Fiabilité de la source	Format/Information
Log4Shell, la faille informatique qui fait trembler la planète	https://www.francetvinfo.fr/replay-radio/nouveau-monde/log4shell-la-faille-informatique-qui-fait-trembler-la-planete_4877969.html 26/12/21	cyberattaque et hacker	Qwant	fiable	article sur Franceinfo
Lutte contre la cybercriminalité : Facebook a recruté des Mauriciens pour s'attaquer aux «commentaires» abusifs en kreol, selon le ministre Balgobin	https://defimedia.info/lutte-contre-la-cybercriminalite-facebook-recrute-des-mauriciens-pour-sattaquer-aux-commentaires-abusifs-en-kreol-selon-le 24/11/21	cybercriminalité	Qwant	peu fiable	article sur defimedia.info
Conseil action – Bureau Veritas: une cyberattaque qui contrarie une belle dynamique	https://bourse.lefigaro.fr/actu-conseils/conseil-action-bureau-veritas-une-cyberattaque-qui-contrarie-une-belle-dynamique-20211124 24/11/21	cyberattaque	Qwant	fiable	article sur le figaro
Une déferlante de cyberattaques en France	https://www.lefigaro.fr/actualite-france/une-deferlante-de-cyberattaques-en-france-202111124 24/11/21	cyberattaque	Qwant	fiable	article sur le figaro

Voici notre premier tableau de gestion de sources qui répertorie les premiers articles que nous avons trouvés intéressants, en général de source fiable et que nous avons donc utilisées. Ces liens datent du 24 novembre 2021 au 29 décembre 2021.

Titre de l'article	Liens et date	Mots clés utilisés	Moteur de recherche	Fiabilité de la source	Format/Information
Cyberattaques, la pandémie du Net	https://www.areion24.news/2022/01/01/cyberattaques-la-pandemie-du-net/ 1/01/2022	cyberattaque	Google	peu fiable	article sur areion24.news
Seine-Saint-Denis : une cyberattaque perturbe plusieurs mairies	https://www.lesechos.fr/pme-regions/ile-de-france/seine-saint-denis-une-cyberattaque-perturbe-plusieurs-mairies-1375797 31/12/2021	cyberattaque	Google	fiable	article sur Les Echos
Piratage d'un cabinet d'avocats lié au procès Charlie Hebdo : "Un marketing de la malveillance", analyse un spécialiste de la cybersécurité	https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/piratage_d-un-cabinet-d-avocats-lie-au-proces-charlie-hebdo-un-marketing-de-la-malveillance-analyse-un-specialiste-de-la-cybersecurite_4857155.html 24/11/2021	cybersécurité	Google	fiable	article sur franceinfo
Dans les coulisses de l'info : comment nous avons été informés de la cyberattaque à l'hôpital de Dax	https://www.sudouest.fr/sante/dans-les-coulisses-de-l-info-comment-nous-avons-ete-informes-de-la-cyberattaque-a-l-hopital-de-dax-7383641.php 26/12/2021	cyberattaque	Google	fiable	article sur SudOuest
En matière de cybersécurité, 2022 pourrait bien ressembler à 2021	https://www.heidi.news/innovation-solutions/en-matiere-de-cybersecurite-2022-pourrait-bien-ressembler-a-2021 28/12/2021	cybersécurité	Qwant	peu fiable	article sur heidi.news
Cyberattaque, fuite de données, panne mondiale... Les gros ratés des géants de la technologie en 2021	https://www.ouest-france.fr/leditiondusoir/2021-12-29/cyberattaque-fuite-de-donnees-panne-mondiale-les-gros-rates-des-geants-de-la-technologie-en-2021-b6634516-179f-4b7f-b6e3-7ef710472362 29/12/2021	cyberattaque	Qwant	peu fiable	article sur l'édition du soir
Un des principaux médias paralysé par une attaque au rançongiciel	https://www.lematin.ch/story/un-des-principaux-medias-paralyse-par-une-attaque-au-rancongiciel-765005892256 29/12/2021	cybercriminalité et attaque	Qwant	peu fiable	article sur le matin.ch
Norvège : De nombreux journaux paralysés après une attaque par rançongiciel	https://www.20minutes.fr/monde/3207603-20211230-norvege-nombreux-journaux-paralyses-apres-attaque-rancongiciel 30/12/2021	cybercriminalité et attaque	Qwant	peu fiable	article sur 20minutes.fr
Une cyberattaque empêche la parution de 80 journaux régionaux en Norvège	https://fr.euronews.com/2021/12/31/une-cyberattaque-empeche-la-parution-de-80-journaux-regionaux-en-norvege 31/12/2021	cyberattaque	Qwant	fiable	article sur euronews
"J'étais opposé au pass sanitaire" : les explications du hacker qui a piraté l'AP-HP	https://www.lepoint.fr/faits-divers/j-etais-oppose-au-pass-sanitaire-les-explications-du-hacker-qui-a-pirate-l-ap-ph-01-01-2022-2458833_2627.php 01/01/2022	cybersécurité et hacker	Qwant	fiable	article sur le point

Voici notre deuxième tableau de gestion de sources qui répertorie nos liens datant du 26 décembre 2021 au 1er janvier 2022. (excepté celui du 24 novembre 2021).



Titre de l'article	Liens et date	Mots clés utilisés	Moteur de recherche	Fiabilité de la source	Format/Information
Cyberattaque en Ukraine : un moyen pour augmenter la tension durant les négociations	https://www.rfi.fr/fr/europe/20220115-cyberattaque-en-ukraine-un-moyen-pour-augmenter-la-tension-durant-les-n%C3%A9gociations 15/01/2022		Qwant	fiable	article sur rfi
Cyberattaque en Ukraine : le ministère des Affaires étrangères ukrainien affirme avoir des "indices" de l'implication russe	https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaque-en-ukraine-le-ministere-des-affaires-etrangeres-ukrainien-affirme-avoir-des-indices-de-l-implication-russe_4917219.html 14/01/2022	cyberattaque	Qwant	fiable	article sur franceinfo
Qu'est-ce qu'une cyberattaque ?	https://information.tv5monde.com/info/qu-est-ce-qu-une-cyberattaque-440427 19/01/2022	Cybersécurité	Qwant	fiable	article dans TVMonde
Cybersécurité : comment faire face aux menaces permanentes de la cybercriminalité	https://www.sanofi.fr/fr/Actualites/nos-actualites/cybersecurite-sanofi-se-mobilise-pour-lutter-contre-la-cybercriminalite 01/2022	cyberattaque et cybercriminalité	Qwant	peu fiable	article sur Sanofi
Craintes pour la cybersécurité des athlètes aux JO de Pékin	https://www.lequipe.fr/Tous-sports/Actualites/Craintes-pour-la-cybersecurite-des-athletes-aux-jo-de-pekin/1311846 20/01/2022	cybersécurité	Qwant	fiable	article sur L'Equipe
Thales refuse le chantage, des hackers publient les données volées à sa branche aérospatiale	https://www.leparisien.fr/high-tech/un-groupe-de-hackers-publie-des-donnees-volees-a-la-branche-aerospatiale-de-thales-18-01-2022-Z4YNRKZ3GJGDBL5EF4JBL64TOY.php 18/01/2022	cybercriminalité et hackers	Qwant	fiable	article sur LeParisien

Titre de l'article	Liens et date	Mots clés utilisés	Moteur de recherche	Fiabilité de la source	Format/Information
La cybersécurité n'est plus l'affaire des entreprises mais des MSSP	https://www.lemondeinformatique.fr/actualites/lire-la-cybersecurite-n-est-plus-l-affaire-des-entreprises-mais-des-mssp-85753.html 11/02/2022	cyberattaque et cybersécurité	Google	peu fiable	chronique
Guerre en Ukraine. Les hackers d'Anonymous revendiquent une cyberattaque contre des médias russes	https://www.ouest-france.fr/monde/guerre-en-ukraine/guerre-en-ukraine-les-hackers-d-anonymes-revendentiquent-une-cyberattaque-contre-des-medias-russes-9caa731e-9896-11ec-a212-1f68235c1350 28/02/2022	cyberattaque et hackers	Google	fiable	article sur Ouest-France
Guerre en Ukraine : "Le risque de cyberattaque est élevé" en France alerte le ministère de l'Intérieur	https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-le-risque-de-cyberattaque-est-eleve-en-france-alerte-le-ministere-de-l-interieur_4982682.html 26/02/2022	cyberattaque	Google	fiable	article sur Franceinfo
Invasion de l'Ukraine : les coulisses des cyberattaques	https://www.francetvinfo.fr/replay-radio/nouveau-monde/invasion-de-lukraine-les-coulisses-des-cyber-attaques_4962966.html 27/02/2022	cyberguerre	Google	fiable	article sur Franceinfo
Cybersécurité : Attention aux escrocs qui se cachent dans vos visioconférences	https://www.zdnet.fr/actualites/cybersecurite-attention-aux-escrocs-qui-se-cachent-dans-vos-visioconferences-39937763.htm 22/02/2022	cyberattaque et cybersécurité	Qwant	fiable	article sur ZNet



Tableau de gestion de source qui répertorie les liens du mois de janvier et février.

PARTIE 2

Sommaire

Introduction.....	13
I. L'Histoire de la cybercriminalité.....	14
A) La cybercriminalité, qu'est-ce que c'est ?.....	14
B) Le premier cas de cybercriminalité.....	17
II. Comment faire pour lutter contre la cybercriminalité ?.....	20
A) Les solutions dans les entreprises: le cas de Sanofi.....	20
B) Les solutions dans la politique.....	24
III. Notre point de vue.....	28
A) Notre point de vue sur le sujet.....	28
B) Notre point de vue face aux solutions.....	29
Conclusion.....	30
Zotero.....	31

Introduction

Nous allons définir trois thèmes principaux de la cybercriminalité,, c'est-à-dire de l'ensemble des moyens utilisés pour assurer la sécurité des systèmes et des données informatiques d'un particuliers ou d'une entreprises. Tout d'abord le cyberterrorisme, d'après la définition de Kevin G. Coleman, est "l'utilisation préméditée des activités perturbatrices, ou la menace de celle-ci, contre des ordinateurs et / ou réseaux, dans l'intention de causer un préjudice de nature sociale, idéologique, religieuse, politique, ou autres objectifs. Ou pour intimider toute personne dans la poursuite de tels objectifs". Ce terme a été inventé par Barry C. Collin. Dans les années 1980, l'intérêt du public pour le cyberterrorisme a fortement augmenté à cause du bug du millénaire. Les attaques potentielles de cyberterrorisme durant cette période se sont accentuées. D'après Jean-Yves Poichotte, Directeur de la Cybersécurité "l'objectif des cyberattaques peut être de soutirer de l'argent, de voler des données ou des informations stratégiques, commerciales ou confidentielles ou de détruire des capacités opérationnelles. Ces attaques font des dégâts colossaux aujourd'hui au sein des entreprises." Quant à une cyberattaque, il s'agit d'un acte malveillant contre un dispositif informatique via un réseau cybernétique. Les cyberattaques peuvent provenir d'individus isolés, comme Kevin Mitnick, qui était l'un des plus connus, d'un groupe de hackers ou encore plus récemment de grands groupes ayant des cibles géopolitiques. L'objectif principal des cybercriminels est de gagner de l'argent en volant les données des utilisateurs, en trompant les personnes vulnérables sur Internet et même en menant des attaques de type phishing (technique utilisée par les fraudeurs pour obtenir des informations personnelles pour le vol d'identité).). Et enfin le terrorisme est l'utilisation de la violence à des fins idéologiques, politiques ou religieuses. Cependant, un grand nombre d'organisations politiques ou criminelles recourent au terrorisme pour faire avancer leurs causes ou en tirer profit.

1. L'histoire de la cybercriminalité

A) La cybercriminalité, qu'est-ce que c'est ?

La cybercriminalité est un ensemble d'activités illégales menées sur Internet et un cybercrime est un comportement criminel qui peut être commis sur ou via un système informatique normalement connecté à un réseau. Les attaques peuvent cibler des individus ainsi que des entreprises et des dirigeants. Leur but est d'obtenir des informations personnelles à des fins d'utilisation ou de revente (données bancaires, identifiants de sites marchands, etc.).

La cybercriminalité peut être dissociée selon 3 types d'infractions. Le premier type est celui spécifiques aux technologies de l'information et de la communication avec notamment, les infractions aux cartes bancaires et les atteintes aux systèmes de traitement automatisé de données. Le second type est celui lié aux technologies de l'information et de la communication qui se concrétise par la haine raciale sur internet et l'incitation au terrorisme, les atteintes aux personnes et leurs biens ou encore par la pédopornographie. Et enfin, le dernier type est celui facilité par ses technologies comme les escroqueries et les violations de propriété intellectuelle en ligne.

Le phishing et les ransomwares sont des exemples connus de comportements malveillants qui nuisent aux internautes. L'hameçonnage, « phishing » ou filoutage, est une technique malveillante en ligne très courante qui a pour objectif d'effectuer une usurpation d'identité afin d'obtenir des informations personnelles et des identifiants bancaires à des fins criminelles. Quant aux rançongiciels, il s'agit de programmes informatiques malveillants de plus en plus courants conçus pour chiffrer des données puis demander à leurs propriétaires d'envoyer de l'argent en échange de clés permettant de les déchiffrer.

le phising →



← le ransomwares

En 2020, le CSIS, Centre d'Études Stratégiques et Internationales qui est un groupe de réflexion américain ainsi que McAfee, un éditeur de logiciel connu pour son logiciel anti-virus McAfee VirusScan, ont réalisé un rapport sur la cybercriminalité et ses coûts. Un total de 1500 dirigeants et décideurs informatiques ont été interrogés au Japon, aux Etats-Unis, au Canada, en France, aux Royaume-Uni ainsi qu'en Australie et en Allemagne. Ce rapport indique que, en 2020, deux tiers des entreprises interrogées ont été victimes d'une cyberattaque. Les pertes mondiales dues à ses attaques représentent plus d'1% du PIB mondial en 2020 (84,71 billions USD), la cybercriminalité a donc augmenté de 50% par rapport à l'année 2018. Les attaques entraînent un temps d'arrêt dans la productivité des entreprises et nécessite une intervention externe afin de réparer les pannes, tout cela peut atteindre des coûts importants pour celles-ci. En effet, 56% des répondants affirment n'avoir aucune stratégie lorsqu'ils sont victimes d'attaques et sur 951 organisations possédant un plan d'intervention, on remarque que seulement 32% admettent avoir un plan efficace. Les entreprises sont donc trop peu préparées aux éventuelles attaques informatiques.

B) Le premier cas de cybercriminalité

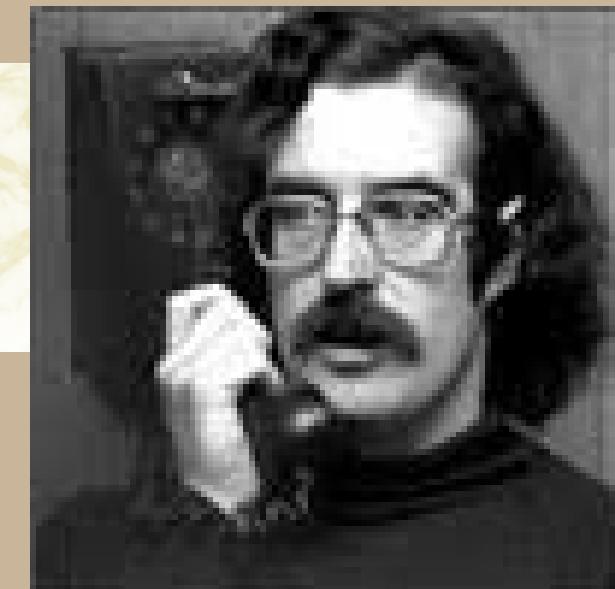
Les premiers cas de cybercriminalité sont apparus avant l'apparition d'Internet et étaient liés au vol de données. La cybercriminalité est née dans les années 1960 par le piratage de lignes téléphoniques, l'objectif était de détourner l'environnement à des fins lucratives. Ce n'est qu'à partir des années 1980 qu'elle s'est développée dans le monde informatique lorsque les réseaux informatiques et Internet ont été créés pour stocker et transférer des informations et des données d'entreprise ou personnelles. L'apparition du numérique a certes été très utile pour l'évolution de l'humanité mais cependant, elle a participé à l'apparition de pirates sur le net, qui veulent déchiffrer des informations difficiles à récupérer, qui sont sous formes de données . En France, la cybercriminalité est légalement prise en compte depuis la loi du 6 janvier 1978 relative à l'informatique, aux documents et aux libertés.

Le premier cas de cybercriminalité a été le détournement de John Draper, également connu sous le nom de Captain Crunch, en 1969. Il a trouvé et utilisé avec succès un sifflet d'enfant, qui a été offert en cadeau dans une boîte de céréales Cap'n Crunch, avec une tonalité semblable à celle de la compagnie téléphonique américaine, Bell (2600 Hz). Les lignes longue distance inoccupées émettaient une tonalité de 2600 Hz ce qui signifiait qu'elles étaient prêtes à recevoir un appel. John Draper composait alors un premier numéro vert, c'est-à-dire un numéro sans frais, puis, avant que le central téléphonique distant ne décroche, il utilisait son sifflet pour laisser croire à une interruption de l'appel. La ligne étant toujours disponible, il pouvait ensuite téléphoner gratuitement en composant un nouveau numéro.

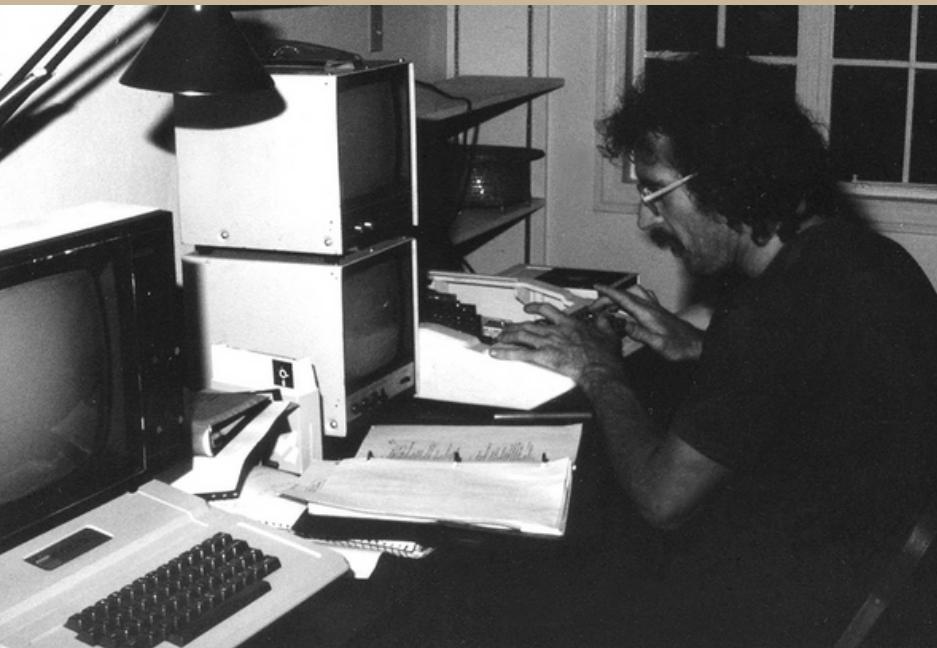


← le sifflet et la boîte
de céréale

John Draper →



Il a alors construit par la suite la “blue box”, la boîte bleue, un boîtier électronique capable de reproduire les tonalités des différents opérateurs, lui permettant ainsi de passer des appels interurbains gratuits. Il a ensuite diffusé des instructions sur la façon de le concevoir et de ce fait les cas de fraude électronique ont augmenté de façon spectaculaire. John Draper a été condamné à deux mois de prison en 1976 et a ensuite créé en 1980, le premier traitement de texte de la plate-forme Apple nommé EasyWriter. Après ça, il est devenu expert en sécurité.



← John Draper programmant EasyWriter

///. Comment faire pour lutter contre la cybercriminalité

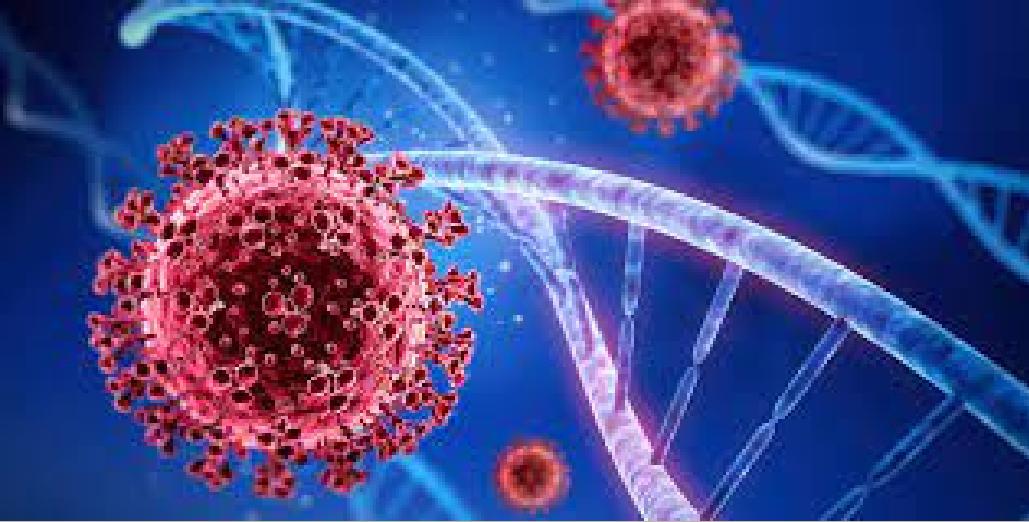
Depuis les premiers cas de cyberattaques, le problèmes s'est énormément développer via le web. Malheureusement, les cas se sont accentués ces dernières années et ce sont les entreprises qui en ont payé les frais ainsi que les citoyens. Mais quelles sont les solutions pour résoudre le problème ?

A) Les solutions dans les entreprises: le cas de Sanofi

Sanofi est une entreprise qui trouve ses racines en France. Elle travaille activement dans le secteur médical de manière à ce qu'une filière santé dynamique se crée en France. Leur but principal est d'inclure tout le monde au travail et de permettre une facilité à l'accès des soins médicaux, le tout en gardant un respect pour l'écologie. C'est une entreprise qui touche à la science dans le domaine thérapeutique, qui propose de nombreux produits à la vente issus de leurs laboratoires, pourtant ils ont subi une cyberattaque à la fin de l'année 2020.

Sanofi est équipé du service “Cyber SOC” ou “Cyber Security Operations Center” qui consiste à assurer une cybersécurité à l’entreprise. Ils ont dédié tout un article sur le site où ils indiquent leurs solutions pour combattre la cybercriminalité. Il s’agit d’une équipe de 80 collaborateurs qui travaillent pour lutter contre le problème, encore plus depuis l’attaque qu’ils ont subie. Ils ont mis en place 10000 protections par jour. Dans cette vidéo issu du site de Sanofi, Jean-Yves Poichotte le directeur de la cybersécurité de l’entreprise nous explique tout en détail.





Depuis la pandémie, de nombreuses cyberattaques sont perpétrées sur les entreprises, actuellement, elles se sont même multipliées. Le travail en distanciel aurait favorisé le développement de ces cybermenaces. Les laboratoires pharmaceutiques, les hôpitaux et bien d'autres institutions touchant au numérique sont les principales cibles pour diverses raisons: l'argent, la concurrence etc... Sanofi a connu, en 2020, plus de 13 millions de cyberattaques qui ont été recensées dont 7000 ont réussi à être contrées par leurs équipes d'ingénieurs.



Ainsi les entreprises sont les cibles du cyberterrorisme et des cyberattaques bien plus souvent que l'on pense. Nous avons choisi le cas de Sanofi car lors de notre démarche de veille, s'en est ressorti l'article de leur site à propos de ce problème. Mais il y a eu d'autres entreprises touchées comme Thalès ou l'hôpital de Dax. Néanmoins Sanofi a décidé de riposter en installant tout un système de cybersécurité avec à sa tête une équipe d'ingénieurs formés. Dans cette vidéo, une ingénierie de l'entreprise témoigne de son travail.

Ig-VcNeCgTU

[Click here to visit the page.](#)

Le cyberterrorisme et les cyberattaques sont un fléau grandissant, notamment en France. Comme on a pu le voir dans l'exemple de Sanofi, les entreprises développent des solutions de cybersécurité pour se protéger. Mais qui peut protéger les citoyens ? La politique commence elle aussi à chercher des solutions.

B) Les solutions dans la politique

La pandémie a poussé beaucoup de monde à travailler de chez soi. Les cyberattaques se sont donc multipliées. On constate que de plus en plus le cyberterrorisme est au centre de l'actualité. Depuis les attentats de Charlie Hebdo, des cyberattaques contre les proches des victimes ou auprès des avocats se multiplient. Des tentatives pour extorquer l'argent des victimes sont faites et de nombreuses informations auraient fuitées. Il est désormais de plus en plus facile d'engager "des pirates en ligne", les réseaux sociaux comme facebook recrute des spécialistes pour combattre les commentaires abusifs, les administrations françaises telles que Véritas se font aussi attaquer, on leur demande des rançons. De plus, les évènements récents entre l'Ukraine et la Russie viennent accentuer le problème puisque cette guerre a débuté par plusieurs cyberattaques.

C'est aussi sur des institutions publiques que le cyberterrorisme s'abat, empêchant la liberté d'expression et violant le secret médical. Enfin cela se passe sur les réseaux sociaux, la cybersécurité est désormais au centre des débats publics, il est de plus en plus urgent de combattre ces attaques et de protéger les citoyens. Désormais nous parlons de lutte contre la cybercriminalité. Les citoyens ne sont pas nécessairement formés à cela et ne savent pas comment riposter. Les politiciens doivent donc prendre en compte ce nouveau problème et l'intégrer à leur programme de la présidentielle de 2022.

V2VJNV0Eyw4

[Click here](#) to visit the page.

Emmanuel Macron par exemple, notre actuel chef d'État, se représente aux élections présidentielles de 2022 avec un nouveau projet de loi qui touche notamment à la cybersécurité. Dans son programme sur le site en marche (<https://en-marche.fr/emmanuel-macron/le-programme/defense>), la catégorie défense présente 3 objectifs. Le premier est de "donner aux armées les moyens d'assurer la souveraineté stratégique de la France", il y a 5 propositions en sous catégorie dont celles ci-dessous.

→ **Nous renforcerons la priorité en matière de cyberdéfense et de cybersécurité. Nous l'avons vu lors des élections américaines, Internet est un nouveau terrain d'opération des conflits et des tensions. Il en va de notre souveraineté.**

- Missions de renseignement et d'investigation : mieux identifier nos failles, détecter des actions hostiles.
- Missions de protection et de défense : bâtir des murailles, patrouiller dans le cyberespace.
- Missions de riposte et de neutralisation : entraver les actions des attaquants cyber, neutraliser des infrastructures utilisées pour causer des dommages à la France.

Il insiste bien sur cette question de sécurité, car elle devient une priorité avec les chiffres en hausse des cyberattaques ces dernières années. Mais la question est d'autant plus primordiale avec les temps qui courrent, dans de nombreuses de ses interviews dans les journaux il évoque ce problème et il en fait même un objet de communication sur ses réseaux sociaux. Cette vidéo est extraite du journal de 20h qu'il a posté sur son compte twitter: <https://twitter.com/EmmanuelMacron/status/841026182669836289>

Bien sûr les candidats comme Anne Hidalgo, Jean-Luc Mélenchon ou encore Jean Lassalle veulent augmenter les moyens en cybersécurité. Certains voudraient revoir la loi de programmation militaire afin de, tout comme Emmanuel Macron, prendre en compte les nouvelles menaces présentes sur le web. D'autres souhaitent, eux, renforcer l'ANSI ou l'Agence Nationale de Sécurité Informatique pour lutter contre l'espionnage numérique. Quoi qu'il en soit les entreprises pourront peut-être désormais compter sur un aide de l'État grâce aux candidats qui intègrent le concept de cybersécurité dans leurs projets de lois. Il en va de même pour les citoyens qui pourront être à égalité devant le numérique.

///. Notre point de vue

A) Notre Point de vue sur le sujet

La cybersécurité est un sujet qui est toujours d'actualité de nos jours, notamment avec le développement d'Internet. Cela fait désormais plusieurs décennies que l'humanité doit faire face à ce problème et pourtant très peu de personnes et d'entreprises ont des stratégies ou des plans d'intervention lorsqu'ils sont victime de cyberattaque, très peu sont assez préparés. Nous pensons que le web doit être une force au service du bien et non pas un espace où les fraudeurs avec des intentions malveillantes prennent le dessus. Des recherches concernant des solutions pour remédier aux attaques devraient donc être plus approfondies même si nous savions très bien que les hackers sont impossibles à éradiquer définitivement, des personnes malhonnêtes essayeront toujours de voler nos biens et nos données. De plus, depuis les premiers cas de cybercriminalité, les hackers et leurs techniques ne cessent de se développer et de ce fait la sécurité et le respect de la confidentialité sur le Web deviennent très compliqué et c'est malheureux car Internet a permis de faire évoluer le monde mais devient peu à peu un espace dangereux. Enfin, de nos jours beaucoup de jeunes utilisent le Web et sont donc contraint à faire face à des attaques eux aussi sans savoir comment réagir et nous pensons que faire plus de prévention leur serait donc très utile.

B) Notre point de vue vis-à-vis des solutions

Les entreprises et les citoyens ne sont clairement pas assez appuyées par ceux qui sont supposés leur apporter une aide. Comme le cas de Sanofi l'a prouvé, c'est aux entreprises de trouver leurs propres solutions pour se protéger. Certes l'entreprise crée des emplois en mettant en place tout cette politique de cybersécurité, certes c'est très efficace pour lutter contre les cyberattaques. Mais dans nos articles ressorti de la démarche de veille, nombreux parlent de cyberattaques visées sur les lieux de santé comme les Hôpitaux ou d'autres institutions publiques comme les mairies. Ce n'est pas normal qu'ils soient dans l'obligation de gérer tout cela seuls. De plus les solutions que les candidats politiques, aux élections présidentielles de 2022, proposent des solutions en matière de cybersécurité mais les cyberattaques existent depuis bien plus longtemps. On en entend un peu plus parler, uniquement cette année, alors que c'est quelque chose qui existe depuis longtemps. Les citoyens auraient dû être un peu plus informés et préparés à toutes les éventualités car, parmi les liens que nous avons sélectionnés, certains articles parlent de cyberattaques touchant des victimes d'attentat comme celui de Charlie Hebdo, ou encore des journaux ne pouvant plus accéder à la liberté d'expression à cause de ce fléau. Mais il est quand même important et c'est une très bonne chose que les choses changent maintenant et qu'on ne laisse pas traîner le problème.

Conclusion

Pour conclure, la cybersécurité est de nos jours un enjeu majeur pour la protection de nos données. Cependant depuis les années 1960 la cybercriminalité à fortement évolué. Elle a commencé par des trafics de lignes téléphoniques et puis a évolué avec l'apparition d'Internet. Partout dans le monde, des cybercriminels tentent constamment de voler des données, de pirater des comptes ou des cartes bleues ou encore de pratiquer le phishing et les ransomware. Il ne suffit que d'un seul clic pour que des logiciels malveillants aient accès à toutes nos informations personnelles. Internet est devenu un espace très dangereux où la sécurité est absente. Les victimes des cybercriminels, trop peu préparées à d'éventuelles attaques, sont les entreprises et la communauté en ligne, aussi bien les enfants que les adultes. Des solutions commencent à être envisagées par les entreprises elles-même ou par le projet de loi d' Emmanuel Macron également. Si nous pouvions donner quelques conseils lors de navigation sur le net ce serait de rester vigilant en ne cliquant pas sur des liens et pièces jointes que peuvent proposer des mails dont la provenance est méconnue. De plus, nous conseillons de faire attention aux logiciels et à la façon dont les médias sociaux et les outils numériques en ligne sont utilisés. Pour finir, la place des cyberattaques en France dans notre vie quotidienne est très importante et ne cesse d'augmenter au fil des années.

LECLERC, Jean-Marc. Une déferlante de cyberattaques en France. [en ligne]. 24 novembre 2021. Disponible à l'adresse : <https://www.lefigaro.fr/actualite-france/une-deferlante-de-cyberattaques-en-france-20211124>

L'article explique que les cyberattaques se multiplient en France contre les entreprises et les administrations.

EURONEWS. Une cyberattaque empêche la parution de 80 journaux régionaux en Norvège. [en ligne]. 31 décembre 2021. Disponible à l'adresse :

<https://fr.euronews.com/2021/12/31/une-cyberattaque-empeche-la-parution-de-80-journaux-regionaux-en-norvege>

L'article raconte comment 80 journaux de Norvège se sont retrouvés paralysés par une cyberattaque.

DA VEIGO, Diego. Seine-Saint-Denis : une cyberattaque perturbe plusieurs mairies. [en ligne]. 31 décembre 2021. Disponible à l'adresse : <https://www.lesechos.fr/pme-regions/ile-de-france/seine-saint-denis-une-cyberattaque-perturbe-plusieurs-mairies-1375797>
Des institutions publiques de Seine-Saint Denis ont été victimes de cyberattaques.

TV5MONDE. Qu'est-ce qu'une cyberattaque ? [en ligne]. 19 janvier 2022. Disponible à l'adresse : <https://information.tv5monde.com/info/qu-est-ce-qu-une-cyberattaque-440427>
L'article décrit ce qu'est une cyberattaque et les dommages qu'elles ont fait en Ukraine.

BANCAL, Damien. Piratage d'un cabinet d'avocats lié au procès Charlie Hebdo : « Un marketing de la malveillance », analyse un spécialiste de la cybersécurité. [en ligne]. 24 novembre 2021.
Disponible à l'adresse : https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/piratage-d-un-cabinet-d-avocats-lie-au-proces-charlie-hebdo-un-marketing-de-la-malveillance-analyse-un-specialiste-de-la-cybersecurite_4857155.html
Une analyse d'un expert en cybersécurité porte sur les attaques électronique qui ont été perpétrées contre les victimes des attentats de Charlie Hebdo.

20 MINUTES. Norvège : De nombreux journaux paralysés après une attaque par rançongiciel. [en ligne]. 30 décembre 2021. Disponible à l'adresse : <https://www.20minutes.fr/monde/3207603-20211230-norvege-nombreux-journaux-paralyses-apres-attaque-rancongiciel>

Une atteinte à la liberté d'expression a été détectée en Norvège après une cyberattaque qui cible des journaux.

VINCENT, Benjamin. Log4Shell, la faille informatique qui fait trembler la planète. [en ligne]. 26 décembre 2021. Disponible à l'adresse : https://www.francetvinfo.fr/replay-radio/nouveau-monde/log4shell-la-faille-informatique-qui-fait-trembler-la-planete_4877969.html

Qu'est-ce que la Log4shell? C'est ce que nous découvrons dans cet article ainsi que l'impact qu'a eu l'affaire.

BARBEY, Grégoire. En matière de cybersécurité, 2022 pourrait bien ressembler à 2021. [en ligne]. 27 décembre 2021. Disponible à l'adresse : <https://www.heidi.news/innovation-solutions/en-matiere-de-cybersecurite-2022-pourrait-bien-ressembler-a-2021>

Heidi.News donne son avis en matière de cybersécurité pour l'année 2022.

SANOFI. Cybersécurité: comment faire face aux menaces permanentes de la cybercriminalité? [en ligne]. 2022. Disponible à l'adresse : <https://www.sanofi.fr/fr/Actualites/nos-actualites/cybersecurite-sanofi-se-mobilise-pour-lutter-contre-la-cybercriminalite>

L'entreprise Sanofi a subit une cyberattaque en 2020. Elle explique son système de cybersécurité mis en place depuis.

TUNG, Liam. Cybersécurité: Attention aux escrocs qui se cachent dans vos visioconférences. [en ligne]. 22 février 2022. Disponible à l'adresse : <https://www.zdnet.fr/actualites/cybersecurite-attention-aux-escrocs-qui-se-cachent-dans-vos-visioconferences-39937763.htm>

L'article explique les méfiances que l'on doit adopter lors du télétravail face aux menaces cybercriminels.

FRANCEINFO, AFP. Cyberattaque en Ukraine: le ministère des Affaires étrangères ukrainien affirme avoir des « indices » de l'implication russe. [en ligne]. 14 janvier 2022. Disponible à l'adresse : https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cyberattaque-en-ukraine-le-ministere-des-affaires-etrangeres-ukrainien-affirme-avoir-des-indices-de-l-implication-russe_4917219.html

L'article porte sur l'enquête que le gouvernement ukrainien a ouverte afin de savoir si, oui ou non, la Russie est impliquée dans une cyberattaque de 70 sites gouvernementaux.

LEPOINT.FR. Attentats contre « Charlie Hebdo » : des éléments confidentiels ont fuité. [en ligne]. 24 novembre 2021. Disponible à l'adresse : https://www.lepoint.fr/justice/attentat-contre-charlie-hebdo-des-elements-confidentiels-ont-fuite-24-11-2021-2453659_2386.php
Cet article raconte ce que les cyberattaques, commises sur les victimes des attentats de Charlie Hebdo, ont récupéré de confidentiel.

LEMATIN.CH. Un des principaux médias paralysé par une attaque au rançongiciel. [en ligne]. 29 décembre 2021. Disponible à l'adresse : <https://www.lematin.ch/story/un-des-principaux-medias-paralyse-par-une-attaque-au-rancongiciel-765005892256>
L'article annonce que le groupe Amedia a été victime d'une cyberattaque qui l'a paralysé.

LICATA CARUSO, Damien. Thales refuse le chantage, des hackers publient les données volées à sa branche aérospatiale. [en ligne]. 18 janvier 2022. Disponible à l'adresse : <https://www.leparisien.fr/high-tech/un-groupe-de-hackers-publie-des-donnees-volees-a-la-branche-aerospatiale-de-thales-18-01-2022-Z4YNRKZ3GJGDBL5EF4JBL64TOY.php>
L'entreprise Thales réponds à l'offensive des cyberattaques.

DEFIMEDIA.INFO. Lutte contre la cybercriminalité: Facebook a recruté des Mauriciens pour s'attaquer aux «commentaires» abusifs en kreol, selon le ministre Balgobin. [en ligne]. 11 2021. Disponible à l'adresse : <https://defimedia.info/lutte-contre-la-cybercriminalite-facebook-recrute-des-mauriciens-pour-sattaquer-aux-commentaires-abusifs-en-kreol-selon-le>
Facebook prend des mesures radicale pour lutter contre la cybercriminalité présente sur le réseau.

AIT, Amine. Lutte conre le cybercriminalité: le justice persiste et signe. [en ligne]. 24 novembre 2021. Disponible à l'adresse : <https://www.algerie360.com/hausse-de-cybercriminalite-la-justice-monte-au-creneau/>
Algérie 360 nous informe que l'Algérie a pris la décision de lutter contre la cybercriminalité.

DOUMENG, Lionel. La cybersécurité n'est plus l'affaire des entreprises mais des MSSP. [en ligne]. 2 novembre 2022. Disponible à l'adresse : <https://www.lemondeinformatique.fr/actualites/lire-la-cybersecurite-n-est-plus-l-affaire-des-entreprises-mais-des-mssp-85753.html>
L'article porte sur les solutions que les entreprises peuvent adopter pour lutter contre les cyberattaques.

VINCENT, Benjamin. Invasion de l'Ukraine : les coulisses des cyber-attaques. [en ligne]. 27 février 2022. Disponible à l'adresse : https://www.francetvinfo.fr/replay-radio/nouveau-monde/invasion-de-lukraine-les-coulisses-des-cyber-attaques_4962966.html
L'article porte sur les cyberattaques que l'Ukraine a subit et la cyber-offensive mise en place.

OUEST FRANCE, Afp. Guerre en Ukraine. Les hackers d'Anonymous revendiquent une cyberattaque contre des médias russes. [en ligne]. 28 février 2022. Disponible à l'adresse: <https://www.ouest-france.fr/monde/guerre-en-ukraine/guerre-en-ukraine-les-hackers-d-anonymous-revendiquent-une-cyberattaque-contre-des-medias-russes-9caa731e-9896-11ec-a212-1f68235c1350>
Ouest France présente l'affaire des hackers Anonymous qui déclarent une cyber guerre à la Russie.

LEAL, Daniel. Guerre en Ukraine : « Le risque de cyberattaque est élevé » en France alerte le ministère de l'Intérieur. [en ligne]. 26 février 2022. Disponible à l'adresse :
https://www.francetvinfo.fr/monde/europe/manifestations-en-ukraine/guerre-en-ukraine-le-risque-de-cyberattaque-est-eleve-en-france-alerte-le-ministere-de-l-interieur_4982682.html
L'article porte sur les inquiétudes, qu'a le ministère de l'intérieur français, concernant les cyberattaques pouvant être liées au conflit entre l'Ukraine et la Russie.

OLAIZOLA, Nick. Engager des pirates en ligne, c'est désormais un jeu d'enfants. [en ligne]. 24 novembre 2021. Disponible à l'adresse : <https://www.fredzone.org/engager-des-pirates-en-ligne-cest-desormais-un-jeu-denfant>

L'article porte sur les dangers du web et la facilité qu'il offre pour obtenir des services de hackers.

COURTIN, Aude. Dans les coulisses de l'info : comment nous avons été informés de la cyberattaque à l'hôpital de Dax. [en ligne]. 26 décembre 2021. Disponible à l'adresse :
<https://www.sudouest.fr/sante/dans-les-coulisses-de-l-info-comment-nous-avons-ete-informes-de-la-cyberattaque-a-l-hopital-de-dax-7383641.php>
L'article porte sur la série de cyberattaques que l'hôpital de Dax a subit.

POULLENNEC, Solenn. Cyberattaques : un rapport rejette l'interdiction du paiement des rançons par les assureurs. [en ligne]. 22 février 2022. Disponible à l'adresse :
<https://www.lesechos.fr/finance-marches/banque-assurances/cyberattaques-un-rapport-rejette-linterdiction-du-paiement-des-rancons-par-les-assureurs-1388776>
Les Echos propose un article sur les solutions, face à la cybercriminalité, de la part des hautes institutions.

BENECH, Emile. Cyberattaque, fuite de données, panne mondiale... Les gros ratés des géants de la technologie en 2021. [en ligne]. 29 décembre 2021. Disponible à l'adresse : <https://www.ouest-france.fr/leditiondusoir/2021-12-29/cyberattaque-fuite-de-donnees-panne-mondiale-les-gros-rates-des-geants-de-la-technologie-en-2021-b6634516-179f-4b7f-b6e3-7ef710472362>
Ce journal en ligne propose un article sur toutes les plus grosses cyberattaques que le monde a connu en 2021.

RFI. Cyberattaque en Ukraine: un moyen pour augmenter la tension durant les négociations. [en ligne]. 15 janvier 2022. Disponible à l'adresse : <https://www.rfi.fr/fr/europe/20220115-cyberattaque-en-ukraine-un-moyen-pour-augmenter-la-tension-durant-les-n%C3%A9gociations>
L'article explique les nouvelles tensions entre l'Ukraine et la Russie à la suite d'une série de cyberattaques.

L'ÉQUIPE. Craintes pour la cybersécurité des athlètes aux JO de Pékin. [en ligne]. 20 janvier 2022. Disponible à l'adresse : <https://www.lequipe.fr/Tous-sports/Actualites/Craintes-pour-la-cybersecurite-des-athletes-aux-jo-de-pekin/1311846>
La cybersécurité devient primordiale pour les citoyens. L'article parle des mesures prises par les athlètes des JO de Pékin afin de ne pas subir de cyberattaques.

DANTON, Loïc. Conseil action – Bureau Veritas: une cyberattaque qui contrarie une belle dynamique. [en ligne]. 24 novembre 2021. Disponible à l'adresse : <https://bourse.lefigaro.fr/actu-conseils/conseil-action-bureau-veritas-une-cyberattaque-qui-contrarie-une-belle-dynamique-20211124>
Le Bureau Véritas, spécialisé dans les diagnostics et les certification pour les entreprise, a subit une cyberattaques qui l'a beaucoup pénalisé.

LICATA CARUSO, Damien. Attentat de Charlie Hebdo : des hackers tentent d'extorquer de l'argent à des avocats de victimes. [en ligne]. 24 novembre 2021. Disponible à l'adresse :
<https://www.leparisien.fr/high-tech/attentat-de-charlie-hebdo-des-hackers-tentent-dextorquer-des-avocats-de-victimes-24-11-2021-7NGHVRDISBAKDhuecksefQ5ELY.php>
Après les attentats de Charlie Hebdo, la persécution continue lorsque les victimes reçoivent des cyber menaces.

LEPOINT.FR. «J'étais opposé au pass sanitaire» : les explications du hacker qui a piraté l'AP-HP. [en ligne]. 1 janvier 2022. Disponible à l'adresse : https://www.lepoint.fr/faits-divers/j-etais-oppose-au-pass-sanitaire-les-explications-du-hacker-qui-a-pirate-l-ap-ph-01-01-2022-2458833_2627.php
L'assistance publique-hôpitaux de Paris (AP-HP) a été piraté par un hacker contre le pass vaccinale.