

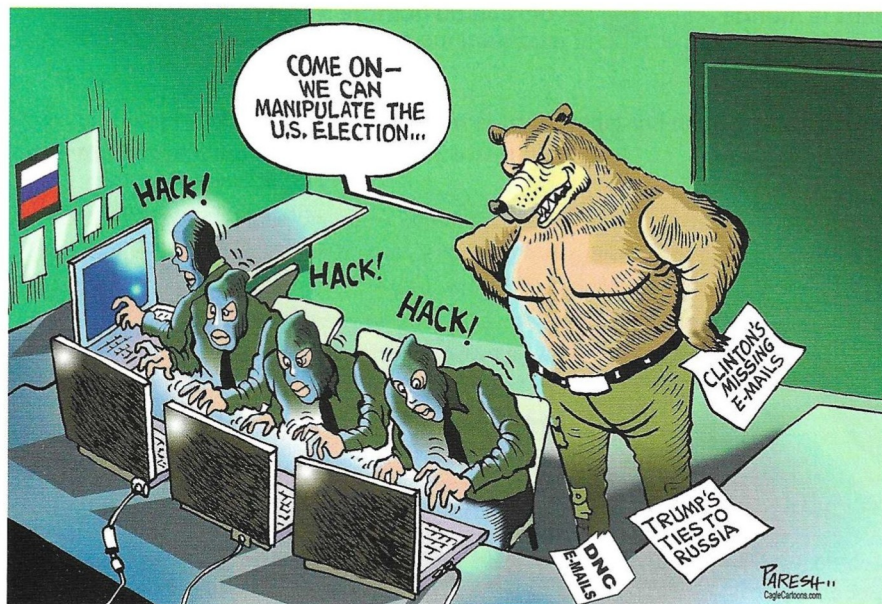
Étude critique de document(s)

SUJET ➡ Le cyberspace, un terrain de tensions géopolitiques

En analysant les documents, en les confrontant et en vous appuyant sur vos connaissances, montrez les cyber-risques qui menacent l'équilibre géopolitique et les moyens mis en œuvre pour y faire face.



Activité à télécharger
hachette-clic.fr/24hggt278



1 Les cybermenaces, un risque pour la démocratie

Source : dessin de Paresh Nath, 29 juillet 2016.

Traduction : Allez ! Nous pouvons manipuler les élections américaines... ; suppression des e-mails de Clinton ; les liens entre Trump et la Russie ; les e-mails du Parti démocrate.

2 Une cybersécurité française et européenne inégalement protectrice

Les cyber-risques constituent une atteinte à des systèmes informatiques avec une portée malveillante, qui peuvent cibler des ordinateurs, des serveurs ou des équipements périphériques [imprimantes, appareils communicants, ...].

5 Au total, quatre risques principaux peuvent être mis en avant : la cybercriminalité, l'espionnage, le sabotage et l'atteinte à l'image.

Face à ces risques, les législations françaises et européennes de protection des données sont considérées comme
10 particulièrement protectrices. L'enjeu principal réside aujourd'hui plutôt en la sécurisation plus poussée des systèmes d'information et dans les réactions à mettre en place lorsqu'un système informatique est attaqué. Il s'agirait également d'agir et d'uniformiser les moyens d'action à

15 l'échelle internationale [car, par définition, une cyberattaque ne se limite pas aux frontières d'un pays] : l'Organisation internationale de la police criminelle [Interpol], créée en 1923 et dont l'objectif est la promotion de la coopération policière internationale, tente d'organiser une collaboration
20 étroite entre les partenaires publics privés pour lutter contre ces attaques. Interpol offre ainsi des plateformes sécurisées d'échange de données, des formations et des analyses pour réduire les cyber-risques. La cybersécurité prend en effet une ampleur géopolitique : l'introduction d'un
25 État au sein des services liés à la cybersécurité d'un autre État constitue une clé majeure pour bénéficier d'informations privilégiées et précieuses sur l'État espionné.

Gilles Jaillot, Valérian Rabot et Éléonore Yidizhan,
Grands enjeux contemporains, Ellipses, 2023.

Internet en Chine

Consigne À partir de l'analyse et de la confrontation des documents, vous caractériserez le développement et les enjeux géopolitiques d'Internet en Chine.

1 Le contrôle d'Internet en Chine

Alors que l'économie chinoise se numérise [...] et que les Chinois sont de plus en plus connectés [...] les grands réseaux sociaux internationaux comme Facebook, Twitter, Instagram ou YouTube, mais également les moteurs de recherche tel Google, ainsi que la plupart des médias occidentaux, sont inaccessibles sur le territoire chinois. Tous sont bloqués par la « grande muraille électronique » érigée par le ministère de la Sécurité publique. Si le gouvernement affirme officiellement souhaiter protéger le peuple chinois des mauvaises influences venues de l'extérieur (le terrorisme, les jeux d'argent, la pornographie, les incitations à la violence, etc.), l'objectif est également d'interdire l'accès à tous les contenus jugés sensibles politiquement. [...] De réels mouvements de protestations se sont fait entendre depuis l'intensification des contrôles sur les contenus « inappropriés » de la plate-forme Sina Weibo, hybride chinois de Twitter et Facebook, à la suite de la nouvelle loi sur la cybersécurité du 1^{er} juin 2017. En avril 2018, la plate-forme annonçait la suppression de contenus liés à l'homosexualité dans le cadre d'une « campagne de nettoyage » visant à assurer un Internet « clair et harmonieux » conforme à la volonté étatique [...]. Après que 220 000 usagers de Sina Weibo ont protesté en utilisant le hashtag¹ #Jesuisgay, la plate-forme et le gouvernement faisaient marche arrière, conscients de la mauvaise publicité nationale et internationale que ce mouvement engendrait.

Nashidil Rouiaï, *Carto*, n° 50, nov.-déc. 2018.

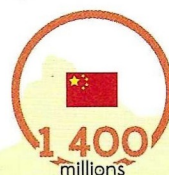
1. Mot clé précédé du symbole # utilisé par les internautes sur les réseaux sociaux et permettant l'accès au contenu qui contient ce mot clé.

2 La Chine, un marché de l'Internet en pleine expansion en 2017

INTERNET

Population chinoise

Total d'utilisateurs¹



802 millions

Pourcentage de la population totale



CHINE

57,7 %

¹ Données 2018

Population américaine

Total d'utilisateurs²



327 millions



292 millions

Pourcentage de la population totale



ÉTATS-UNIS

89 %

² Données 2017

ET 2 : La surveillance des darknets, un enjeu pour les États

CONSIGNE : À partir du document, montrez que le contrôle des darknets représente un enjeu important pour les États.

1 La traque des délinquants sur les darknets : une entreprise difficile

« En quelques clics, vous pouvez commander de la drogue, acheter des armes, voire même commanditer un meurtre. Tout ceci est possible sur le darknet, un réseau internet quasi-invisible où les trafics illicites sont monnaie courante. Sur le plan international, cet “Amazon du vice” est devenu le repère des dealers en tous genres.

- 5 Comme sur les sites de vente en ligne [...], les stupéfiants (ou autres) sont exposés avec une photo, le prix et l’avis des clients. [...] Il existe même des forums où les usagers peuvent commenter les produits et filer leurs “bons plans”. Sans oublier les offres promotionnelles [...]

Aujourd’hui, la lutte contre ce fléau est primordiale pour le gouvernement. Le Centre
10 de lutte contre la criminalité numérique (C3N) et l’Office central de lutte contre la criminalité liée aux technologies de l’information et de la communication (OCLCTIC) œuvrent au quotidien pour traquer les dealers du darknet. Deux organismes qui travaillent en collaboration avec d’autres à l’étranger comme Europol¹, Interpol² ou encore le FBI.

- 15 Mais à l’échelle internationale, difficile de lutter, ensemble, contre ce réseau mondial [...]. Pour cause : les lois diffèrent d’un pays à l’autre, et la question de la sécurité internationale prime. [...]

Au quotidien, policiers et gendarmes spécialisés réalisent un travail “de petite souris”. L’une de leurs principales missions ? La veille. À Caen (Calvados), cinq gen-
20 darmes N’Tech (comprenez enquêteurs en technologies numériques) spécialisés dans la cybercriminalité et rattachés au C3N, consacrent une partie de leur activité au darknet. Faux profils sur des sites de drogues, surveillance des transactions,... cette “cyberpatrouille” met les mains dans le cambouis. [...]

[Le darknet], réseau de l’ombre, très structuré, possède son propre modèle écono-
25 mique. À aucun moment, l’acheteur et le vendeur ne se rencontrent. Tout est dématérialisé et les achats s’effectuent grâce à une monnaie virtuelle, le bitcoin. Une réelle difficulté pour les enquêteurs. [...]

Pour Éric Filiol, professeur à l’ESIEA (École supérieure d’informatique, électro-
nique, automatique) de Laval et ancien de la DGSE³, il faut passer en mode offen-
30 sif, comme le fait le FBI. [...] Autre solution selon l’expert : un travail collaboratif accru entre universitaires et gendarmes qui, d’après lui, “n’ont pas les connaissances nécessaires”. »

Éloïse Aubé, « Drogues, armes, sexe sur le Darknet : comment les autorités luttent contre “l’Amazon du vice” », actu.fr, 19 mars 2018, D. R.

1. Europol : agence européenne de police criminelle qui facilite l’échange de renseignements entre les polices des États européens.
2. Interpol : organisation qui favorise la coopération des polices de tous les pays.
3. DGSE (Direction générale de la sécurité extérieure) : services de renseignements extérieurs français.

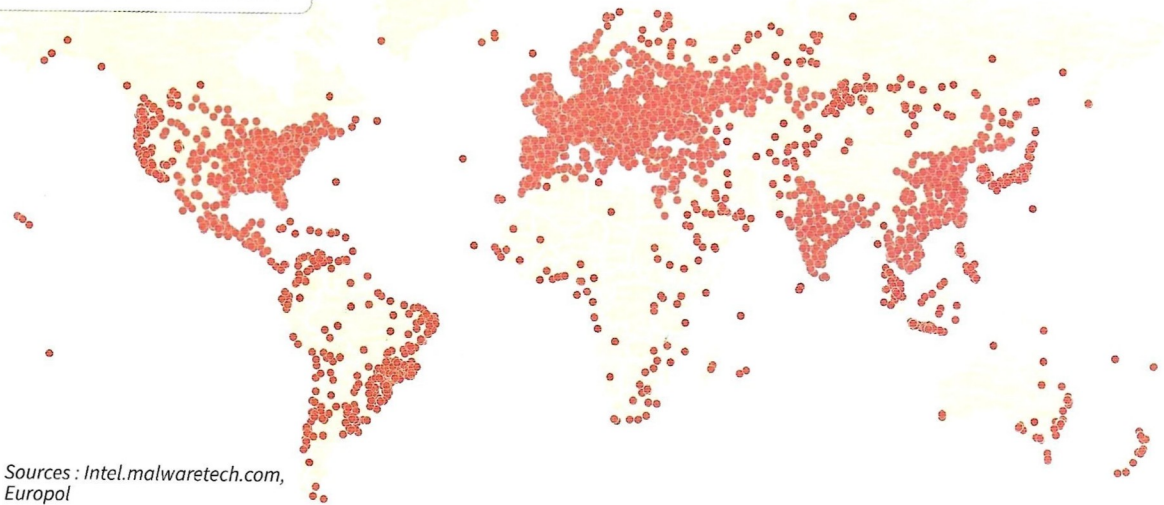
Sujet 3 Les rançongiciels : un risque cybermondial

► À partir des documents, montrez en quoi les rançongiciels constituent des risques majeurs, concernant des acteurs, des échelles et des enjeux variés.

La cyberattaque mondiale «WannaCry»

Ce logiciel malveillant qui réclame une rançon après le blocage de fichiers a fait plus de 200 000 victimes dans 150 pays

● IP infectées entre samedi et dimanche 15h30 GMT



Sources : Intel.malwaretech.com, Europol

© AFP

1 La diffusion de la cyberattaque

2 La cyberattaque du rançongiciel Wannacry, mai 2017

Royaume-Uni, Russie, Espagne, Portugal, France, Mexique... Vendredi 12 mai, des dizaines de milliers d'ordinateurs, dans au moins 99 pays, ont été infectés par un logiciel malveillant bloquant leur utilisation. [...] Outre-Manche, c'est le système de santé qui a été largement perturbé par ce virus informatique. Examens médicaux annulés ou perturbés, communications téléphoniques affectées, accès aux données bloqués... le Service national de santé (NHS) britannique [...] a été largement déstabilisé vendredi après-midi par ce logiciel qui prend en otage les usagers des ordinateurs en bloquant l'accès à leurs fichiers. [...] L'attaque aurait été renforcée par l'utilisation d'Eternal Blue, un outil de piratage mis au point par les services de renseignement américains et qui aurait été volé à l'Agence nationale de sécurité (NSA). [...] Le NHS n'a pas été la seule cible touchée par les pirates. [...] Ainsi, Telefonica, le géant espagnol des télécommunications, et plusieurs autres entreprises du pays ont été victimes d'un virus similaire. [...] Des opérateurs téléphoniques portugais et l'entreprise américaine de livraison FedEx ont également été

touchés, de même que le ministère de l'intérieur russe [...].

L'attaque, à ce stade, semble d'ampleur limitée en France, mais le secrétariat général pour la défense et la sécurité nationale estime qu'il n'y a aucune raison que le pays soit épargné. [...] L'Agence nationale de sécurité des systèmes d'information diffuse des messages de bonnes pratiques. [...] Selon la police française, plus de 75 000 ordinateurs ont été infectés dans le monde et ce nombre «devrait très vraisemblablement s'alourdir dans les jours qui viennent». [...] Les rançongiciels ont connu un développement exponentiel ces trois dernières années. Ils sont généralement conçus par des groupes criminels, et touchent le plus souvent les petites et moyennes entreprises, auxquelles ils extorquent des sommes variant entre quelques dizaines et quelques centaines d'euros par machine infectée – le paiement s'effectue en bitcoins, une monnaie virtuelle anonyme.

Philippe Bernard, Damien Leloup et Nathalie Guibert, « Une cyberattaque massive bloque des ordinateurs dans des dizaines de pays », *Le Monde*, 13 mai 2017.