OTC. LE CYBERESPACE : CONFLICTUALITE ET COOPERATION ENTRE LES ACTEURS

Introduction : de l'actualité du cyberespace à l'enjeu de la connaissance

Document 1. Des acteurs et des machines nécessaires au fonctionnement du cyberespace.

« De la fumée a été détectée peu avant 19 heures, vendredi, dans le local de batteries non raccordées et non connectées, précise OVHcloud dans un communiqué. Ce nouveau départ de feu aurait touché 300 batteries pesant chacune 25 kilogrammes sur le data center* SBG1, selon le journal local Dernières Nouvelles d'Alsace. Ce data center avait déjà été partiellement détruit par le précédent incendie, qui avait par ailleurs réduit un autre data center, SGB2, à néant. (…)

Ce site strasbourgeois d'OVHcloud avait été victime, dans la nuit du 9 au 10 mars, d'un important incendie. Ce sinistre, auquel s'était ajoutée une panne de courant, avait eu des répercussions bien au-delà des frontières françaises, ayant selon OVH affecté « 12 000 à 16 000 clients ». Des structures comme Coinhouse (le spécialiste français de vente et d'achat de bitcoins), le Centre Pompidou ou la plate-forme d'accès aux données* publiques data.gouv.fr avaient ainsi signalé des perturbations, seulement temporaires pour certaines, dans l'accès à leur site Internet* ou à l'utilisation des courriels*.

Mais, du fait que certains clients sont eux-mêmes des hébergeurs*, il s'est avéré que le nombre de sites touchés a été beaucoup plus important : 464 000 noms de domaines* distincts (dont 59 600 français) et 3,6 millions de serveurs* Web liés à OVHcloud étaient ainsi inaccessibles après l'incendie, tel que l'a comptabilisé la société américaine Netcraft. Diverses entreprises ont fait part de pertes définitives de données, tel le studio britannique de jeux vidéo Facepunch, éditeur de Rust.

OVHcloud a été créé en 1999 sous le nom d'« OVH » par Octave Klaba, jeune Français d'origine polonaise arrivé dans l'Hexagone à l'adolescence. L'entreprise avait commencé par faire de l'hébergement de sites Internet, avant de se lancer dans les services cloud* pendant la décennie 2010. Avec quelques – rares – autres acteurs, elle porte les espoirs du cloud européen face aux géants américains et chinois de ce secteur, devenu stratégique pour l'économie numérique. »

Le Monde avec Reuters, « Le site d'OVH à Strasbourg de nouveau touché par un incident », publié sur lemonde.fr, 20 mars 2021

CONSIGNES

1. Pourquoi les incendies de l'entreprise OVHcloud à Strasbourg vous ont-ils impactés personnellement depuis 15 jours ?
2. Définissez tous les termes marqués par une astérisque (*).
3. Montrez que les problèmes de cette entreprise française dépassent les frontières de la France.
4. Faites des hypothèses pour expliquer la phrase soulignée à la fin du texte.
5. Quels liens faire entre cet article et « l'enjeu de la connaissance » ?

Document 2. Tensions et conflits dans le cyberespace entre grandes puissances

« Que se passe-t-il dans le cyberespace ? Assiste-t-on à un tournant dans l'usage des moyens cyber et à leurs répercussions dans la sphère diplomatique ? C'est en tout cas ce que considèrent de plus en plus d'observateurs.

Après une première cyberattaque d'ampleur, officiellement attribuée à la Russie et révélée en décembre 2020[1], les Etats-Unis doivent gérer depuis début mars les conséquences d'une deuxième opération, majeure, contre un de leurs fleurons informatiques, Microsoft. Celle-ci serait le fait de hackers liés à la Chine, selon certains spécialistes.

Le dernier épisode de tensions est survenu mercredi 10 mars, lorsque l'accès à plusieurs sites officiels russes a été bloqué pendant plusieurs heures de manière inhabituelle. Ont notamment été atteints le portail de la Douma – la Chambre basse du Parlement russe –, celui du Kremlin ou encore celui de Roskomnadzor, l'équivalent russe de l'Agence française de la sécurité des systèmes d'information (Anssi) et de l'Autorité de régulation des communications électroniques (Arcep).

Moscou n'a pas officiellement réagi. Des experts y ont vu un dégât collatéral des manœuvres russes, le même jour, pour ralentir le réseau Twitter. Mais d'autres y ont lu la première traduction d'une réplique venue des Etats-Unis. (…)

Une volonté de cyber-riposte – dite de « *hack back* » –, elle-même avancée comme une réponse à l'opération de « *cyberespionnage* » sophistiquée de SolarWinds, révélée fin 2020. Pendant de longs mois, probablement à partir de mars 2020, des hackers russes ont ainsi réussi à s'introduire dans le système de dizaines de milliers de clients de cette société texane de logiciels. Parmi eux, de nombreuses firmes présentes dans Fortune 500 – un classement des 500 premières entreprises américaines selon l'importance de leur chiffre d'affaires –, ainsi que des agences fédérales sensibles, dont le département de la sécurité intérieure et le Pentagone.

(…) début mars, la Maison Blanche a reconnu qu'un autre front venait de s'ouvrir dans le cyberespace, avec une attaque visant cette fois la très populaire messagerie Exchange de Microsoft.

A ce stade, les autorités américaines se sont gardées d'attribuer cette attaque. Mais de nombreux spécialistes en cybersécurité, et la direction de Microsoft elle-même, ont dit y avoir identifié le mode opératoire de hackers liés à la Chine. Des accusations immédiatement dénoncées par le porte-parole du ministère chinois des affaires étrangères (…)

Dans le cyberespace, les Etats-Unis avaient signé avec la Chine un pacte de non-agression en 2015. Mais celui-ci a fait long feu, selon de nombreux observateurs. Dès le départ, cet accord établi sur la base d'un consensus minimum ne prenait pas en

compte les attaques commises par des acteurs non étatiques contre des sociétés privées, comme dans le cas de Microsoft. Depuis la révélation des dernières intrusions, l'Agence nationale de sécurité américaine (NSA), qui gère à la fois les actions cyberoffensives et défensives, se retrouve en tout cas fortement remise en cause.

Les autorités françaises et plus largement européennes s'efforcent quant à elles, pour l'heure, de rester en retrait de ces tensions et du narratif qui l'accompagne. Et ce, bien qu'un certain nombre d'institutions comme l'Autorité bancaire européenne (ABE), le 7 mars, et le Parlement norvégien, le 10 mars, aient d'ores et déjà annoncé avoir été victimes d'intrusions permises par les failles de Microsoft.

La France évite traditionnellement les attributions officielles de cyberattaques. (…) Interrogée par Le Monde le 10 mars, l'Anssi[2], le gendarme français de la cybersécurité, a indiqué « ne pas avoir, à ce stade, eu de retour particulier sur des cas de compromissions », à la suite des attaques contre SolarWinds et Microsoft. (…) »

Elise Vincent, « Tensions entre les Etats-Unis, la Russie et la Chine après deux cyberattaques majeures », publié dans lemonde.fr, 13 mars 2021.

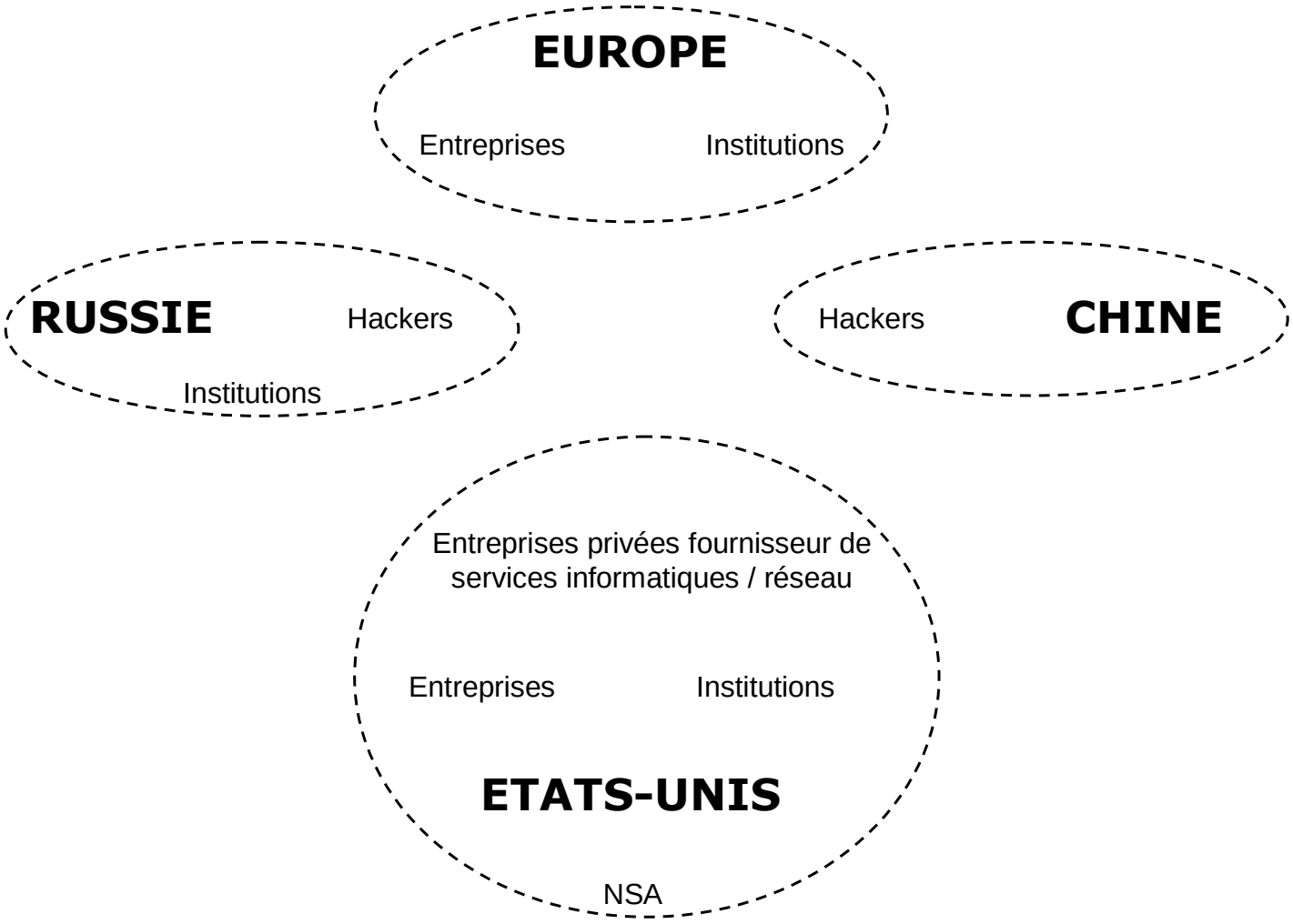
[1] Opération de cyberespionnage de SolarWind, voir plus loin dans l'article.

[2] L'ANSSI : Agence nationale de la sécurité des systèmes d'information, service du Premier ministre créé en 2009 ; l'Agence est l'autorité nationale chargée d'accompagner et de sécuriser le développement du numérique en France et apporte son expertise et son assistance technique aux administrations et aux entreprises.

CONSIGNES

6. Complétez le schéma ci-dessous en établissant les liens suivants avec des traits de différentes couleurs :

Liens présumés
Cyberattaque
Fournit des services
Lien officiel
Pacte de non-agression



7. Pourquoi les cyberattaques relèvent de conflictualités non-conventionnelles mais ayant des répercutions sur les relations interétatiques de plus en plus importantes ?

8. Quels liens faire entre cet article et « l'enjeu de la connaissance » ?