II Cyberdéfense, entre coopération européenne et souveraineté nationale : le cas français (paragraphe 2 p. 524).

En quoi défendre le cyberespace français est-il un enjeu de souveraineté nationale et suppose une politique de coopération ?

Exercice 1. Défendre le cyberespace : en enjeu national

1. Faites un bref rappel des différentes cybermenaces tout en identifiant les acteurs exposés aux risques (documents 1 à 3 ci-dessous et documents 1 à 3 p. 516)
2. Expliquez pourquoi la sécurité est particulièrement difficile à assurer dans le cyberespace (document 3 p . 516 et documents 1 à 3)
3. Définissez ce qu'est la cyberdéfence et Identifiez les différents moyens dont se dotent la France pour assurer la protection du cyberespace (introduction p. 518, documents 1 à 3 p. 518 et document 2 ci-dessous) ; présentez-en les limites
4. Montrez que la stratégie de la France évolue en 2019. Dites quelles critiques sont formulées (document 5 p. 518 et document 2)
5. Dites en quoi le document 6 p. 519 peut expliquer la citation de la ministre des armées : « la cybersécurité est un sport collectif ».

Exercice 2. Protéger le cyberespace : une impossible coopération internationale ?

1. Dites quel constat les eurodéputés font-ils et indiquez quelle stratégie ils préconisent en matière de cyberdéfense (document 4)
2. Dites quelles sont les réponses que l'UE apporte en matière de cybersécurité et montrez que celles-ci restent limitées (documents 4 à 6 p. 517 et document 4 ci-dessous)
3. Dites ce qu'est l'appel de Paris et indiquez sa portée (document 5 ci-dessous - à partir de 3 min. 54).
4. Expliquez la difficile mise en place d'une politique de coopération entre les Etats dans ce domaine (document 5 p. 517).

Document 1. Les hôpitaux victimes de cyberattaques (C'est dans l'air, France 5, 27 février 2021)
https://www.youtube.com/watch?v=Yh1LRwsRW7M

Document 2. Faire face à la cyberguerre (C'est dans l'air, France 5, 27 février 2021)
https://www.youtube.com/watch?v=8YvOgf44uUM

Document 3. Les citoyens face à la cybercriminalité (C'est dans l'air, France 5, 27 février 2021)
https://www.youtube.com/watch?v=kSw6ZJ3_Si0

Document 4. Pour une cyberdéfense européenne robuste et des liens plus étroits avec l'OTAN

Au vu des nouvelles menaces hybrides, il est vital de renforcer la cyberdéfense de l'UE avec une équipe d'intervention rapide et une coopération plus étroite avec l'OTAN.
C'est ce qu'ont déclaré les députés mercredi 13 juin dans une résolution adoptée par 476 voix pour, 151 voix contre et 36 abstentions. Le texte souligne que la Russie, la Chine et la Corée du Nord mais aussi des acteurs non étatiques ont été impliqués dans des attaques contre des infrastructures critiques de l'UE, la surveillance de masse des citoyens européens, des activités de cyberespionnage, des campagnes de désinformation et des restrictions d'accès à Internet (…).
Les députés précisent que la fragmentation des stratégies et des capacités de défense européennes a conduit à la vulnérabilité actuelle aux cyberattaques. C'est pourquoi ils exhortent les États membres à renforcer la capacité de leurs forces armées à travailler ensemble ainsi que la cybercoopération au niveau européen, avec l'OTAN et d'autres partenaires. Cela impliquerait davantage de cyberexercices conjoints, la formation et l'échange d'officiers militaires, le recrutement d'experts en cybercriminalistique, ainsi que l'amélioration de l'expertise en cyberdéfense des missions et opérations de l'UE.
Les députés se félicitent du lancement de deux cyberprojets dans le cadre de la coopération structurée permanente (PESCO), à savoir une plateforme d'échange d'informations sur les cyberincidents et des équipes

d'intervention rapide en cas d'incident informatique. Ils espèrent que cela mènera à la création d'une équipe européenne d'intervention rapide en matière de cybersécurité, qui coordonnerait, détecterait et contrerait les cybermenaces collectives. (…).

Le rapporteur sur la cyberdéfense, Urmas Paet (ALDE, EE), a déclaré: "*Une cyberattaque réussie peut transformer une centrale nucléaire en bombe nucléaire ou provoquer le chaos dans un hôpital, mettant la vie des patients en danger. Pour nous défendre contre de telles menaces, nous devons renforcer les capacités de cyberdéfense en renforçant la coopération entre les États membres, l'UE et l'OTAN*."

Communiqué de presse des députés européens, 13 juin 2018

Document 5. L'appel d'Emmanuel Macron à sécuriser le cyberespace (France 24, 12 novembre 2018)

https://www.youtube.com/watch?v=u89Z0fjZKC4

Pour aller plus loin :

Cybermenaces, cybertensions, cybersabotage, cyberespionnage, cyberguerres… Que recoupent ces termes ?
https://www.vie-publique.fr/parole-dexpert/276997-cyberespace-nouveaux-defis-nouveaux-risques

Cybercriminalité : comment lutter contre ce fléau mondial ? France Info 31 janvier 2021
https://www.francetvinfo.fr/internet/securite-sur-internet/cyberattaques/cybercriminalite-comment-lutter-contre-ce-fleau-mondial_4278495.html

Cybercriminalité : quel est le profil type des hackers qui attaquent hôpitaux et entreprises ?
Europe 1, le 20 février 2021
https://www.europe1.fr/technologies/cybercriminalite-quel-est-le-profil-type-des-hackers-qui-attaquent-hopitaux-et-entreprises-4026467

Cybercriminalité : Emmanuel Macron annonce un plan contre les attaques informatiques à l'hôpital de Villefranche
https://france3-regions.francetvinfo.fr/auvergne-rhone-alpes/rhone/lyon/cyberattaque-emmanuel-macron-en-direct-de-l-hopital-de-villefranche-1961509.html

Cellule de crise. Espions et pirates informatiques. La cyberguerre est déclarée. 02/03/2020
https://vimeo.com/397257776

Deepfakes : la menace devient réelle
https://www.lci.fr/high-tech/video-deepfake-la-menace-devient-reelle-2143709.html

La stratégie de la France en matière de cyberdéfense et cybersécurité
https://www.ssi.gouv.fr/publication/la-strategie-de-la-france-en-matiere-de-cyberdefense-et-cybersecurite/

Le livre blanc de la cyberdéfense
http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/