

En analysant le document et en vous appuyant sur vos connaissances, montrez que le cyberspace est conflictuel et expliquez comment la France répond à ces menaces.

Document

Rédigés à la demande du président de la République, les Livres blancs sur la Défense et la sécurité nationale fixent les orientations stratégiques de la France. Quatre Livres blancs ont été rédigés entre 1972 et 2020.

Les systèmes d'information sont désormais une donnée constitutive de nos sociétés. Au-delà des facilités considérables qu'elle apporte, l'interconnexion des systèmes d'information est une source de vulnérabilités nouvelles. Déjà identifiés dans le précédent Livre blanc, les menaces et les risques induits par l'expansion généralisée du cyberspace ont été confirmés, qu'il s'agisse d'atteintes à des systèmes résultant d'actes intentionnels ou de ruptures accidentelles mettant en cause le fonctionnement d'une infrastructure numérique critique.

Le développement rapide des infrastructures numériques ne s'est pas toujours accompagné d'un effort parallèle de protection, de sorte que les agressions de nature cybernétique sont relativement faciles à mettre en œuvre et peu coûteuses. Leur furtivité complique l'identification de leurs auteurs qui peuvent être aussi bien étatiques que non-étatiques. Les agressions les plus sophistiquées requièrent néanmoins une organisation complexe. Une attaque d'envergure contre une infrastructure numérique repose sur une connaissance détaillée de la cible visée, connaissance qui peut s'acquérir par des attaques préalables de moindre ampleur destinées à tester la cible, ou par des renseignements obtenus par d'autres moyens.

Les menaces qui se développent dans le cyberspace sont de plusieurs ordres. Au plus bas niveau, elles sont une forme nouvelle de criminalité, qui ne relève pas spécifiquement de la sécurité nationale : vol d'informations personnelles à des fins de chantage ou de détournements de fonds, usurpation d'identité, trafic de produits prohibés, etc. Relèvent en revanche de la sécurité nationale les tentatives de pénétration de réseaux numériques à des fins d'espionnage, qu'elles visent les systèmes d'information de l'État ou ceux des entreprises. Une attaque visant la destruction ou la prise de contrôle à distance de systèmes informatisés commandant le fonctionnement d'infrastructures d'importance vitale, de systèmes de gestion automatisés d'outils industriels potentiellement dangereux, voire de systèmes d'armes ou de capacités militaires stratégiques pourrait ainsi avoir de graves conséquences.

Le cyberspace est donc désormais un champ de confrontation à part entière. La possibilité, envisagée par le précédent Livre blanc, d'une attaque informatique majeure contre les systèmes d'information nationaux dans un scénario de guerre informatique constitue, pour la France et ses partenaires européens, une menace de première importance.

Lecture cursive...

=> On repère ce qui est utilisable, ce qu'on commente et là où je peux me servir du cours (**en bleu gras**)... il n'est noté QUE ce qui est dans le cours que l'on a eu ensemble.....

Plus j'en sais, mieux je peux exploiter le doc
en utilisant mes connaissances

=> qui **donnent du sens** à ce qui est dit (et sans paraphrase),

=> qui font **comprendre** ce que l'auteur dit,

=> qui permettent de mettre le doc et ses idées **en perspective**,

=> qui permettent enfin d'**élargir** le questionnement

Donc qqpart on doit décrire le cyberspace

Donc il faut relever les moyens employés par la France pour lutter contre les menaces, voir à participer au conflit....

En analysant le document et en vous appuyant sur vos connaissances, montrez que **le cyberspace est conflictuel** et **expliquez comment la France répond à ces menaces.**

Document

Rédigés à la demande du président de la République, les Livres blancs sur la Défense et la sécurité nationale fixent les orientations stratégiques de la France. Quatre Livres blancs ont été rédigés entre 1972 et 2020.

Source : Livre blanc sur la défense et sur la sécurité nationale, 2013

*Qui est l'auteur ???
Sans doute des spécialistes
du conflit, donc des
Militaires....*

*L'exécutif s'en occupe directement
La défense est de la prérogative du psdt
Même si il y a un ministre de la défense...
(=connaissance de la Ve république)*

*48 ans.. donc en moyenne un livre blanc
pour une douzaine d'années ?.... en fait pas
du tout mais ça vous ne le saviez pas : 1972/
1994/ **2008** et 2013 ... 2013, 5 ans après le
Dernier (**ça c'est dans le cours...**) c'est qu'il
y a urgence... **Dès 2008 l'Etat a intégré
les questions cyber => ANSSI 2009...(dans
le cours, le 1er rapport sur le sujet date
de 2006)***

Les systèmes d'information sont désormais une donnée constitutive de nos sociétés. Au-delà des facilités considérables qu'elle apporte, l'interconnexion des systèmes d'information est une source de vulnérabilités nouvelles. Déjà identifiés dans le précédent Livre blanc, les menaces et les risques induits par l'expansion généralisée du cyberspace ont été confirmés, qu'il s'agisse d'atteintes à des systèmes résultant d'actes intentionnels ou de ruptures accidentelles mettant en cause le fonctionnement d'une infrastructure numérique critique.

Le développement rapide des infrastructures numériques ne s'est pas toujours accompagné d'un effort parallèle de protection, de sorte que les agressions de nature cybernétique sont relativement faciles à mettre en œuvre et peu coûteuses. Leur furtivité complique l'identification de leurs auteurs qui peuvent être aussi bien étatiques que non-étatiques. Les agressions les plus sophistiquées requièrent néanmoins une organisation complexe. Une attaque d'envergure contre une infrastructure numérique repose sur une connaissance détaillée de la cible visée, connaissance qui peut s'acquérir par des attaques préalables de moindre ampleur destinées à tester la cible, ou par des renseignements obtenus par d'autres moyens.

À partir de ça, évoquer le cyberspace, ses structures, son histoire...(*)

► 2008 (=cours!)

Les menaces, les cyberattaques (#)

On n'a pas évoqué d'accident, mais on sait que tout ce système dépend de l'alimentation électrique qui peut faire défaut...

► Suite du (*)

► Suite du (#)

► Précisions sur les auteurs étatiques ou non... et donc leurs motivations => idéologiques ou géopolitiques

► Couche infrastructurelle – suite du (*)

► Espionnage par signint ou humint / encore la connaissance !!! / connaissance par attaque

Les menaces qui se développent dans le cyberspace sont de plusieurs ordres.

Au plus bas niveau, elles sont une forme nouvelle de **criminalité**, qui ne relève pas spécifiquement de la sécurité nationale : vol d'informations personnelles à des fins de chantage ou de détournements de fonds, usurpation d'identité, trafic de produits prohibés, etc.

Relèvent en revanche de la sécurité nationale les **tentatives de pénétration de réseaux numériques à des fins d'espionnage**, qu'elles visent les systèmes d'information de l'État ou ceux des entreprises. Une attaque visant la destruction ou la prise de contrôle à distance de systèmes informatisés commandant le fonctionnement [d'infrastructures d'importance vitale], de systèmes de gestion automatisés / d'outils industriels potentiellement dangereux/, voire de systèmes d'armes ou de capacités militaires stratégiques pourrait ainsi avoir de graves conséquences.

Le cyberspace est donc désormais un champ de confrontation à part entière.

La possibilité, envisagée par le précédent Livre blanc, d'une attaque informatique majeure contre les systèmes d'information nationaux dans un scénario de guerre informatique constitue, pour la France et ses partenaires européens, une menace de première importance.

Phrase d'annonce... c'est la typologie du livre blanc, donc ce qui aide le pouvoir exécutif à prendre les décisions **que l'on connaît par ailleurs => LID 2011, LIO 2018**

Donc ça n'est pas de la cyberdéfense... **Ministre intérieur+DGSI => cybersécurité**

C'est presque une définition de ce qui est stratégique pour l'Etat... il faut entendre [hopitaux => **cyber attaques de 2021**] , /barrages électriques, usines seveso .../ et bien sur tout ce qui est militaire...avions de chasse aussi suivez l'actualité, il y a des pannes tous les mois !!!!

Justification de l'intérêt pour l'armée
=> comcyber, recrutements, budget

Conflits numériques en cours : Ukraine au moins... **=> Stuxnet 2010 / F Parly en 2019 « la cyber guerre est commencée »**

=> association dans le cadre de l'UE, RGPD au moins