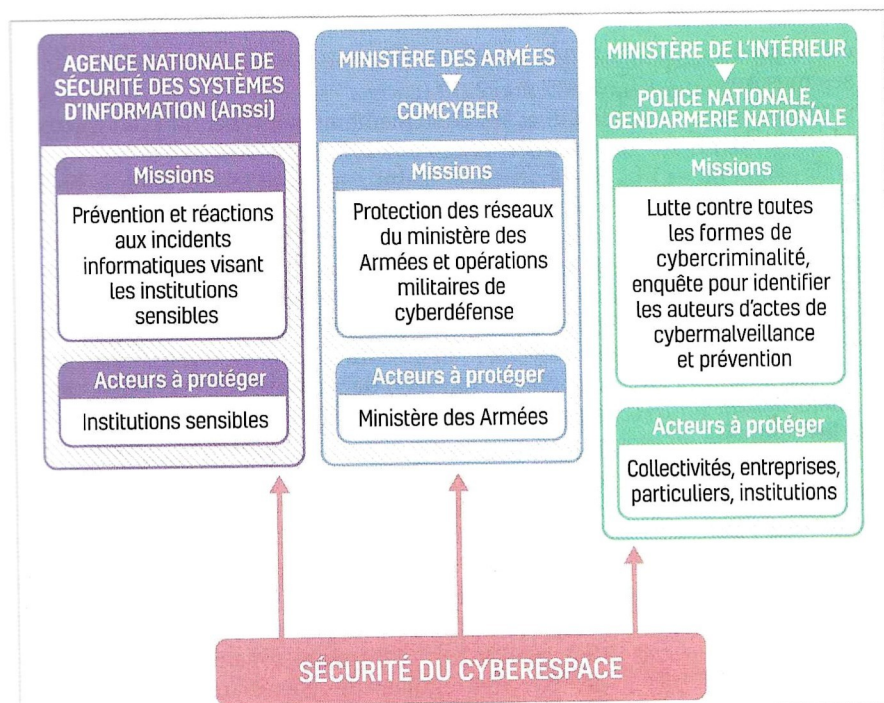


Défendre le cyberspace, un enjeu pour la France

En 2008, le Livre blanc de la défense nationale affirme que la protection des systèmes d'information constitue une composante à part entière de la politique de défense et de sécurité. Alors que la société et l'économie françaises dépendent de plus en plus de ces systèmes d'information, l'État se dote de différents moyens pour garantir sa cybersécurité et sa cybergdéfense.

→ En quoi défendre le cyberspace français est-il un enjeu de souveraineté nationale ?



1 Les acteurs de la stratégie nationale de la sécurité du numérique en France

3 La mise en place de moyens dédiés au cyberspace

En 2009, la France fonde l'Agence nationale de la sécurité des systèmes d'information. L'année suivante, les États-Unis créent l'US Army Cyber Command. Le Livre blanc sur la défense et la sécurité nationale de 2013 élève le cyberspace au rang de priorité stratégique en France. En décembre 2016, Jean-Yves Le Drian, alors ministre de la Défense, annonce la création d'un cybercommandement. Entre 2014 et 2019, la France consacrera un milliard d'euros à la cybergdéfense et se dotera d'une cyberarmée de 3200 hommes. La cyberguerre permet aux États de combattre des ennemis, mais aussi d'espionner des pays alliés en exploitant les failles de sécurité zero-day et les limites des machines. « Nous n'avons pas d'amis », rappelait Churchill.

Après le sommet Netmundial de 2014, le Brésil et l'Europe décident d'installer un câble sous-marin pour contourner cette domination. Pour Jean-Yves Le Drian, « si une attaque cyber s'apparente à un acte de guerre, une riposte adéquate s'imposera, dans une logique de conflit ouvert », conformément à l'article 51 de la Charte des Nations unies pour les conflits conventionnels. Toutefois, la difficulté d'établir les responsabilités rend les représailles délicates. Trouver l'origine d'un programme malveillant sophistiqué est plus complexe que suivre la trajectoire d'un missile. Sans oublier que la propagation des virus peut faire des victimes collatérales.

Soline Toussaint, « Le cyberspace : champ de bataille du XXI^e siècle », *Diplomates*, 19 décembre 2017.

REPÈRES

► **Livre blanc** Texte qui définit les grandes orientations dans un domaine donné.

► **Hacker** Pirate informatique, individu capable de s'introduire dans un réseau et de le détourner.



2 Le Comcyber

Créé en 2017, le Comcyber est l'unité opérationnelle qui commande l'ensemble des forces de cybergdéfense des armées françaises sous l'autorité du chef d'État-major des armées. Il est notamment en charge de la défense des systèmes d'information du ministère des Armées ainsi que de la conduite des opérations militaires de cybergdéfense. Il compte 3 400 cyber-combattants en 2018. Il assure également le développement et l'animation de la réserve citoyenne de cybergdéfense.

REGARD D'EXPERT

Le Bureau des Légendes, saison 4

Créée en 2015 par Éric Rochant, la série met en scène des agents de la DGSE (Direction générale de la sécurité extérieure en France) et montre, notamment dans la saison 4, les enjeux liés au contrôle du cyberspace.



5 La doctrine cyber offensive

La cybersécurité, c'est un sport collectif. La faille peut venir de partout. Les hackers sont pleins d'inventivité. [...] En 2017, les réseaux de la défense ont subi 700 événements de sécurité dont 100 cyberattaques. [...] Et non seulement le nombre d'attaques augmente mais les attaquants ont toujours des profils aussi variés. Un adolescent peut pirater les mails de la chancellerie allemande pour s'amuser, presque par hasard. Un groupe anonyme peut s'en prendre à nos industries, nos transports, nos hôpitaux sans raison apparente. Un État, enfin, peut chercher à affirmer sa puissance en nous espionnant, nous manipulant ou même en sabotant nos capacités. [...] La guerre cyber a bel et bien commencé [...] et nous allons nous y préparer. J'ai annoncé devant le Commandement cyber [...] que la France revendiquait d'utiliser l'arme cyber au même titre que toutes les armes conventionnelles. J'ai pu énoncer les grands principes de notre nouvelle doctrine cyber offensive et le renforcement de notre défense cyber. L'arme cyber n'est pas seulement pour nos ennemis ou nos fictions. Non. Nous aussi, en France, pouvons défendre, répliquer et attaquer. En opération, nous employons déjà l'arme cyber. Nous avons publié les grandes lignes de cette doctrine pour le faire savoir [...].

Discours de Florence Parly, ministre des Armées, janvier 2019.

6 Le rôle des entreprises du numérique



L'omniprésence du numérique dans tous les aspects de la vie quotidienne fait des entreprises du numérique des acteurs à part entière de la sécurité nationale. Ces entreprises, qui gèrent le réseau au quotidien, sont les premières à observer les attaques. Elles conçoivent également les produits et les services de sécurité informatique utilisés dans la détection et la protection contre les attaques. Elles sont également les opérateurs des plateformes d'intermédiation (réseaux sociaux) utilisées par les djihadistes pour leur propagande. Elles touchent ainsi jusqu'aux fonctions les plus régaliennes de l'État. Dès lors, la coopération entre le secteur public et ces entreprises du numérique est devenue non seulement une nécessité, mais une condition même à la sécurité nationale. La France est fortement dépendante d'entreprises étrangères, tant en matière de plateformes que de produits et services numériques. Face au déficit d'acteurs privés du numérique d'envergure, elle a développé une posture réactive en mettant en œuvre des dispositifs de certification de produits et services de sécurité, mais aussi certains produits « souverains » jugés particulièrement critiques en termes de sécurité nationale. L'objectif est de garantir la pleine maîtrise de la conception de ces produits.

Alix Desforges, chercheuse au sein de la chaire Castex de Cyberstratégie, « Défense et sécurité de l'espace numérique : la nécessité d'une stratégie globale et inclusive », Les Champs de Mars, 2018.

Activités

1. Présentez les missions du Comcyber (docs 1 et 2).
2. Comparez les rôles du ministère des Armées et du ministère de l'Intérieur dans le cadre de la stratégie nationale de la sécurité du numérique (doc 2).
3. Montrez que l'année 2019 constitue un tournant en matière de cyberdéfense (doc 5).
4. À partir de la description de l'affiche, identifiez la place du cyberspace dans cette série consacrée au renseignement extérieur. En quoi la fiction peut-elle contribuer à la cyberpuissance de la France (doc 4) ?
5. En quoi le document 6 peut-il expliquer la citation de la ministre des Armées : « la cybersécurité, c'est un sport collectif » ?

→ **L'enjeu géopolitique** Dans quelle mesure peut-on parler de cyberpuissance pour la France ?

► Pour approfondir

Résumez les grandes lignes de l'*Appel de Paris pour la confiance et la cybersécurité* du président Macron le 12 novembre 2018.

Vers le BAC

Rédigez un paragraphe de composition montrant que la France s'affirme comme une cyberpuissance. Conseil : pensez à toutes les dimensions de la puissance, pas seulement à la puissance militaire.