

Cyberdéfense, entre coopération européenne et souveraineté nationale

Le cas français

Confrontée à des cyberattaques de plus en plus nombreuses, la France se dote d'une politique de **cyberdéfense** qui cherche à garantir la souveraineté nationale du cyberspace français tout en s'inscrivant dans un cadre de coopération européenne.

? Comment la France se protège-t-elle contre les cybermenaces ?

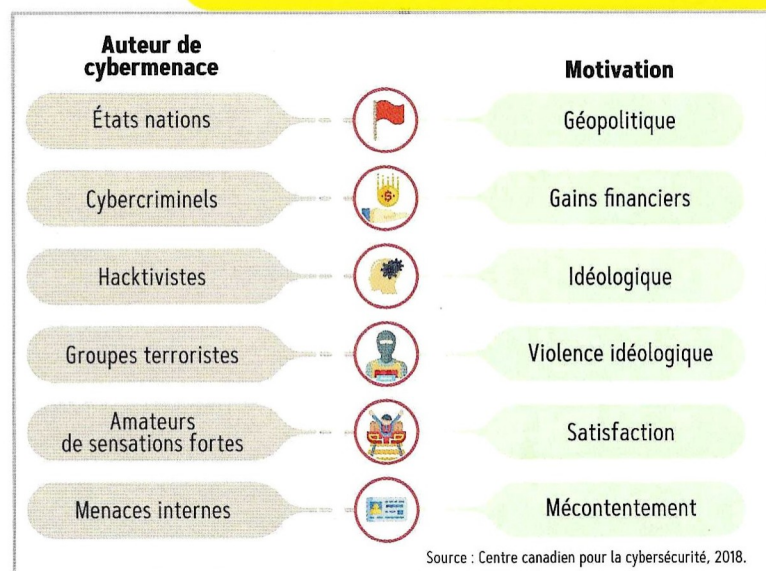


Vidéo Web

« Le "rançongiciel WannaCry porterait la signature de la Corée du Nord »

Envoyé spécial, France 2, 18 décembre 2017, 1'58.

www.lienmini.fr/hggspT-138



2 L'Union européenne et la cybersécurité

« Compte tenu de leur rôle essentiel dans nos sociétés et nos économies modernes, les ordinateurs, les téléphones portables, les banques et l'internet doivent fonctionner ensemble correctement. L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) a pour mission d'assurer un niveau élevé de sécurité des réseaux et de l'information. Elle agit de différentes façons :

- En intervenant en tant qu'expert en matière de sécurité des réseaux et de l'information auprès des autorités nationales et des institutions européennes ;
- En favorisant l'échange de meilleures pratiques ;
- En facilitant les contacts entre les institutions (nationales et européennes) et les entreprises.

L'ENISA, en collaboration avec les instances nationales et les institutions européennes, s'emploie à développer une culture de la sécurité des réseaux d'information dans toute l'Union. »

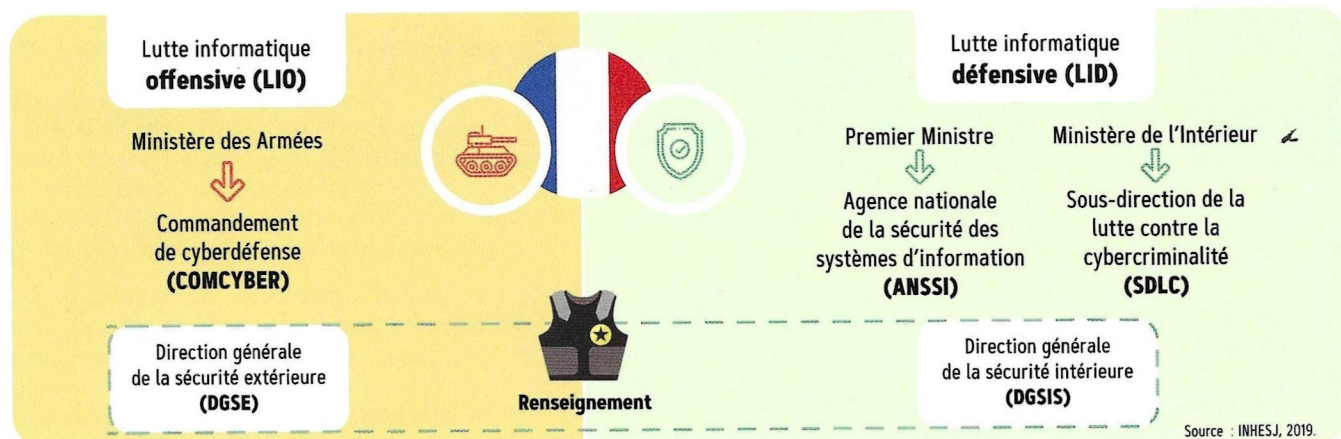
Site internet de l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), 2019.

1 Des cybermenaces multiformes

3 La doctrine militaire de lutte informatique offensive (LIO) française

	Emplois de niveau tactique	Emplois de niveau stratégique
Évaluation des capacités adverses	– Renseignement d'intérêt immédiat lié à l'action des forces	– Renseignement en préparation des opérations
Réduction voire neutralisation des capacités adverses	– Neutralisation d'un système d'arme – Neutralisation d'un poste de commandement	– Neutralisation d'une capacité opérationnelle adverse – Neutralisation d'un système de commandement de niveau stratégique
Action sur les perceptions ou la capacité d'analyse adverse	– Altération des données d'un système de commandement	– Désorganisation des centres de propagande adverses

Source : Délégation à l'information et à la communication de la défense, ministère de la Défense, janvier 2019.



4 Les principaux acteurs français de la lutte informatique

5 Le Cybersecurity Act européen

« Pleinement investie pour défendre les positions françaises lors des négociations, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) se félicite de l'adoption définitive du *Cybersecurity Act*. Paru au Journal officiel de l'Union européenne le 7 juin [2019], ce règlement marque une véritable avancée pour l'autonomie stratégique européenne. Il poursuit un double objectif : l'adoption du mandat permanent de l'ENISA, l'Agence européenne pour la cybersécurité, et la définition d'un cadre européen de certification de cybersécurité, essentiel pour renforcer la sécurité du marché unique numérique européen. »

Site internet de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), 2019.

DÉFINITIONS

Cyberdéfense : moyens mis en place par un État pour défendre dans le cyberspace les systèmes d'information jugés d'importance vitale et qui contribuent à assurer la cybersécurité.

Stratégique : le terme désigne, ici, l'ensemble des opérations menées de façon coordonnée pour produire des effets à long terme.

Tactique : le terme s'applique, ici, à des opérations ponctuelles destinées à avoir des effets immédiats.

6 Coopération et autonomie stratégique numérique européenne

« Au sein de l'Union européenne (UE), la France défend une vision ambitieuse et le concept "d'autonomie stratégique numérique de l'UE", gage de notre capacité collective d'initiative et d'action. [...] La politique extérieure de l'Union européenne doit définir des réglementations prenant en compte les exigences de compétitivité et les potentialités du numérique tout en restant protectrices des citoyens, des entreprises, des États membres, conformément à nos valeurs communes (droit à la vie privée et protection des données à caractère personnel, protection des infrastructures critiques). [...] L'Union européenne a un rôle essentiel dans la promotion et le soutien au développement des capacités de cyberdéfense des entités publiques et privées au sein des États membres ainsi que des institutions européennes elles-mêmes, en s'appuyant sur des savoir-faire européens. Elle peut également apporter son soutien dans les domaines de la formation et de l'entraînement, ce qui crée des synergies et évite les redondances de capacités. Au-delà de ces différentes dimensions, il apparaît nécessaire de renforcer la coopération opérationnelle entre les États membres de l'Union européenne. L'objectif est de disposer, à l'échelle européenne, d'outils de partage d'information technique sur les menaces, permettant d'anticiper et de répondre rapidement à une attaque informatique. La mise en place en 2017 d'un cadre pour une réponse diplomatique conjointe de l'UE face aux actes de cybermalveillance [...] s'inscrit pleinement dans cette démarche de coopération. »

Ministère de l'Europe et des Affaires étrangères, www.diplomatie.gouv.fr, mai 2019.

QUESTIONS

MISE EN RELATION DES DOCUMENTS

- À quelles cybermenaces la France est-elle confrontée ? (doc. 1 et 3)
- Quels sont les objectifs de la doctrine française de cyberdéfense ? Quels moyens sont mis en œuvre pour lutter contre les cyberattaques ? (doc. 3 et 4)
- Comment l'Union européenne renforce-t-elle la coopération entre États membres en matière de cybersécurité ? Montrez que la France s'engage dans cette démarche. (doc. 2, 5 et 6)
- Comment la France entend-elle assurer sa souveraineté numérique ? (doc. 2 à 6)

REMOBILISER
LES NOTIONS



Montrez que le renforcement par l'État du contrôle d'Internet constitue l'un des enjeux de la nouvelle économie de la connaissance. (axes 1 et 2)