BACCALAURÉAT GÉNÉRAL

ÉPREUVE D'ENSEIGNEMENT DE SPÉCIALITÉ

SESSION 2025

HISTOIRE-GÉOGRAPHIE, GÉOPOLITIQUE ET SCIENCES POLITIQUES

———

Durée de l'épreuve : **4 heures**

L'usage de la calculatrice et du dictionnaire n'est pas autorisé.

Dès que ce sujet vous est remis, assurez-vous qu'il est complet.

Ce sujet comporte 3 pages numérotées de 1/3 à 3/3.

Répartition des points

Dissertation	10 points
Étude critique	10 points

Le candidat traitera un sujet de dissertation au choix parmi les sujets 1 et 2.

Il précisera sur la copie le numéro du sujet choisi pour la dissertation.

Sujet de dissertation 1 :

Les acteurs de la conquête de l’espace et des océans.

Sujet de dissertation 2 :

Pourquoi la France préserve-t-elle son patrimoine ?

Le candidat traitera l'étude critique de document suivante.

Étude critique de document – La cyberdéfense : un enjeu pour la souveraineté nationale de la France

Consigne – En analysant le document et en vous appuyant sur vos connaissances, vous montrerez les défis auxquels les acteurs de la cyberdéfense en France sont confrontés et les réponses qu'ils y apportent pour défendre la souveraineté nationale.

Document :

Les cyberattaques en France ont été multipliées par quatre en l'espace d'un an, imposant à la France et en particulier ses militaires de « renforcer sa chaîne de cyberdéfense de bout en bout », a déclaré ce jeudi la ministre des Armées. « En seulement un an, entre 2020 et 2021, les attaques cyber ont été multipliées par quatre », a assuré Florence Parly. « S'il existe bien un espace où la malveillance ne dort jamais, pas même d'un œil, un espace où chacun d'entre nous peut devenir la cible, le vecteur, voire même l'amplificateur de sa menace, c'est bien l'espace cyber », a-t-elle ajouté en signant une convention avec le Groupement d'Intérêt Public Action contre la cybermalveillance (GIP ACYMA). « Le ministère des Armées porte l'ambition de renforcer sa chaîne de cyberdéfense de bout en bout, de l'administration centrale à la PME sous-traitante d'un grand groupe de défense », a-t-elle encore précisé.

Créé en 2017, le GIP ACYMA regroupe des acteurs étatiques impliqués dans la cyberdéfense, dont l'Agence nationale de la sécurité des systèmes d'information (ANSSI), les services des ministères de l'Intérieur, de la Justice, de l'Économie et des Armées ainsi que le secrétariat d'État en charge du Numérique et des acteurs de la société civile (associations de consommateurs, fédérations et syndicats, assureurs, etc.). La convention mettra notamment à disposition du GIP ACYMA à plein temps un officier de la Direction du renseignement et de la sécurité de défense (DRSD), l'agence de renseignement spécialisée dans la contre-ingérence[1].

Après les cyberattaques qui ont ramené deux hôpitaux au « tout papier », Emmanuel Macron a confirmé en février un plan d'un milliard d'euros pour renforcer la cybersécurité des systèmes sensibles. Florence Parly a rappelé que son ministère avait consacré 1,6 milliard d'euros à la cyberdéfense sur la période 2019-2025 en vertu de la Loi de programmation militaire, soulignant aussi le recrutement de « 1 000 cybercombattants d'ici 2025 ».

« La DRSD a observé, au second semestre 2020, une large mobilisation d'individus menant des actions cyber, offensives et propagandistes, à caractère islamiste. Ces actions ont conduit à une vague de défigurations[2] de sites web [appartenant à des] entités ou [à des] personnes physiques françaises liées à la sphère Défense », a insisté la ministre, faisant état d'attaques venant tout à la fois de puissances étatiques, de groupes terroristes et de leurs soutiens.

Source : Site du journal *Le Figaro* avec l'Agence France Presse, le 4 mars 2021.

[1] Contre-ingérence : vise à déceler les intentions adverses en identifiant et en neutralisant toute menace pouvant conduire à des actes hostiles de la part d'organisations, de groupes ou d'individus isolés.
[2] Défiguration de site web : attaque pirate entraînant un dysfonctionnement ou une paralysie du site.