BACCALAURÉAT GÉNÉRAL

ÉPREUVE D'ENSEIGNEMENT DE SPÉCIALITÉ

HISTOIRE-GÉOGRAPHIE, GÉOPOLITIQUE et SCIENCES POLITIQUES

Jour 2

SUJET

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 4 pages numérotées de 1/4 à 4/4.

Le candidat traitera un sujet de dissertation, au choix parmi les sujets 1 et 2 ET l'étude critique de document(s)

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 de sujet choisi pour la dissertation.

Dissertation 1

Comment les sociétés se sont-elles adaptées au changement climatique depuis le Moyen Âge ?

Dissertation 2

Comment le patrimoine contribue-t-il au rayonnement mondial de la France ?

Le candidat traite l'étude critique de document suivante

Étude critique de document :

Consigne :

En analysant le document et en vous appuyant sur vos connaissances, montrez que le cyberespace est un espace de conflictualités et décrivez la stratégie de cyberdéfense de la France.

Document : la France face aux dangers du cyberespace

Dans la seconde moitié des années 2010, le cyberespace n'est plus une somme anarchique d'équipements ou de systèmes informatiques, mais bien un véritable milieu complémentaire aux champs physiques traditionnels (terre, mer, air et espace). On lui prêtera deux caractéristiques principales : il est entièrement façonné par l'homme et sa structure est multicouche. […] La particularité du cyberespace est la manière dont il s'est constitué, a évolué et évolue encore. On a dit comment la philosophie de ses bâtisseurs a initialement contribué à sa nature incontrôlée. Désormais, ce sont les intérêts commerciaux des industriels qui entretiennent cet aspect : il faut développer vite, abreuver le public de nouvelles fonctionnalités, les rendre obsolètes sous peu pour vendre et vendre toujours, sans considération pour les effets secondaires. […]

De nos jours, toute la société repose sur du cyber : toujours plus de moyens connectés, d'usagers, d'utilisations… La surface d'attaque du cyberespace grandit et mute sans cesse, son exploitation par des acteurs hostiles également. Le cas du hacker isolé agissant par idéologie ou esprit de compétition est maintenant obsolète. La cyberattaque devient un composant essentiel des actions des groupes criminels ou terroristes comme de la stratégie de certains gouvernements. C'est cette structuration de la menace qui impose désormais de reconnaitre le cyberespace non plus comme un milieu à défendre uniquement, mais comme un domaine d'opérations à conquérir. […]

Historiquement et politiquement, c'est la composante cyberdéfense qui contribue à la sécurité et à la souveraineté nationale et revêt un intérêt stratégique. Dévoilée en février dernier par Emmanuel Macron, la stratégie d'accélération cyber réaffirme l'enjeu de protéger les infrastructures critiques et veut diffuser la globalisation de la cyber protection dans toute la société par la formation, le développement technologique et le renforcement des liens au sein de la filière […]. La culture de la sécurité pour protéger les processus et les informations critiques est une caractéristique forte que les militaires ont développée bien avant l'ère de la numérisation. Ainsi, lorsque la cyberdéfense devient une priorité interministérielle à la fin des années 2000, le ministère de la Défense vient renforcer l'ANSSI (1), chef d'orchestre interministériel, et le ministère de l'Intérieur, chargé de la lutte contre la cybercriminalité. Les Armées intègrent et mûrissent les concepts de sécurité des systèmes d'information pour assumer leur part de la protection de l'espace numérique souverain. En 2017, après la reconnaissance du cyberespace comme

domaine d'opérations, la composante cyber militaire se structure et le commandement de la cyberdéfense (COMCYBER) est créé. En 2019, la France se dote d'une doctrine de lutte informatique défensive et offensive, entrant ainsi dans le club des nations s'autorisant l'usage du spectre d'opérations cybernétiques (2) le plus varié […].

La coopération revêt également un aspect plus stratégique en donnant davantage de consistance à la dissuasion. La détection d'un assaillant et l'ajustement dynamique d'une cyberdéfense passe par l'échange d'informations caractéristiques d'une menace et par le partage de mesures d'atténuation. C'est surtout avec le monde civil que ce type de partenariat peut se développer : avec les collaborateurs industriels comme avec les centres gouvernementaux de veille, d'alerte et de réponses aux attaques.

Notes :
(1) ANSSI : agence nationale de la sécurité des systèmes d'information a été créée en 2009.
(2) Opérations cybernétiques : opérations de régulation des échanges d'informations sur les réseaux informatiques.

Source : Sébastien Picard, officier français spécialiste du domaine cyber, « Intégrer les opérations cyber à la guerre moderne », Conflits, revue de Géopolitique (revueconflits.com), octobre 2021