BACCALAURÉAT GÉNÉRAL

ÉPREUVE D'ENSEIGNEMENT DE SPÉCIALITÉ

SESSION 2023

HISTOIRE-GÉOGRAPHIE, GÉOPOLITIQUE et SCIENCES POLITIQUES

JOUR 2

Durée de l'épreuve : **4 heures**
Coefficient : **16**

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 5 pages numérotées de 1/5 à 5/5.

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 les numéros de sujets choisis pour la dissertation.

PREMIÈRE PARTIE

Dissertation 1 :

Le patrimoine, un objet de conflits

Dissertation 2 :

Les défis de la construction de la paix

DEUXIÈME PARTIE

Le candidat traite l'étude critique de document(s) suivante

Étude critique de document : Le contrôle du cyberespace

Consigne : En analysant les documents, en les confrontant et en vous appuyant sur vos connaissances, expliquez les objectifs et les actions des États dans le cyberespace.

DOCUMENT 1 :

« La gouvernance du cyberespace fait l'objet de multiples définitions, qui recouvrent à la fois la gouvernance de l'internet (son fonctionnement, ses protocoles, son architecture, ses noms de domaines) et une gouvernance sur l'internet (gestion des contenus, infractions, liberté d'expression). Cette gouvernance est complètement décentralisée, elle s'organise dans de multiples forums où participent toutes les parties prenantes (société civile, communauté technique, secteur privé, gouvernements). Les réseaux sont possédés et administrés pour l'essentiel par le secteur privé. Pour autant, le cyberespace n'échappe pas aux lois des États-nations et au principe de souveraineté, mais il oblige à le repenser.

Le cyberespace n'est pas un espace de non-droit. Bien au contraire, il est soumis à un enchevêtrement de juridictions et de souverainetés nationales. Les États peuvent faire appliquer leurs lois sur leur territoire et, donc, sur les infrastructures physiques, les personnes, les entreprises basées sur leur territoire mais la mise en œuvre peut s'avérer complexe. L'exercice de la souveraineté est compliqué par la possibilité d'opérer à distance — les criminels et les preuves peuvent se trouver dans un autre pays —, l'extrême volatilité des preuves, ou encore l'utilisation de plates-formes (Google, Weibo, Facebook, Twitter) basées à l'étranger, sur lesquelles l'État n'a pas d'autorité. Les procédures de coopération internationale s'avèrent souvent trop lentes pour être efficaces.

Les récentes décisions de la Cour de justice de l'Union européenne et les initiatives législatives en matière de protection des données montrent que les États européens, fortement dépendants aux plates-formes américaines, cherchent à réaffirmer leur souveraineté. Dans le contexte de la lutte anti-terroriste, de nombreux États ont mis en place des procédures d'accès, de blocage et de surveillance sur les réseaux. La Chine a développé des stratégies dynamiques de contrôle des accès et des contenus sur « son cyberespace », qu'elle considère comme un domaine de souveraineté. La Russie a même donné un nom à ce qu'elle se représente comme son Internet souverain, le « RuNet ».

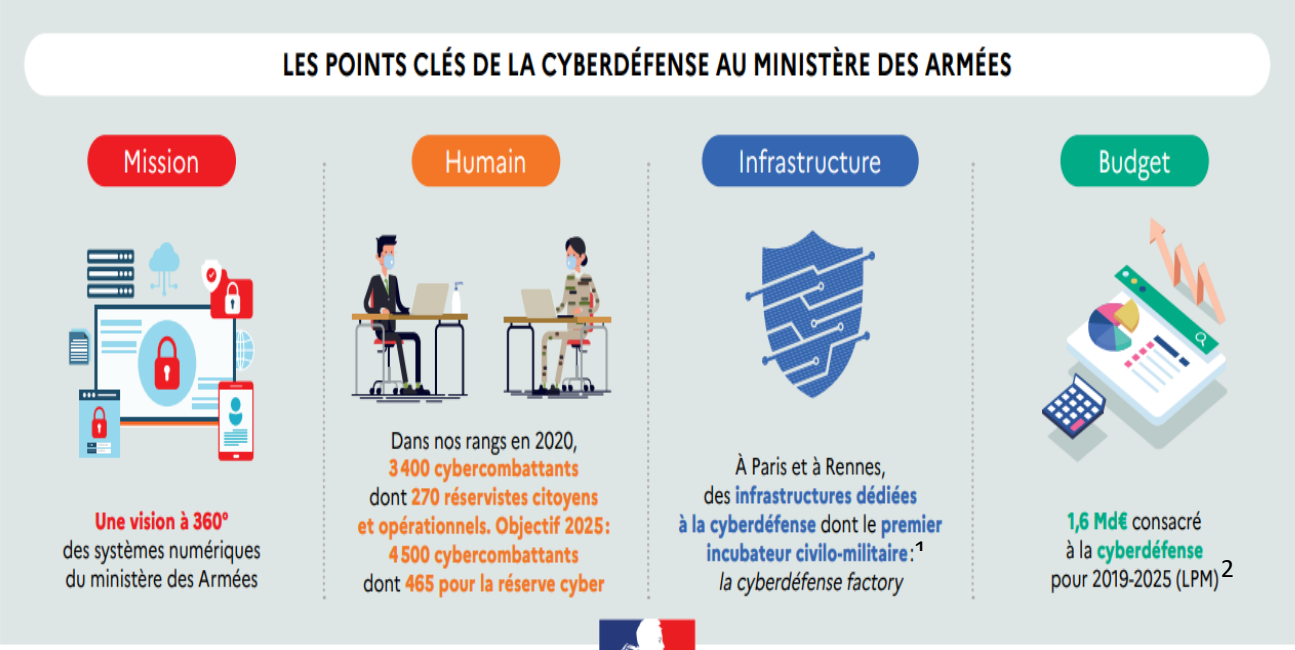
Le cyberespace est aussi soumis aux règles du droit international, même si les modalités restent encore à définir. Ce principe a été acté dans le rapport du Groupe des experts gouvernementaux de l'ONU, ainsi qu'au G20 et au G7. Des normes de

comportement responsable des États — certes non contraignantes — et des mesures de confiance ont également été adoptées par les États, pour réguler cet espace et prévenir le risque d'escalade des conflits.

Les réseaux qui constituent le cyberespace sont partagés entre une multiplicité d'acteurs, des individus, des organisations politiques, des hackers, des militants, des entreprises, des gouvernements, des terroristes, des militaires. Ils sont omniprésents dans tous les aspects de notre vie quotidienne, notre économie et nos sociétés. De ce fait, des enjeux et des risques émergent dans tous les domaines. Les nouveaux services en ligne bouleversent les équilibres économiques et menacent des secteurs entiers ; les cyberattaques sont de plus en plus nombreuses, ciblées et sophistiquées et menacent la sécurité des infrastructures vitales et des citoyens ; les entreprises peuvent voir leurs données volées, divulguées, détruites ou leurs installations sabotées à distance ; les individus sont exposés à l'exploitation de leurs données personnelles et de leur intimité par des gouvernements ou des entreprises ; les policiers et les juges font face au défi du chiffrement des communications en ligne par des terroristes et des criminels ; les militaires risquent de voir leurs capacités opérationnelles affectées par des actions de sabotage, manipulation de l'information ou d'influence ».

Source : Fredérick DOUZET, « le cyberespace, un enjeu majeur de géopolitique », site Internet, INA, la revue des médias, 1er Juillet 2016 [en ligne consulté le 22/09/2022].

DOCUMENT 2 :



Notes :

[1] Incubateur civilo-militaire : lieu réunissant des acteurs de l'innovation (des militaires, des universitaires, des start-up et des PME).

[2] LPM : loi de programmation militaire

Source : Ministère des Armées, site Internet [en ligne consulté le 22/09/2022].