Corrigé et barème – Objet conclusif : le cyberespace, conflictualité et coopération entre les acteurs

Le cyberespace entre réseaux et territoires (couches, infrastructures, acteurs, liberté ou contrôle des données), ses conflits (espionnage, sabotage, déstabilisation, crime, guerre hybride, attribution), les coopérations de l'ONU à l'OTAN et à l'Union européenne, et la cyberdéfense française.

Durée : 240 min – Calculatrice interdite – Sur 20 points · Spe-hggsp Terminale

Exercice 1 – Dissertation ★★★ *(10 pts)*

a) Un État souverain n'est soumis à aucun pouvoir extérieur et fait respecter ses lois sur son territoire. Le cyberespace est l'espace formé par l'interconnexion mondiale des équipements numériques, avec trois couches (physique, logique, informationnelle). Période : de l'ouverture d'Internet au public (années 1990) à aujourd'hui, surtout depuis les attaques contre l'Estonie (2007). Problématique : alors que le cyberespace semble ignorer les frontières, comment les États y reconstruisent-ils leur souveraineté, et pourquoi celle-ci reste-t-elle partielle et inégale ? (2)

b) I. Les États reprennent prise sur le cyberespace. 1) Des infrastructures localisées, soumises à leurs lois : centres de données, points d'atterrissement des câbles ; le *Cloud Act* (2018) étend même le droit américain hors des frontières. 2) Des frontières numériques : Grand pare-feu chinois, loi russe sur l'Internet souverain (2019), 296 coupures d'Internet dans 54 pays en 2024. 3) Le cyberespace comme arme : Stuxnet contre Natanz (2010), intrusion SolarWinds attribuée au SVR (2021), attaque contre Viasat le 24 février 2022. (2)

c) II. Une souveraineté limitée et contestée. 1) Des firmes plus puissantes que bien des États : GAFAM et BATX ; les révélations de 2013 (PRISM) montrent que le renseignement passe par elles ; un opérateur privé de satellites devient indispensable à l'armée ukrainienne. 2) Des attaques sans frontières et sans auteur certain : WannaCry dans environ 150 pays (2017), fausse bannière de l'attaque contre TV5Monde (2015). 3) Des règles mondiales faibles et concurrentes : normes non contraignantes des experts de l'ONU (2015), Appel de Paris sans la Chine ni la Russie (2018), convention de l'ONU née d'une initiative russe (2024) face à celle de Budapest (2001). (2)

d) III. La France, une souveraineté partagée. 1) Un modèle national complet : Livre blanc (2008), ANSSI (2009), opérateurs d'importance vitale (2013), COMCYBER (2017), doctrine offensive (2019), Viginum (2021), attribution au GRU (2025). 2) L'Europe, multiplicateur de souveraineté : RGPD (2018), arrêts Schrems (2015, 2020), directives NIS (2016, 2022), sanctions (2020). 3) Des limites : dépendance aux hébergeurs américains (qualification SecNumCloud), attribution tardive. Conclusion : les États peuvent être souverains dans le cyberespace, mais seulement en partie, inégalement selon leur puissance, et souvent en partageant cette souveraineté avec des alliés. (2)

e) Accroche : le 24 février 2022, une heure avant l'invasion de l'Ukraine, une cyberattaque met hors service les modems du réseau satellitaire Viasat utilisés en Ukraine ; elle sera attribuée à la Russie. Puis les définitions, la période, la problématique et l'annonce du plan : des États qui reprennent prise sur le cyberespace ; une souveraineté limitée par les firmes, les attaques et la faiblesse des règles ; le cas français d'une souveraineté partagée. (2)

Erreur fréquente — opposer simplement des démocraties « libres » à des régimes « qui contrôlent », ou réciter une liste de cyberattaques : il faut montrer qui exerce le pouvoir dans le cyberespace (États, firmes, alliances) et avec quelles limites, en datant chaque exemple.

Exercice 2 – Étude critique de document ★★★ *(10 pts)*

a) Déclaration politique internationale, présentée sous forme résumée, lancée par le président Emmanuel Macron le 12 novembre 2018 à l'UNESCO, lors du Forum sur la gouvernance de l'Internet réuni à Paris. Ce n'est pas un traité : il ne crée aucune obligation juridique. Contexte : l'année 2017 a montré la dangerosité du cyberespace (WannaCry en mai, NotPetya en juin, divulgation de courriels de l'équipe de campagne d'Emmanuel Macron en mai), et le groupe d'experts de l'ONU n'a pu s'accorder en 2017. (2)

b) L'Appel est ouvert aux États mais aussi aux entreprises, aux collectivités et aux ONG : c'est une coopération multi-acteurs, qui reconnaît que l'infrastructure du cyberespace appartient largement à des acteurs privés. Microsoft, qui plaidait depuis 2017 pour des règles protégeant les civils, figure parmi les soutiens. Le texte s'appuie pourtant sur le droit international existant (Charte des Nations unies) et sur des normes de comportement, dans la ligne du rapport des experts de l'ONU de 2015. (2)

c) La défense des processus électoraux (principe 3) renvoie aux ingérences de 2016-2017 ; le vol de propriété intellectuelle (principe 4) prolonge le pillage technologique révélé par l'affaire Farewell (1981-1982) ; la lutte contre la prolifération des outils malveillants (principe 5) rappelle que WannaCry réutilisait une faille découverte par la NSA ; la protection du « cœur public » de l'Internet (principe 2) vise les infrastructures dont tout dépend. Le principe 8, qui interdit aux acteurs privés leurs propres cyberactions offensives, réaffirme le monopole des États sur la riposte. (2)

d) Deux visions s'opposent. La Chine et la Russie défendent une souveraineté informationnelle : dès 2011, avec d'autres membres de l'Organisation de coopération de Shanghai, elles proposent à l'ONU un code de conduite centré sur le contrôle des contenus par les États ; la Russie adopte en 2019 sa loi sur l'Internet souverain. Un texte qui associe entreprises et ONG et défend un Internet ouvert leur est étranger. Les États-Unis, première cyberpuissance, refusent en 2018 toute contrainte qui pourrait limiter leurs capacités ; ils ne rejoignent l'Appel qu'en novembre 2021, sous l'administration Biden. (2)

e) Portée d'abord symbolique : ni contrôle ni sanction, et les États les plus actifs dans les cyberopérations n'avaient pas signé au départ. C'est aussi un instrument d'influence : la France se pose en médiatrice entre le modèle américain des firmes et le modèle sino-russe du contrôle. Mais elle ne renonce pas à la puissance : COMCYBER (2017), doctrine de lutte informatique offensive (janvier 2019), attribution publique d'attaques au GRU (2025) ; il n'y a pas contradiction, car l'Appel vise d'abord la protection des civils et les acteurs non étatiques. Limite : en décembre 2024, c'est une convention de l'ONU née d'une initiative russe, plus centrée sur les États, qui est adoptée. Conclusion : l'Appel montre le besoin d'une coopération multi-acteurs, mais aussi qu'elle reste fragile tant que les grandes puissances défendent des visions opposées du cyberespace ; c'est un acte diplomatique autant qu'un engagement. (2)

Méthode — un texte non contraignant se juge par ses signataires, ses absents et les actes de son auteur : relever qui signe et qui manque, puis confronter les principes à ce que fait la France elle-même.

Ce document est la propriété intellectuelle de Ben, professeur particulier (benprofparticulier.fr), protégée par le Code de la propriété intellectuelle (art. L. 111-1 et L. 122-4). Il est mis à disposition pour un usage personnel de révision. Toute reproduction, diffusion, mise en ligne ou revente, totale ou partielle, sans autorisation écrite est interdite et constitue une contrefaçon (art. L. 335-2).