GOUVERNEMENT
Liberté
Égalité
Fraternité

Terminale

Enseignement de spécialité : Histoire, Géographie, Géopolitique, Sciences Politiques

Thème 6 – L'enjeu de la connaissance

NB : Les documents en rouge sont téléchargeables en accompagnement dans le dossier *Documents HGGSP Terminale Thème 6*

Chapitre : La connaissance, enjeu politique et géopolitique

La littérature sur l'espionnage est multiple, selon qu'on aborde le sujet par le prisme de la fiction ou des acteurs (les espions). Un pan entier de la recherche scientifique aborde la problématique du renseignement au travers des « *Intelligence studies* ». Un premier travail tient à la définition de ce qu'est le renseignement, comment il fonctionne :

- Hugues Moutouh, Jérôme Poirot, *Dictionnaire du renseignement.* Perrin, « Hors collection », 2018, 848 pages (https://www.cairn.info/dictionnaire-du-renseignement--9782262070564.htm)
- Voir aussi le Hors-série de *Hermès, la Revue* : Le renseignement, un monde fermé dans une société ouverte, 2016/3 (n° 76)

En France, une école dynamique s'est développée, qui réfléchit spécifiquement à la culture du renseignement, sa formation, et les structures associées :

- Olivier Forcade, « Actualité scientifique du renseignement », *Stratégique*, 2014/1 (N° 105), p. 15-21. (https://www.cairn-int.info/revue-strategique-2014-1-page-15.htm)
- Olivier Chopin, Bastien Irondelle, Amélie Malissard, « Étudier le renseignement en France », *Hérodote*, 2011/1 (n° 140), p. 91-102 (https://www.cairn-int.info/revue-herodote-2011-1-page-91.htm)

Cette question du renseignement de façon générale est d'autant plus d'actualité quand il s'agit d'enjeux liés à la lutte contre le terrorisme et fait la part belle aux coopérations internationales :

- Olivier Passot, « Renseignement français et lutte contre le terrorisme. Évolutions récentes et perspectives », *Les Champs de Mars*, 2018/2 (N° 31), p. 63-71 (https://www.cairn-int.info/revue-les-champs-de-mars-2018-2-page-63.htm)

- Benjamin Oudet, « Les coopérations internationales de renseignement et la politique étrangère française en Afrique au XXI[e] siècle », *Les Champs de Mars*, 2019/1 (N° 32), p. 181-185 (https://www.cairn-int.info/revue-les-champs-de-mars-2019-1-page-181.htm)

Sur les lanceurs d'alerte, ceux qui révèlent les failles ou les dysfonctionnements dans les systèmes étatique, économique, politique ou financier. Ces signalements confrontent deux valeurs fondamentales des démocraties modernes, le secret et la transparence : *Carnet du temps* numéro 131, p.36-37.

D'un point de vue militaire, le renseignement est aussi une pratique essentielle pour les opérations dans tous les milieux :
« Renseigner pour opérer », *Air Actualités*, hors-série, 2015, pp. 12-15.
Que ce soit en temps de paix ou en temps de guerre, le renseignement est un enjeu vital pour les armées. Les apports technologiques de l'imagerie et du *big data* permettent d'anticiper les menaces extérieures mais aussi les déploiements, en toute légalité, des armées françaises. Le développement de l'intelligence artificielle permettra aussi une meilleure analyse des risques.

Encart : Le renseignement au service des États : les services secrets soviétiques et américains durant la guerre froide

Le monde de l'espionnage et du renseignement fascine et donne régulièrement à voir des expositions comme Espion(s) à la Cité des Sciences et de l'Industrie (http://www.cite-sciences.fr/fr/au-programme/expos-temporaires/espions/lexposition/) ou l'exposition *Guerres secrètes* au Musée de l'Armée :

- Christophe Bertrand, David Guillet, Carine Lachèvre, François Lagrange, Emmanuel Ranvoisy (dir.), *Guerres secrète*s, musée de l'Armée/Somogy éditions d'art, 2016.

Sur la période de la Guerre froide et les enjeux associés, on consultera avec profit certains des articles suivants sur l'URSS et les États-Unis :

- Françoise Thom, « Staline et le renseignement », *Stratégique*, 2014/1 (N° 105), p. 89-104. (https://www.cairn-int.info/revue-strategique-2014-1-page-89.htm)
- Andreï Kozovoï, *Les Services secrets russes. Des tsars à Poutine.* Tallandier, « Texto », 2020, 604 pages (https://www.cairn.info/les-services-secrets-russes--9791021042674.htm)
- Philippe Silberzahn, Milo Jones, « L'identité et la culture organisationnelle comme sources de la surprise stratégique : Les leçons des échecs de la CIA », *Annales des Mines - Gérer et comprendre*, 2014/2 (N° 116), p. 70-80 (https://www.cairn-int.info/revue-gerer-et-comprendre1-2014-2-page-70.htm)
- Gildas Le Voguer, « Le « complexe industriel » du renseignement américain et la préservation des libertés », *Politique américaine*, 2014/2 (N° 24), p. 29-44 (https://www.cairn-int.info/revue-politique-americaine-2014-2-page-29.htm)

Les séries se sont aussi mises de la partie pour rappeler l'ambiance de cette guerre secrète. On citera deux exemples : The Americans, l'histoire d'un couple d'agents dormants infiltrés aux USA sous la présidence Reagan, et La Compagnie (une adaptation du livre éponyme de Robert Littell)

Chapitre : Le cyberespace : conflictualité et coopération entre les acteurs

François-Bernard Huyghe : « Une cyberstratégie à inventer » *Penser les Ailes françaises* n°32, juillet 2015, p.11-18
Tous les grands types d'acteurs, Etats, organisations, groupes activistes et individus, ont investi le cyberespace avec une énergie et une inventivité croissantes. La nécessité d'une cyberstratégie s'impose dans tous les Etats et cet enjeu soulève de nombreuses questions notamment d'un point de vue de la législation et des partenariats publics-privés.

Encart : La Chine, la technologie au service de la puissance

« L'Internet chinois : outil de contrôle social » *Carnet du temps*, HS Chine, p.60
L'Internet chinois se compose de quatre grandes firmes nationales : Baidu, Alibaba, Tencent et Xiaomi (BATX). Il est aujourd'hui considéré comme l'équivalent asiatique de l'Internet occidental, les GAFAM, composés de Google, Amazon, Facebook, Apple et Microsoft. Au-delà de l'intérêt économique, il joue un rôle dans le control social. A rapprocher de cet article sur « l'omnicontrôle » et le numérique comme instrument de répression.

Note du CERPA n°92, « Quelle structuration de la cyberdéfense en République Populaire de Chine ? », 2016
L'observation par la République Populaire de Chine (RPC) de l'opération *Desert Storm* en 1991 fut le point de départ d'un renouveau doctrinal dans l'Armée populaire de libération (APL). En effet, c'est à l'occasion de la première guerre du Golfe que les États-Unis ont démontré leur capacité de mener une guerre électronique en rompant les communications de l'armée irakienne. Les Chinois ont ainsi pu mesurer leur retard dans ces techniques et sont parvenus à se hisser en quelques années au rang de cyberpuissance.

Voir aussi les articles qui accusent la Chine d'actions utilisant les nouvelles technologies pour assurer leur supériorité technologique (https://www.lefigaro.fr/international/cyberattaques-desinformation-surveillance-industrielle-la-grande-offensive-des-espions-chinois-20200717) ou pour réprimer les mouvements ouvertement hostiles comme à Hong Kong (https://cyberguerre.numerama.com/1703-comment-les-cyberattaques-et-la-desinformation-ont-tente-de-juguler-les-manifestations-de-hong-kong.html)

Encart : exemples de stratégies cyber en comparaison

Note du CERPA n°53, « Estonie, une stratégie de cyberdéfense », 2016
En 2007, l'Estonie est victime d'une cyberattaque de grande ampleur. La vigueur de cette dernière est telle que seul un État peut en être à l'origine. Le voisin russe est alors fortement soupçonné. Depuis, de nombreuses mesures ont été prises pour éviter ce genre de crise. Grâce à sa population hyper-connectée et à une coopération renforcée avec les organisations internationales (OI), l'Estonie est devenue un acteur majeur de la cyberdéfense.

Note du CERPA n° 75, « Industrie de la cyberdéfense israélienne », 2016
Dès le milieu des années 1990, les autorités israéliennes se sont emparées de la problématique cyber pour la placer au centre de leur réflexion stratégique. Les efforts pour développer la cyberdéfense se

sont d'abord focalisés sur le domaine militaire tandis que les risques encourus par les systèmes d'information civils étaient peu pris en compte. Depuis, un tissu industriel de cybersécurité s'est développé et a noué des liens privilégiés avec les pouvoirs publics, ce qui place Israël au rang des leaders mondiaux de la cyberdéfense.

Note du CERPA n°198, « La nouvelle stratégie cyber des États-Unis », 2019
Depuis 2018, la stratégie cyber des États-Unis se veut plus offensive. La posture cyber actuelle se lit au prisme de plusieurs textes publiés en 2018 : le *White House National Cyber Strategy*, *l'Unclassified Summary Department of Defense Cyber Strategy* et le *Department of Homeland Security Cyber Security Strategy*. Le cyber s'érige de plus en plus comme la cinquième dimension des affaires militaires, comme le démontre la nette croissance du budget alloué à ce domaine.

Encart : Les armées et la cyberdéfense

En 2020, le chef d'état-major de l'armée de Terre (CEMAT), le général Burkhard, livre sa vision stratégique, et expose ses pensées sur les conflits à venir. Tout en rappelant que l'armée de Terre se prépare à affronter un « *ennemi symétrique* » dans le cadre d'une guerre de haute intensité, il souligne le fait que la « *guerre investit de nouveaux espaces en particulier immatériels* », dont la « *cyberguerre* », ainsi que la « *manipulation des opinions* ». En effet, le monde d'aujourd'hui voit réapparaître des logiques de puissances prétendant exercer – ou continuer d'exercer – une influence à l'échelle régionale et/ou planétaire. L'influence de l'opinion, la démoralisation de l'« arrière », la manipulation des informations et la désinformation (en particulier ce que l'on nomme aujourd'hui les *fake news*), l'encouragement aux divisions sociétales internes, etc., n'ont rien de nouveau. Mais l'outil internet conduit à l'ouverture d'un champ immatériel de la guerre tout aussi crucial que le champ matériel plus classique, dans un temps immédiat, sur de très larges espaces, auprès de millions d'utilisateurs.

L'adaptation des outils militaires se fait à la fois par armées, mais aussi de façon transverse, en développant des compétences propres et des savoirs-faire particuliers.
https://www.chaire-cyber.fr/-Les-publications-
- Aude Géry, « La stratégie française de cyberdéfense », *Brennus 4.0*, 27 mars 2020 (https://www.penseemiliterre.fr/plugins/cdec/pdf/to_pdf.php?entry=114299)
- Colonel Jean-Michel Fouquet, « Cyber, cyber... Vous avez dit cyber ? », *Brennus 4.0*, 15 mars 2020 https://www.penseemiliterre.fr/plugins/cdec/pdf/to_pdf.php?entry=114293
- Lieutenant-colonel Le Dez, « La cyberdéfense est d'abord un combat », *Brennus 4.0*, CDEC, 2020, URL : (https://www.penseemiliterre.fr/la-cyberdefense-est-d-abord-un-combat_114297_1013077.html)
- Jean-François Caverne, « La conquête des ressources humaines en cyberdéfense », *Brennus 4.0*, 25 mars 2020 (https://www.penseemiliterre.fr/la-conquete-des-ressources-humaines-en-cyberdefense_114298_1013077.html)
- « Regard sur la cyberdéfense », *Air Actualités*, 710, avril 2018, p.46-51
Regard sur les experts de la cyberdéfense dans l'armée de l'air.
- « Renseigner au futur, renseignement militaire et technologique », in *Air actualités*, 709, mars 2018, p.36-47

La complexification des champs de bataille et l'afflux important de données sont un défi majeur pour les acteurs air du renseignement militaire. L'emploi des capteurs dans la troisième dimension a évolué et permis d'élargir les méthodes de recherche des données.

Pour aller plus loin

Adjudant Valérie Grillet : « Galileo, Glonass, Beidou : vers une indépendance accrue envers le GPS » *Carnet du temps*, n°123, p. 52-53
Le système de guidage par radionavigation via les satellites a son utilité dans une multitude de secteurs autre que celui des transports. L'accroissement des besoins en la matière et l'exigence d'une couverture étendue à l'ensemble du globe ne peuvent être satisfaits par un système unique. Ainsi les quatre structures existantes sont complémentaires mais offrent aussi d'autres avantages aux nations qui les ont développées.

« Règlement général sur la protection des données : un outil de protection des citoyens, pas de souveraineté » *Carnet du temps*, n°135, p.18
Le règlement général sur la protection des données (RGPD) place la protection des données du citoyen au cœur de sa démarche, introduisant une dimension extraterritoriale qui contraint l'ensemble des acteurs, y compris extra-européens, à s'y conformer. Il reste cependant sans réponse face à la réplique américaine que constitue le *Cloud Act*.

« Les pirates modernes » *Carnet du temps*, n°131, p.34
Depuis les années 2000, les systèmes informatiques se développent dans divers secteurs de notre société. Ils participent au fonctionnement de l'économie et à la vie quotidienne. Cependant, des programmes pirates mis au point par des hackers s'insinuent désormais dans la vie des citoyens et peuvent aller jusqu'à la paralysie d'un pays.

« Les enjeux de cyber sécurité pour le secteur aérospatial », *Penser les Ailes françaises* n°37, 2018, p.113-128
Les enjeux de cyber sécurité constitue une problématique aussi bien pour l'aéronautique civile que militaire. Face à l'ampleur du défi, des synergies se mettent en place entre industriels et institutionnels.

Note du CERPA n° 79, « Les enjeux de l'hyperconnectivité pour la défense », 2016
L'ère digitale sera l'ère du *Big Data*. L'hyperconnectivité a pour principale conséquence un accroissement exponentiel des métadonnées produites par nos sociétés. Parvenir à traiter, à fusionner, à croiser, à stocker et à protéger cette immense quantité de données constitue l'enjeu principal du *data analysis*.

Note du CERPA n°101, « Les enjeux de cyberdéfense pour les objets connectés », 2016
Le numérique a révolutionné une part importante de notre vie quotidienne. De plus en plus de supports que nous exploitons dépendent aujourd'hui de l'informatique et d'Internet. Cependant, les systèmes innovants, comme les objets connectés, manquent souvent de maturité en matière de sécurité. Une faille que savent exploiter les hackers pour pénétrer les systèmes que nous utilisons.

Note du CERPA n°102, « Enseigner à l'ère numérique », 2016

Si l’avènement du numérique est synonyme pour certains d’une révolution des finalités de l’école, ce bouleversement concerne en réalité davantage les outils de transmission du savoir. Dans ce contexte, le collège des Bernardins a proposé, lors d’un colloque le 6 octobre 2016, quelques axes de réflexion sur l’influence du numérique à l’école