La cyberdéfense. Politique de l’espace numérique

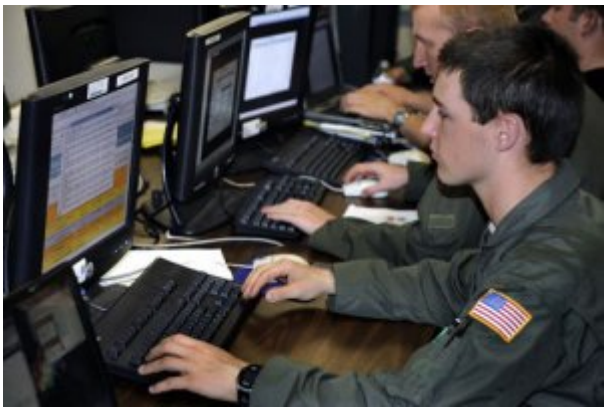
mercredi 16 janvier 2019, par Florent PARMENTIER

Voici un ouvrage qui présente la cyberdéfense sur le plan technique en mettant en lumière des stratégies et des représentations, des interactions d’acteurs, des réalisations et des pratiques. Présentation de l’ouvrage dirigé par Stéphane Taillat, Amaël Cattaruzza, Didier Danet, « La cyberdéfense. Politique de l’espace numérique », Paris, Armand Colin. En écho au nouveau programme de 1ère spécialité Histoire-Géographie et Géopolitique, cette présentation permet de nourrir le thème 4 et son axe 1 pour l’extension du réseau Internet.

LE PIRE adversaire de la connaissance n’est pas l‘ignorance, mais le fait de croire savoir, disait le physicien Stephen Hawkins. Nous ne saurions mieux dire concernant le cyberespace, qui apparaît bien comme un espace d’expression du pouvoir et de la force, de tension entre différentes identités, mais que l’on pense parfois neutre sur le plan technique. Nous savons qu’il existe, mais on descend rarement à un niveau de détail adéquat pour en comprendre les ramifications.

C’est bien l’objet de cet ouvrage collectif, qui aborde la cyberdéfense sur le plan technique en mettant en lumière des stratégies et des représentations, des interactions d’acteurs, des réalisations et de pratiques, en dehors du déterminisme technologique. Il est intéressant de noter à cet égard qu’il existe plusieurs définitions du cyberespace, dont un certain nombre font l’impasse sur la dimension humaine et politique de celui-ci. Environnement, domaine, milieu ou moyen, chaque acteur produit sa propre définition de ce champ. Le cyberespace ne peut pas être considéré « comme un bloc homogène et uniforme, mais il faut plutôt le voir comme une multitude de cyberespaces : chaque acteur, chaque usager construit son « espace » en fonction de son utilisation, de ses représentations, de ses intérêts » (p.8). Nous ne serons ainsi pas surpris de retrouver des notions de dissuasion et de coercition déjà présentes pendant la Guerre froide.

On a assisté progressivement à une sécuritisation du cyberespace, c’est-à-dire à la prise en compte d’une dimension de sécurité à laquelle on prêtait moins d’importance dans les discours et les pratiques par le passé. La cyberdéfense désigne une certaine conception de l’action sur, dans et à travers les réseaux numériques et les activités qu’ils soutiennent (p.11), ou « l’ensemble des activités conduites afin d’intervenir militairement ou non dans le cyberespace pour garantir l’effectivité de l’action des forces armées, la réalisation de mission confiées et le bon fonctionnement du Ministère » (p.45). Ce champ connaît une autonomisation croissante, même si ses discours et ses représentations technoscientifiques restent liés aux autres champs de la conflictualité. Pour aborder la cyberdéfense le plus largement possible, l’ouvrage se compose de trois grandes parties : l’étude du contexte global de la cyberdéfense, les enjeux du domaine numérique ainsi que l’espace numérique comme domaine opérationnel.



Le cyberespace est un espace géopolitique

A première vue, la dématérialisation engendrée par le numérique contrevient à notre idée classique de géopolitique, classiquement définie comme une rivalité de puissances sur un territoire donné (Yves Lacoste) : si internet est partout, et que les infrastructures sont des artefacts techniques, n'est-ce pas poser la mauvaise question ? On pourrait certes objecter, comme le fait Guillaume Pitron, que le monde numérique qui se dessine est fortement consommateur d'énergie, et participe donc pleinement à des jeux économiques au-delà de ce qui existe en ligne. [1]

Les géographes et géopoliticiens ont abordé le cyberespace sous plusieurs angles, avec un corpus riche de plusieurs approches : la géographie du numérique, les géographies produites par le numérique, et les géographies produites via le numérique. Entre géographie et numérique, les individus, les Etats et la gouvernance mondiale sont les échelles pertinentes. Le cyberespace peut également se diviser en différentes couches, à la manière des géologues : la couche matérielle (les périphériques d'accès et les infrastructures nécessaires), la couche logicielle (les logiciels et protocoles permettant la circulation de grandes quantités de données) et enfin la couche sémantique – ou cognitive (contenu informationnel). Ces différentes couches font l'objet de rapports de force spécifiques, à tel point qu'on peut affirmer que la cyberdéfense n'est pas exempte de facteurs spatiaux particuliers.

Ces rapports de force se manifestent à notamment à l'occasion de crises, opposant dans les représentations courantes les Etats-Unis et les Européens face aux Russes et aux Chinois. Elles jalonnent les dernières années à travers le globe : la cyberattaque de 2007 en Estonie, attaques contre la Géorgie en 2008, le virus Stuxnet contre l'Iran (2010), les révélations d'Edward Snowden de l'été 2013, les élections présidentielles américaines de 2016 et françaises en 2017… La question de la prise de décision sous contrainte reste essentielle en la matière, comme l'illustre le parallèle avec la crise de Cuba. L'absence de régime partagé de régulation de ces enjeux, la force relative des acteurs non-étatiques et l'incitation à l'action offensive. En dehors des crises, la non-neutralité du code ou des flux de données apparaissent également avec une force d'évidence, tout comme l'importance du facteur humain – les biais cognitifs faisant pleinement partie des éléments à considérer dans l'analyse. [2]

Prospective du cyberespace

Par la diversité des approches proposées, de l'étude de la technologie jusqu'aux aspects juridiques et stratégiques, l'ouvrage aborde également la dimension prospective du cyberespace, dans la limite de la difficulté de l'exercice dans un secteur où le rythme de développement est extrêmement rapide. Par ailleurs, trois questions semblent importantes : la souveraineté numérique (avec l'enjeu des *clouds* souverains), la technologie et la sécurité (le Big data et le renseignement, selon les différentes étapes : l'expression du besoin, la collecte, le traitement et l'exploitation, l'analyse, la diffusion et la sécurité), et la politique internationale.

La « course technologique » à l'intelligence artificielle apparaît ainsi parmi les enjeux les plus importants, la Chine ayant élaboré le plan « Ambition 2030 », dont l'objectif annoncé est de viser un leadership mondial à cette date. Les moyens économiques, la collecte des données peu respectueuse des libertés individuelles et la vision font de la Chine un candidat crédible à une place de premier choix. L'un des co-auteurs, Julien Nocetti, l'affirme d'ailleurs très directement : « L'Europe, qui n'a guère mené de réflexion prospective à ce sujet, devra pourtant s'interroger sur les conséquences économiques et stratégiques qu'aura pour elle une IA maîtrisée par le duopole sino-américain » (p.109). Les Etats-Unis suivent évidemment avec une attention toute particulière cette question, à même de redistribuer les cartes au niveau international, et ce d'autant que Washington a considéré depuis le début des années 2010 que le cyberespace constitue le « 5e champ de bataille ». A ces deux puissances s'ajoute la Russie, qui a su développer un discours du cyberespace centré autour de la souveraineté numérique, ce pays apparaissant comme une véritable « exception numérique » (à travers le « *Runet* ») ; comme le souligne Kevin Limonier : « Grâce à son écosystème spécifique, la Russie a en effet les moyens techniques, politiques et économiques d'apparaître comme une « puissance souveraine » du cyberespace, ce qui n'est d'ailleurs pas sans faire écho à la situation de l'Union européenne que certains qualifient d'ailleurs de véritable « colonie numérique » des Etats-Unis » (p. 124).

La conclusion de l'ouvrage tente d'ébaucher les perspectives de l'espace numérique à horizon 2040. De 500 000 personnes en 1995, le nombre de connectés atteint aujourd'hui plus de la moitié de la population mondiale. Le phénomène a donc depuis longtemps quitté les rives technologiques pour devenir un véritable enjeu de société. Dans un contexte propice aux innovations de rupture, trois innovations de ce type sont en cours, offrant potentiellement des convergences technologiques disruptives : le développement de l'imprimante 3D, de l'intelligence artificielle et de la blockchain. [3] Si la reprise de certains épisodes de la série *Black Mirror* permet de mettre les choses en perspective, on peut regretter, à cet égard, que la possibilité d'un rapprochement entre l'infotech et les biotechnologies ne soit pas évoquée. De même, l'ouvrage aurait pu être enrichi de quelques illustrations sur les enjeux techniques, qu'il est toujours compliqué de retranscrire. Le défi consistant à faire toucher du doigt la complexité des enjeux multiformes du cyberespace, au-delà de l'écume du traitement médiatique quotidien, semble toutefois totalement réussi.

Stéphane Taillat, Amaël Cattaruzza, Didier Danet (dir.), « *La cyberdéfense. Politique de l'espace numérique* », Paris, Armand Colin, 2018. Sur Amazon

4e de couverture

Rapports de forces, cyberattaques sur les infrastructures, hacking, espionnage, fake news, le cyberespace est devenu en quelques décennies un champ privilégié des relations internationales où coopèrent et s'affrontent anciens et nouveaux acteurs de la conflictualité, étatiques et non étatiques, publics et privés, civils et militaires.
Les enjeux sont considérables car la plupart des activités humaines dépendent aujourd'hui de l'interconnexion des systèmes de traitement de l'information permise par les réseaux numériques. Or, les menaces associées à la digitalisation de la société ont profondément transformé la manière de concevoir les conflits contemporains. Elles ont amené les États et les principaux acteurs de la sécurité à repenser leurs politiques, leurs architectures et leurs stratégies de défense sur la scène internationale.
Ce domaine doit être appréhendé de manière globale, au croisement des approches politiques et géopolitiques, stratégiques et juridiques, économiques, techniques et sociotechniques. Cet ouvrage présente de manière concise et accessible l'ensemble des connaissances disponibles aujourd'hui sur le sujet de la cyberdéfense et de la gestion de crise dans l'espace numérique. Rédigé par de nombreux spécialistes, universitaires et praticiens, il offre une vision large et pluridisciplinaire des enjeux de la

cyberconflictualité.

Voir Stéphane Taillat, Amaël Cattaruzza, Didier Danet (dir.), « *La cyberdéfense. Politique de l'espace numérique* », Paris, Armand Colin, 2018. Sur Amazon

---

P.-S.

Florent Parmentier, docteur en Science politique, est enseignant et responsable de programmes au Master Affaires Publiques à l'Institut d'études politiques de Paris.

Notes

[1] Guillaume Pitron, La guerre des métaux rares. La Face cachée de la transition énergétique et numérique, Paris, Les liens qui libèrent, 2018.

[2] A ce sujet, voir Vincent Berthet, L'erreur est humaine. Aux frontières de la rationalité, Paris, CNRS Editions, 2018.

[3] Sur cette dernière technologie, voir : Martin Della Chiesa, François Hiault, Clément Téqui, Blockchain. Vers de nouvelles chaînes de valeur, Paris, Prospectives Accuracy, 2018.