Stéphane Taillat

LA CYBERGUERRE

Que sais-je?

À lire également en
Que sais-je ?

COLLECTION FONDÉE PAR PAUL ANGOULVENT

Bruno Tertrais, *La Guerre*, n° 3866.
Nicolas Arpagian, *La Cybersécurité*, n° 3891.
Frédéric Encel, *Les 100 mots de la guerre*, n° 4192.
Catherine Blaya, *La Cyberviolence*, n° 4302.
Jérôme Pellistrandi, *Les Armées françaises*, n° 4331.

ISBN 978-2-7154-3216-1
ISSN 0768-0066

Dépôt légal – 1re édition : 2026, avril

170 *bis*, boulevard du Montparnasse, 75014 Paris

INTRODUCTION

Qu'est-ce que la « cyberguerre » ?

Dans un article de 1993, John Arquilla et David Ronfeldt annonçaient l'émergence de deux dimensions de conflits : la « cyberguerre » (*cyberwar*), caractérisée par la lutte pour la maîtrise de l'information sur le champ de bataille, et la « guerre des réseaux » (*netwar*), mettant aux prises des factions idéologiques au sein de la société qui s'affrontent par le biais d'Internet[1].

Ces auteurs ne pouvaient qu'entrevoir l'échelle à laquelle se développerait Internet en tant qu'espace global et transnational et en tant que moyen de communication, puis comme infrastructure supportant des activités aussi bien virtuelles que matérielles. Surtout, leur analyse était prescriptive. Elle supposait inévitable l'usage militarisé du cyberespace.

Étudier la cyberguerre revient à se demander de quelle manière les États, mais aussi les groupes criminels, les activistes politiques et les entreprises privées se sont approprié l'espace structuré par les infrastructures numériques (le cyberespace) comme fin, comme théâtre, comme enjeu et comme moyen

1. J. Arquilla, D. Ronfeldt, « Cyberwar is coming ! », *Comparative Strategy*, vol. 12, n° 2, 1993, p. 141-165.

d'atteindre un objectif ou de conduire un conflit. Ce processus est à la fois social (du point de vue des acteurs), politique (sous l'angle des rapports de pouvoir qu'il crée, renforce, modifie, déséquilibre) et historique (car profondément contingent). Les analyses prospectives d'Arquilla et Ronfeldt il y a trente ans ne doivent pas nous laisser croire rétrospectivement au développement linéaire et déterminé de ce processus. Les pratiques, les organisations et les doctrines ont interagi et tantôt favorisé, renforcé ou contrecarré des évolutions technologiques mais aussi sociales. Elles ont résulté d'emprunts mutuels et d'interactions réciproques entre les acteurs. Si donc le cyberespace s'est constitué comme « un champ de confrontation à part entière » (selon le *Livre blanc sur la défense et la sécurité nationale* de 2013), ce n'est pas de manière linéaire ni univoque et ce n'est pas uniquement en y transposant les logiques classiques des opérations militaires et des conflits armés.

La terminologie importe en premier lieu. Le recours au préfixe « cyber » rappelle le contexte historique dans lequel sont apparues aussi bien les conceptions que les premières expérimentations de ce que l'on appelle « cyberguerre », plus particulièrement au sein du département de la Défense des États-Unis au début de la décennie 1990. « Cyber » renvoie en effet à deux imaginaires spécifiques. Il trouve sa source la plus évidente dans la littérature cyberpunk étatsunienne de la décennie 1980, plus particulièrement dans la nouvelle « Burning Chrome » que William Gibson fait paraître dans la revue *Omni* en 1982. Outre le fait qu'il a introduit le mot « cyberespace », ce genre littéraire et culturel insiste sur les

dynamiques politiques (voire métapolitiques) suscitées par l'émergence de nouveaux moyens de communication qui offrent des perspectives d'émancipation comme d'oppression.

Le terme « cyber » renvoie également à la cybernétique et à son appropriation par la pensée militaire et stratégique étatsunienne pendant la guerre froide. Décrite par Norbert Wiener au lendemain de la Seconde Guerre mondiale, la cybernétique se définit comme l'étude du rôle central de l'information au sein des systèmes complexes. Elle est notamment au cœur des projets financés par le département de la Défense, dont certains sont à l'origine de l'Internet. La cybernétique imprègne aussi la pensée militaire sous l'angle de l'approche systémique qui cherche à encadrer et standardiser la planification et la conduite des opérations[1]. Au lendemain de la guerre froide, ces deux imaginaires sont restructurés au sein d'un référentiel global articulant des menaces et des risques pouvant provenir de multiples sources et acteurs (étatiques comme non étatiques). En outre, ils permettent à la communauté stratégique de rendre compte des effets révolutionnaires des technologies numériques en matière d'information et de communication, à la fois sous l'angle d'avantages à tirer et de vulnérabilités majeures à compenser. Pourtant, si le terme « *cyberwar* » trouve un large écho dans le monde des analystes de défense, ce n'est pas immédiatement le cas pour « *cyber warfare* » dans la doctrine militaire, auquel on préfère d'abord « *information warfare* », puis « *cyberoperations* » ou « *cyberspace*

1. S.T. Lawson, *Nonlinear Science and Warfare. Chaos, Complexity and the U.S. Military in the Information Age*, Abingdon, Routledge, 2018.

operations ». De la même manière, il faut attendre la fin des années 2000 pour que le département de la Défense introduise le cyberespace comme milieu ou domaine de combat (aux côtés de la terre, de la mer, de l'air et de l'espace).

Cette généalogie suscite deux observations provisoires. L'étude de la cyberguerre passe par celle des représentations. Considérer le cyberespace comme un milieu opérationnel au même titre que l'espace terrestre ou aérien suppose en effet :

- qu'il est doté de caractéristiques spécifiques rendant possible de manœuvrer et de produire des effets cinétiques (le feu, le choc) ou non cinétiques (la surprise, la perturbation, la paralysie, la décohésion, etc.) ;
- que ces missions relèvent d'unités spécialement formées, encadrées, armées et dotées de ressources comme de l'autonomie nécessaire à leur conduite ;
- que s'y déroulent donc des combats où le terrain peut être contesté, conquis, perdu, etc.

D'autres représentations existent. Parler d'infrastructures numériques conduit à insister sur le rôle et l'articulation des dispositifs et des acteurs qui permettent leur fonctionnement. Tel est le cas du modèle structurant le cyberespace en couches physique (routeurs, câbles, serveurs, etc.), logique (logiciels, données, protocoles de routage, etc.) et sociocognitive (utilisateurs, applications, services, etc.). Ici, il est plus important de comprendre le niveau d'intégration et le type d'interactions entre les différents acteurs (l'écosystème) pour appréhender les potentialités d'exploitation ou les vulnérabilités structurelles.

Ces représentations diffèrent selon les contextes. Ainsi, la pratique de la cyberguerre par les militaires n'est pas allée de soi aux États-Unis, existant aux côtés de pratiques plus anciennes au sein des services de renseignement. En France, la standardisation des cadres opérationnels autour des différents domaines de « lutte informatique » (offensive, défensive ou d'influence) s'est opérée à partir d'une double représentation de la cyberguerre comme relevant de configurations asymétriques (du faible au fort) et de tactiques considérées comme « hybrides » (combinant moyens militaires et non militaires dans des cadres temporels entre guerre et paix). En Russie comme en Chine, la cyberguerre est l'une des modalités de l'affrontement dans la sphère informationnelle. Par conséquent, elle s'inscrit dans un spectre très large associant l'espionnage par l'intermédiaire des réseaux numériques à la subversion et à la propagande.

Cette diversité de regards pose un problème à l'analyse. Le terme « cyberguerre » a été contesté dans le champ académique pour son imprécision autant que pour la difficulté à associer les cyberopérations à la catégorie « guerre ». Parler de cyber « guerre » n'est en effet pas neutre dans la mesure où cette dernière catégorie transporte avec elle son lot de représentations, mais aussi de pratiques politiques, juridiques, sociales et institutionnelles. Les unes comme les autres ont été façonnées de manière prédominante par les expériences occidentales des deux derniers siècles, bien que de manière sélective : centralité des acteurs étatiques, encadrement juridique du droit à la guerre et du droit dans la guerre, etc. Or, ces représentations et pratiques ont eu tendance à minimiser d'autres

expériences, notamment le recours à la force armée dans le cadre impérial ou colonial, plutôt comme forces de police et non comme instrument de régulation des antagonismes entre États souverains. En outre, elles ont tardé à s'aligner sur les évolutions de la seconde moitié du XX^e siècle : prédominance des guerres civiles, importance des organisations combattantes non étatiques « irrégulières », recours à la force sans déclaration de guerre ou sous le seuil de l'agression armée, etc. La réticence à utiliser le concept de « guerre » vient aussi des confusions qu'il peut engendrer (entre l'affrontement politique et ses manifestations militaires, par exemple) ou de l'usage inflationniste du terme comme métaphore dans la rhétorique politique ou médiatique. On peut néanmoins s'entendre ici sur la manière de la définir, à savoir « comme conflit létal que soutiennent à grande échelle des organisations politiques entre elles[1] ».

Au début de la décennie 2010, le politologue Thomas Rid a expliqué qu'on ne pouvait pas parler de « cyberguerre », car trois conditions essentielles n'étaient pas réunies : la violence létale, la rationalité instrumentale, la finalité politique[2]. En conséquence, ce que l'on appelle cyberguerre s'apparenterait plutôt à l'espionnage, à la subversion ou au sabotage. Complétant et nuançant Rid une décennie plus tard, James Shires et Florian Egloff ont élargi la conception traditionnelle de la violence, centrée sur le dommage physique ou

1. E. Baranets, « Faut-il changer la définition de la guerre ? », *Raisons politiques*, vol. 88, n° 4, 2022, p. 16.
2. T. Rid, *Cyber War Will Not Take Place*, Londres, Hurst Publishers, 2013.

létal. En incluant les préjudices intentionnels directs contre les corps, la vie affective et la communauté, ils en ont proposé une vision plus nuancée, prenant en compte les différents effets de la cyberguerre en les intégrant dans les programmes de recherche sur la sécurité humaine[1]. Dans cette perspective, la cyberguerre inclut donc des situations aussi diverses que la mise en place de systèmes de contrôle et de surveillance par des gouvernements, les opérations conduites contre les infrastructures civiles pour en perturber l'activité, le vol et la divulgation de données à caractère personnel à des fins d'intimidation ou de manipulation (*hack-and-leak*). Cette grille de lecture permet aussi de dépasser les oppositions entre temps de paix et temps de guerre, théâtre des opérations et « arrière », actions « cinétiques » (produisant des effets physiques) et « non cinétiques ».

On peut également réfléchir à la cyberguerre à partir de la notion de cyberopération. En réintroduisant les critères opérationnels, on insiste sur les facteurs de temps, d'organisation, de mobilisation des ressources, mais aussi de probabilité et de chance. Aborder la cyberguerre sous l'angle opérationnel exige aussi de s'interroger sur les acteurs eux-mêmes, leurs modes d'organisation, leur inscription dans un écosystème social, institutionnel et politique spécifique ou encore leurs objectifs.

La cyberguerre est aussi un objet d'étude. On peut tenter de la quantifier dans des bases de données.

1. F. Egloff, J. Shires, « The better angels of our digital nature ? Offensive cyber capabilities and state violence », *European Journal of International Security*, vol. 8, n° 1, 2023, p. 130-149.