72

Cyberguerres et cyberattaques

« *This isn't a video game. It's a war. A real war.* » (Colin Powell, *Fox News*, 2003)

Dès la fin des années 1980, les NTIC sont placées au cœur des réflexions relatives à l'impact des technologies sur l'art de la guerre. On parle alors de « révolution dans les affaires militaires » (RMA*). Les États-Unis sont alors leaders dans la réflexion stratégique, tactique, conceptuelle et doctrinale et s'interrogent sur la manière dont ces nouvelles technologies vont radicalement changer l'organisation des armées et la conduite de la guerre au XXIe siècle. Désormais, les moyens de pression des différents acteurs s'expriment aussi bien sur le champ de bataille que dans le cyberespace. Si les robots de combat sont encore de la science-fiction, les drones-tueurs sont devenus d'usage courant (frappes américaines en Afghanistan, au Pakistan, en Somalie et au Yémen).

La notion de « cyberguerre » renvoie aux conflits ayant pour territoire les réseaux informatiques mondiaux. Au début des années 1990 des auteurs américains comme John Arquilla et David Ronfeldt proposent la notion de « *netwar* » pour désigner ces nouvelles formes de combat (*The Advent of Netwar*). Le « cyberconflit » renvoie la dimension cybernétique des conflits infra et interétatiques. Il n'est pas un conflit virtuel : quand un antagonisme a émergé, le conflit est réel. Tous les passages à l'acte (piratage informatique) et tous les moyens de pression (attaques de serveurs) ne sont pas uniquement déployés sur les réseaux informatiques et de communication. À l'inverse, les « cyberattaques » désignent ces actions dans le cyberespace qui peuvent se substituer aux guerres conventionnelles. Les cyberattaques peuvent être considérées comme des moyens de pression à l'encontre des États (diplomatie coercitive).

Les acteurs de cette guerre sont des experts informatiques (*hackers*), leur arme la plus connue le virus informatique. Le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants ou « *malware* ». Les « maliciels » englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces. Le virus le plus connu fut le virus Stuxnet américain et israélien injecté dans les systèmes de contrôle des centrifugeuses du site nucléaire de Natanz en Iran en 2010. Les hackers bénéficient de l'effet de surprise : il est difficile de savoir l'origine d'une attaque, parce que l'agresseur s'abrite souvent derrière un réseau d'ordinateurs qu'il a piraté. Les cyberattaques se classent ainsi dans la catégorie des conflits asymétriques.

Le cyberespace* peut être à la fois l'enjeu d'un conflit portant sur un marché ou sur des informations stratégiques, le théâtre du conflit dans le cas des cyberattaques ou bien l'outil essentiel de la maîtrise de champs de bataille éloignés. Il désigne ce nouvel environnement de combat.

Les cyberattaques accompagnent les conflits militaires. Ces nouveaux types d'offensives viennent s'ajouter à des opérations militaires ou de renseignements plus classiques. Mais bien qu'elles aient lieu dans le cyberspace elles ne sont pas déterritorialisées : elles ont lieu en majeure partie aux États-Unis, en Russie, et en Chine. La géographie des cyberattaques exprime ainsi les rapports de force géopolitiques contemporains. Le conflit entre la Russie et l'Ukraine a mobilisé des moyens visant à maîtriser la propagande sur les réseaux sociaux dans les deux camps ; la Russie a également eu recours à des attaques par *malware*. Ces mêmes réseaux sociaux se sont trouvés au cœur de la guerre en Lybie, mobilisant des cyberactivistes et hacktivistes de diverses nationalités. Les conflits récents ont bien intégré la dimension cybernétique.

L'informatisation des forces armées se poursuit. Pendant la guerre du Vietnam, l'armée américaine avait installé près de 20000 capteurs électroniques pour surveiller 250 km de front. Les informations étaient traitées et transmises en temps réel aux forces aériennes pour qu'elles interviennent. Le conflit en Afghanistan a vu le déploiement des drones pilotés depuis des centres de commande éloignés du champ de bataille. Pour leurs pilotes, la cible est déshumanisée, mise à distance sur un écran, mais les conséquences des frappes sont bien réelles. Les forces armées se réorganisent en laissant plus de place à ces nouveaux systèmes de communication et échanges de données. La plus importante transformation fut la création en 2010 aux États-Unis du *Cyber Commandement* intégré à la NSA (*National Security Agency*). Cette création marque la reconnaissance officielle du cyberespace comme domaine d'affrontement, et implique la création de forces dédiée comme la création d'un « cyber-arsenal » ou de « cyber-armes ».

La simulation des conflits s'est longtemps appuyée sur des jeux qui servaient d'entraînement, comme au XVII^e siècle le jeu de plateau le *Koenigspiel* pour former l'aristocratie à la guerre. L'émergence des jeux vidéo s'inscrit dans la filiation entre jeu et guerre. Le premier jeu informatique, un jeu de morpion sur 9 cases (XOX) a été programmé sur l'EDSAC, un calculateur construit en 1949 à Cambridge pour faire des calculs balistiques. Tout jeu vidéo repose sur du conflit : le joueur ne peut avancer que par élimination d'un obstacle, sous peine d'être éliminé lui-même. Les jeux violents et les enjeux de guerre, toujours plus réalistes et sanglants, se multiplient depuis les années 1990. La géographie des conflits dans les jeux vidéo évolue en lien avec leur contexte de production et avec l'actualité. Les premiers jeux vidéo situent plutôt l'action

dans des univers « hors du monde ». Dans les années 1980 et 1990, la Guerre froide est la référence, comme la Seconde Guerre mondiale utilisée pour les simulations financées par le CMI* américain. En 2002, l'armée américaine finance le jeu *America's Army* : ce jeu a permis de redorer l'image de l'armée alors engagée en Afghanistan, de faciliter le recrutement et stimuler les entraînements. En 2009, est sorti *Balance of power : 21th Century*. Le jeu se passe désormais après le 11 septembre 2001 et le joueur ne peut incarner que le président des États-Unis. L'ennemi à abattre n'est plus le Rouge, mais le terroriste. La cartographie des jeux vidéo de guerre exprime bien les représentations et idéologies d'un monde en guerre. Finalement, le stade ultime de la numérisation des conflits, le cyberconflit qui ne se déroule que dans le cyberespace, ce sont les jeux vidéo mondialisés multi-joueurs.

Les cibles des cyberattaques ne concernent plus seulement les États, mais aussi les entreprises les organisations et les particuliers, dans le cadre de la compétition économique ou de tensions politiques. La société Google a révélé en janvier 2010 que ses serveurs en Chine avaient été attaqués et qu'un important volume de données y avait été dérobé en décembre 2009. Google a accusé Pékin. En 2010, le conflit entre Wikileaks et les autorités américaines a conduit à une « cyberguérilla ». Après la révélation de 200 000 documents confidentiels, dont les documents classés « secret défense » sur les guerres en Irak et en Afghanistan. Le 28 novembre 2010, les transferts bancaires à destination de Wikileaks ont été bloqués par les sociétés Visa, Mastercard et Paypal. En représailles des sympathisants ont lancé l'opération Payback en décembre 2010 : une série d'attaques par déni de service contre les sites de ces sociétés et contre la banque suisse PostFinance qui avait gelé un compte du fondateur de Wikileaks, Julien Assange. En 2013, une opération de cybercriminalité et d'espionnage cible l'entreprise américaine Yahoo. Les attaquants ont volé les données de 3 milliards d'utilisateurs. La mise en vente de ces données a été détectée en août 2017.

La cyberdéfense devient un enjeu sécuritaire pour les États. Elle se définit comme « l'ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'informations jugés essentiels » et comme « l'ensemble des activités qu'il conduit afin d'intervenir militairement ou non dans le cyberespace pour garantir l'efficacité de l'action des forces armées, la réalisation des missions confiées et le bon fonctionnement du ministère » (Ministère français des armées). L'enjeu de la sécurité numérique appartient à un enjeu plus global de sécurité nationale, avec l'informatisation toujours plus accrue des sociétés. Alors que la « cybersécurité » couvre le domaine de la protection des systèmes d'information de manière générale (technologies, organisations, processus, lois, techniques de sécurité des systèmes d'information...), la « cyberdéfense » décrit plutôt

ce qui est du ressort de la défense nationale. La cyberdéfense représente un enjeu économique considérable. À l'échelle planétaire, selon le magazine *Forbes* en 2015, elle portait sur un marché évalué à 75 milliards de dollars, culminant à plus de 170 milliards de dollars en 2020. Elle participe des évolutions actuelles du complexe militaro-industriel (CMI)*. Les entreprises liées à la cyberdéfense sont de plus en plus nombreuses. Parmi celles-ci, on trouve en France Airbus CyberSecurity, Thales, ou encore le Groupe Orange avec sa filiale Orange Cyberdefense créée en 2014.

🕮 Références

- John Arquilla et David Ronfeldt, *The Advent of Netwar*, Rand Corp., 1996.
- Les Grands Dossiers de Diplomatie, *Géopolitique du cyberespace*, Areion Group, n° 23, octobre-novembre 2014.
- Daniel Ventre, « Vers la militarisation du cyberespace », dans *Internet, ça sert, d'abord, à faire la guerre, La Revue des médias*, INA, 2016 (en ligne).
- Daniel Ventre, *Intelligence artificielle, cybersécurité et cyberdéfense*, Londres ISTE, 2020.
- Stéphane Taillat, Amaël Cattaruzza et Didier Danet, *La Cyberdéfense. Politique de l'espace numérique*, Armand Colin, 2018.
- Nicolas Ténèze, *Combattre les cyberagressions : enjeux, politiques et limites*, éd. Nuvis, 2018.

➢ Voir entrées

Guerre de l'information, RMA, Cyberespace, Terrorisme, Médias, CMI.