L'équilibre stratégique au défi des drones et des cyber-armes

Justin Vaïsse | Directeur du Centre d'analyse, de prévision et de stratégie.

Je voudrais essayer de mettre la notion d'équilibre stratégique (un concept d'ailleurs discutable, la stratégie étant par nature dynamique et politique) à l'épreuve des nouvelles technologies de la guerre moderne, les drones et les cyber-armes. L'équilibre stratégique, à la fois l'équilibre réel des forces militaires et les rapports stratégiques traditionnels entre les acteurs du système international, se trouve-t-il remis en cause, renversé ou bien renforcé par ces armes nouvelles ?

Je serai conduit à me servir abondamment de l'exemple américain, puisque ce sont les États-Unis qui ont, en premier, développé et fait usage de ces armes à grande échelle, au cours des années 2000. Je pense notamment aux drones, qui avaient connu de grands progrès depuis quelque temps déjà mais n'avaient pas été armés, que ce soit dans les Balkans ou en Afghanistan. C'est lorsque la *CIA* a eu un visuel sur Oussama Ben Laden dans les environs de Kandahar en 2000, depuis un drone *Predator*, sans pouvoir tirer sur lui autrement que par une frappe de missiles trop lente depuis l'océan Indien que les drones ont été armés, avec une efficacité croissante et des développements très rapides. Quant aux cyber-armes, c'est aussi au cours de la décennie 2000 qu'elles ont connu leur développement le plus rapide, même si la technologie des virus n'est pas nouvelle. Depuis que deux ordinateurs ont été reliés entre eux, de Stanford à Berkeley en 1972, on sait qu'il est très difficile de protéger les communications et de se prémunir de l'introduction de lignes de code malveillantes par un tiers (espionnage, sabotage, prise de contrôle).

L'âge d'or de ces deux armes n'a pas été les années Bush, même s'il a été le premier président à les utiliser, mais le premier mandat d'Obama, tout simplement parce que cela correspondait à la nécessité stratégique du moment, celle du désengagement, de la diminution des soldats dans les deux guerres au sol d'Irak et d'Afghanistan sans pour autant compromettre la sécurité des États-Unis. Drones et cyber-armes permettaient à Obama d'agir de façon furtive, de se retirer tout en combattant à moindre coût, d'où la multiplication spectaculaires des frappes de drones et l'utilisation du virus « Jeux Olympiques » (*Stuxnet*) contre l'Iran.

Ces armes nouvelles ont en commun d'éliminer ou de diminuer l'asymétrie stratégique gagnée par certains des nouveaux acteurs de l'équation

stratégique, je me référerai ici notamment aux écrits de Pierre Hassner. Le terroriste kamikaze qui s'expose totalement car il ne craint pas la mort trouve en quelque sorte son répondant dans le pilote de drone, qui ne s'expose plus du tout (il est vrai que le pilote de *F16* ne risquait déjà plus grand chose). Avec les armes cyber, l'anonymat permet d'agir de façon secrète ou furtive : l'inverse de l'organisation terroriste dont l'objectif est l'action d'éclat.

La remise en cause de l'équilibre stratégique et des rapports de force tient alors au brouillage des notions de guerre et de paix traditionnelles, avec par exemple, des notions nouvelles comme celle d'occupation par le ciel, ce qu'on voit par exemple au-dessus de Gaza par l'armée israélienne *via* les drones ; le brouillage de la frontière entre guerre et maintien de l'ordre ; le problème – pointé plus tôt par l'amiral de Tarlé – de caractérisation stratégique et juridique de l'adversaire, avec le brouillage irrémédiable entre militaires et civils, par exemple dans le domaine cyber, le recours des « brigades de volontaires » par la Russie (*cyber berkouts*) ou la Syrie (Armée numérique syrienne) ; la baisse de la létalité et de la violence physique ; pour le drone, parce qu'après un ciblage et un suivi des cibles, les frappes sont plus précises et dans l'ensemble moins létales (même si elles peuvent encourager un recours accru à ces armes par abaissement du seuil), et pour les armes cyber, par la possibilité de cibler plus précisément par exemple les centrifugeuses iraniennes ou les ordinateurs et installations d'Aramco, plutôt que de les bombarder ou de commettre un attentat contre elles.

On peut sans doute voir dans ces différentes évolutions une remise en cause du rapport de force traditionnel des puissances.

Est-ce que cette tendance au brouillage et à l'égalisation peut aller jusqu'à un renversement des rapports de force ? Il y a sans doute ici une dialectique en trois temps : à l'âge de l'innocence et du monopole (l'avance des Américains leur permet d'avoir un avantage, tant que les drones et le cyber restent une « frontière » technologique) succède l'âge de la démocratisation, le faible coût de ces technologies conduisant à un renversement de leurs implications pour le domaine stratégique. Avec cette égalisation, le cyber, voire le drone, deviennent l'arme du pauvre, à tel point que non pas seulement des puissances en développement, mais aussi des civils ou des groupes non étatiques comme le *Hezbollah* peuvent utiliser ces armes en bénéficiant notamment de l'anonymat qu'elles permettent. On observe aussi l'utilisation massive du cyber par la Chine, non pas dans un sens directement militaire, mais pour aider son rattrapage économique à la fin des années 1990 et au début des années 2000, à un moment où les défenses occidentales étaient minimes. Quant à l'Iran, après avoir subi les attaques des virus « Jeux Olympiques » lancés par les Américains et les Israéliens, il a comblé son retard et on lui attribue les attaques contre l'Aramco.

Bien sûr, les puissances établies, à commencer par les États-Unis, réagissent à cette démocratisation, à cette perte de monopole, par une volonté

graduelle de codification, en introduisant des règles de route. L'analogie, c'est celle du nucléaire, après la période brève de monopole américain puis de duopole puis d'oligopole à partir des années 1960, qui voient les grandes initiatives de contrôle des armements, notamment le TNP. Mais on n'en est pas là et il n'est pas certain qu'une codification soit possible, en raison du faible coût et de l'accessibilité de ces armes nouvelles.

Mais il y a une autre raison pour laquelle il est permis de douter que la codification, l'encadrement par des normes, pourra vraiment progresser. Il se pourrait bien que le troisième temps de la dialectique soit celui du renforcement des rapports de force et de l'équilibre stratégique en faveur des puissances établies et des règles traditionnelles. C'est au fond l'idée ancienne de l'épée et du bouclier : l'épée développée par les Occidentaux, à commencer par les Américains, puis imitée par d'autres et retournée contre eux, suscite des contre-mesures de haute technologie et l'érection de murs efficaces. Je pense, dans le domaine cyber, à la diffusion de mesures d'hygiène informatique et au perfectionnement institutionnel des défenses (*cf.* l'Anssi – Agence nationale de la sécurité des systèmes d'information – et le Calid – Centre d'analyse de lutte informatique défensive – en France), d'où une hausse du coût et de la sophistication des attaques cyber qui va en limiter l'emploi à un plus petit nombre d'acteurs essentiellement étatiques. De la même façon, les drones sont des engins lents et vulnérables, et les pays occidentaux peuvent se prémunir contre eux.

Finalement, on devrait assister, à terme, à un renforcement des rapports de force et des puissances établies : les cinq du Conseil de sécurité de l'ONU, plus quelques autres comme l'Iran, Israël et l'Allemagne, qui ont au premier chef les capacités, dans le domaine cyber, de jouer dans « la cour des grands », et de pouvoir avoir à la fois des murs de défense plus élevés que les autres et des échelles qui leur permettent de voir chez les autres. Bref, il y aurait bel et bien un moment de remise en cause voire de renversement des rapports de force traditionnels par les armes nouvelles, mais au bout du compte c'est à leur confirmation et leur renforcement qu'à mon avis on devrait assister, à terme.

⁂

Je conclurai sur le cas français. Nous avons souffert, dans les années 2000, d'un double retard dans ces armes nouvelles. Celui-ci est moins marqué aujourd'hui avec le sérieux effort de rattrapage effectué : très partiellement pour ce qui est des drones, de façon beaucoup plus sérieuse dans le domaine cyber, depuis le *Livre blanc* de 2008. Il était temps. Le retard que nous accusions sur les principaux acteurs était préoccupant, et si ma conclusion d'ensemble est exacte, il est fondamental de nous affirmer comme une puissance cyber et une puissance dans le domaine des drones afin de coller au peloton de tête des pays qui assurent l'équilibre stratégique de la planète.