A propos de la cyberdéfense chinoise

Daniel Ventre, CNRS (CESDIP/GERN). Titulaire de la Chaire Cybersécurité & Cyberdéfense

Mai 2015, Article III.23

I - Forces de cyberdéfense

La Chine parle de l'existence de ses unités dédiées à la cyberdéfense (les médias anglo-saxons retiennent le vocable « cyberwarfar »). Selon McReynolds1[1], chercheur au CSIS (Washington), la reconnaissance officielle de l'existence de ces unités serait contenue dans la dernière version de « The Science of Military Strategy »[2] (Décembre 2013). On y apprendrait que les forces de cyberdéfense sont de trois types :

- les forces militaires spéciales de guerre sur les réseaux (specialized military network warfare forces) qui sont des unités militaires opérationnelles
- des équipes de spécialistes du monde civil (le ministère de la sécurité publique, le ministère de la sécurité d'Etat…) autorisées par l'armée à mener des opérations de cyberdéfense ;
- et des entités extérieures au gouvernement, qui peuvent être mobilisées, organisées pour de telles opérations.

Toujours du point de vue de McReynolds, cette reconnaissance officielle :

- vient conforter les Etats-Unis et nombre d'autres nations qui ont depuis plusieurs années mené des enquêtes sur les cyberattaques et concluant souvent à l'implication des acteurs étatiques chinois.
- vient mettre un terme à des années de déni de la part de la Chine, qui a toujours jusque-là refusé de reconnaître à la fois l'existence de structures de type cybercommandement ou le soutien des forces armées dans de quelconques cyberattaques, notamment à des fins d'espionnage industriel.
- implique la nécessite de repenser les coopérations engagées par la Chine en matière de lutte contre la cybercriminalité (la Chine aurait collaboré avec près de 50 pays dans le cadre d'enquêtes sur des milliers de cas de cybercriminalité au cours des 10 dernières années ; et conclu une trentaine d'accords bilatéraux, dont des accords avec les Etats-Unis et le Royaume-Uni). On ne saurait en effet, selon lui, faire confiance à des institutions étatiques chinoises qui d'un côté prétendent lutter contre la cybercriminalité, mais de l'autre soutiennent des opérations de hacking contre les intérêts des Etats avec lesquels elles coopèrent…

Cette analyse appelle des commentaires. La « révélation » de l'existence d'unités de cyberdéfense chinoises n'est pas véritablement un scoop. Les Etats modernes se dotent de capacités cyber, et la

1 http://www.thedailybeast.com/articles/2015/03/18/china-reveals-its-cyber-war-secrets.htm

2 http://www.amazon.com/Science-Military-Strategy-Chinese-Edition/dp/7802376505

Chine a fait du cyberespace, on le sait depuis longtemps, l'un de ses domaines stratégiques. Que cela soit écrit dans un document officiel est certes important. Mais reconnaître l'existence de structures de cyberdéfense n'est pas l'aveu des cyberattaques qu'on leur attribue. De l'organisation décrite, il ressort que se multiplient, comme ailleurs, les acteurs de la cyberdéfense. Et même si le tout peut paraître parfaitement hiérarchisé, des tensions au sein même des institutions étatiques pourraient gripper la machine. McReynolds évoque ce risque lorsqu'il affirme que des signes de tensions sont apparus, pour savoir qui de l'armée ou des institutions sécuritaires civiles doit assurer le leadership sur les cyber-opérations.

II - Les faiblesses de l'armée chinoise

La RAND Corporation vient de publier un long rapport (184 pages) portant sur les faiblesses de l'armée chinoise (China's incomplete military transformation. Assessing the weaknesses of the People's Liberation Army. Février 2015)[3].
La « faiblesse » militaire (military weakness) y est définie (p.2) comme l'impossibilité totale de remplir une mission ; le risque élevé d'échec d'une mission ; toute inefficacité susceptible de dégrader les résultats attendus d'une mission. Le rapport propose tout d'abord un regard sur le processus de modernisation engagé dans les années 1990 et programmé jusqu'en 2025 ; puis s'intéresse aux missions de l'armée ; se focalise sur les faiblesses organisationnelles, en termes de ressources humaines, en termes de capacités de combat ; et enfin s'intéresse aux faiblesses de son industrie de défense.
Il est question du cyberespace (p.114-119) dans le chapitre consacré aux faiblesses capacitaires. Les domaines y sont traités un à un (terre, mer, air, nucléaire, espace, cyber et électromagnétique). La Chine a lancé ces dernières années de nombreux satellites, renforçant ainsi ses capacités ISR, navigation, positionnement, communications. Pour protéger ces capacités satellitaires, la Chine déploie aussi des moyens de défense spécifiques. L'armée développe également d'importants moyens de guerre électronique (radio, radar, infrarouge, optique, informatique, systèmes de communication). Les capacités cyber pour le combat sont au cœur de cette politique de développement capacitaire (collecte d'information, perturber l'action de l'adversaire, multiplicateur de force). Mais si le développement des capacités offensives semble suivre une courbe ascendante, il n'en va pas de même des capacités de protection des intérêts chinois dans les domaines spatiaux et électro-magnétiques, qui resteraient relativement vulnérables. Les études chinoises s'inquiètent de la dépendance croissante aux systèmes spatiaux (satellites) et retiennent que dans ce domaine l'offensive prime sur la défense. Les questions cyber sont englobées dans les considérations sur l'usage du spectre électromagnétique : la Chine se définit dans ce domaine comme vulnérable. Les faiblesses ne procèdent pas seulement des obstacles techniques, technologiques, qu'il faut surmonter pour mettre en œuvre des systèmes C4ISR, mais aussi des procédures (faible coordination entre les agences de renseignement, les opérationnels et les décideurs au plus haut niveau). Soulignons que ces constats, formulés par les auteurs du rapport, s'appuient principalement sur des publications chinoises, ce qui oblige à relativiser l'analyse. Les quelques lignes dédiées au cyberespace restent assez générales dans leur propos, et nous ne voyons là rien de véritablement spécifique aux forces chinoises. Le rapport souligne, pour terminer ce chapitre (p.117), l'absence de considération, par les analystes chinois, de la problématique des effets non intentionnels et des risques d'escalade non maîtrisés. Les analystes chinois auraient tendance à insister sur les avantages, sur les aspects positifs des gains de la guerre de l'information, mais à ignorer ses limites et ses risques.

3 http://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR893/RAND_RR893.pdf