La note du CESA
N°92
11 / 2016

Stagiaire Clémence Bouchard

Quelle structuration de la cyberdéfense en République Populaire de Chine ?

L'observation par la République P*opulaire de Chine (RPC) de l'opération* Desert Storm *en 1991 fut le point de départ d'un renouveau doctrinal dans l'Armée populaire de libération (APL). En effet, c'est à l'occasion de la première guerre du Golfe que les États-Unis ont démontré leur capacité de mener une guerre électronique en rompant les communications de l'armée irakienne. Les Chinois ont ainsi pu mesurer leur retard dans ces techniques et sont parvenus à se hisser en quelques années au rang de cyberpuissance.*

L'« informationalisation » de l'Armée populaire de libération

C'est le général Dai Qingmin qui, en 1999, théorise la stratégie de l'armée chinoise dans le cyberespace sous le sigle *INEW* : *Information Network Electronic Warfare*. Cette théorie repose sur trois piliers : perturber les systèmes d'information pour désorganiser et paralyser l'adversaire, conduire des opérations d'information préventives en les combinant avec les techniques de frappe conventionnelles et enfin, défendre constamment ses propres informations tout en exploitant celles de l'opposant.

Le terme *xinxihua* ou « informationnalisation » est employé pour la première fois dans le Livre blanc chinois de 2004. Ce néologisme peut être relié à la théorie des vagues de développement conçue par les époux Toffler[1]. Ceux-ci pensent que la « vague de la connaissance » succède à la « vague industrielle » et que cette succession a des implications dans tous les domaines, y compris dans l'art de la guerre. L'APL s'engage donc dans ce processus qui consiste à développer et à adopter des techniques d'information dans toutes les strates de l'armée pour faire corps avec la doctrine *INEW*.

En 2014, Xi Jinping annonçait la création d'une nouvelle branche de l'APL : la force de soutien stratégique (FSS). Celle-ci est chargée de l'espace, du renseignement, de la guerre électronique, de la cyberguerre et des opérations psychologiques. Le poids substantiel du cyber dans la stratégie globale chinoise est désormais acté. Quant à la FSS, elle s'inscrit dans la vaste politique de réforme menée par le Président chinois afin de renforcer son contrôle sur l'armée.

Des méthodes de recrutement audacieuses

Dès la fin des années 1990, l'APL a développé ses propres formations militaires dans le but de constituer des unités cyber. L'institution recrute aussi de nombreux étudiants issus des universités et des centres technologiques du pays.

Elle a été parmi les premières armées à s'appuyer sur des acteurs non-institutionnels. Des milliers de *hackers* nationalistes se sont fait connaître par des attaques spontanées dirigées contre l'Indonésie, contre Taïwan et contre les États-Unis entre 1990 et 2004 à la suite d'incidents diplomatiques avec ces derniers. Ces *hackers* sont ensuite sortis de la clandestinité en créant des agences de conseil en sécurité informatique pour travailler directement au profit de l'État. Des lois anti-*hacking* draconiennes ont permis à Beijing de dissocier les pirates progouvernementaux de ceux hostiles au régime pour enrôler les uns et pour neutraliser les autres. Selon le rapport de la *Northrop Grunman Corporation*[2] au Congrès américain, le gouvernement chinois aurait directement publié des offres d'emploi sur les forums de *hacking* les mieux établis.

Grâce au soutien d'une partie de la communauté des *hackers* chinois, l'armée a pu combler son besoin urgent en cyber-guerriers tout en s'entourant de profils talentueux et déjà expérimentés. La réactivité de la classe dirigeante chinoise pour intégrer la dimension cyber dans la stratégie militaire ainsi que le recours à des experts issus du sérail du *hacking* démontrent le fort potentiel d'adaptation de l'APL.

En l'espace de deux décennies, la Chine a recouvré son retard technique en cyberdéfense et défie les États-Unis par une institutionnalisation rapide et poussée du phénomène. Désormais, Beijing s'intéresse à la régulation d'Internet et se montre en faveur d'une gouvernance mondiale sous le contrôle des États afin de sanctuariser son propre cyberespace. En témoigne l'instauration, en septembre 2015, d'un dialogue sino-américain sur la cybercriminalité en vue d'établir un accord de non-agression dans le cyberespace. Le but de cet accord n'est pas de mettre un terme à toute forme de cyberattaque ou de cyberespionage mais d'établir un cadre juridique qui puisse conduire à une forme de stabilité dans ce domaine.

Ces propos ne reflètent que l'opinion de l'auteur.

1 Alvin Toffler, *La Troisième Vague*, Delanoël, Paris, 1980
2 « *Capability of the People's Republic of China to Conduct a Cyber Warfare and Computer Network Exploitation* »