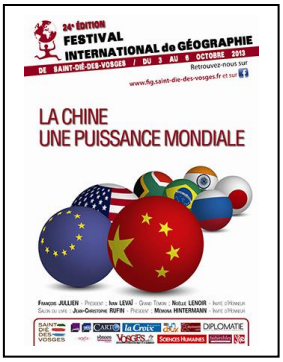
Conférence




# L'ART DE LA GUERRE REVISITE, LA CYBERSTRATEGIE DE LA CHINE.

Par Alix Desforges, chercheuse à la chaire Castex de cyberstratégie et doctorante à l'Institut Français de Géopolitique, Université de Paris 8.

Les attaques informatiques contre les états commencent dès les années 1990 et se multiplient depuis 2008, en nombre et en taille. Le cyberespace est devenu un enjeu majeur de défense, avec des attaques destinées à déstabiliser (modification de la page d'accueil d'un site par exemple), des attaques d'espionnage classique, et des attaques de sabotage , par exemple le « ver Stuxnet » développé par les Etats-Unis et Israël en 2010 contre les centrales nucléaires iraniennes. (http://fr.wikipedia.org/wiki/Stuxnet) .

Ces attaques sont rapides, anonymes, asymétriques, discrètes pour les victimes et inconnues du grand public. Les états tentent de se protéger en particulier les Etats-Unis et l'Europe.

La Chine est un leader de la cyberstratégie. Sa stratégie est compréhensive (intégrée), très globale et donc inquiétante, car ces attaques peuvent être considérées comme des actes de guerre. Internet a eu en Chine un développement très rapide, avec un maintien d'une main mise de l'état. 42% des chinois ont accès à Internet par des fixes ou des mobiles.

## 1. La cyberstratégie de la Chine.

Le « great firewall of China » permet un développement très contrôlé, par surveillance des mots clés, la priorité étant donnée à la survie du régime, et donc à "la supervision des informations nocives". La censure ne s'applique pas systématiquement, elle est plus importante dans les régions "à risques" ou quand un sujet devient médiatique, et toujours intraitable contre la pornographie et la critique de la censure. Les méthodes évoluent avec une tendance à la condamnation des porteurs de rumeurs si leur information est relayée. Les trois grands distributeurs sont liés directement à l'état, et les acteurs du web international sont soumis à la censure chinoise. Par exemple, Facebook et Twitter sont exclus sauf dans la ZEE de Shanghaï. Tous les réseaux sociaux sont contrôlés, doublés par des entreprises chinoises et sont des moyens de propagande chinoise, par exemple Weibo.

Une grande méfiance demeure, car Internet est considéré comme porteur d'une volonté systématique d'espionnage et de déstabilisation de la part de l'occident.

Dans ce contexte, l'attaque « Aurora » contre Google viendrait de la Chine, et cet incident est allé jusqu'à un conflit diplomatique avec le discours d'Hillary Clinton sur les « pirates Internet ».

L'armée chinoise a introduit le concept "d'informationisation" dans sa stratégie militaire, en utilisant les concepts ancestraux de l'art de la guerre contre les ennemis invisibles sans coups de feu.
Le gouvernement soutient massivement les entreprises de routage (Lenovo par exemple), les études d'informatique sont valorisées, la recherche est encouragée.

**2. la montée en puissance de la cyberstratégie de la Chine.**

La Chine tente de participer à la gouvernance de l'Internet, et critique ce modèle qui fait une grande place à la société civile, ce qui n'est pas acceptable pour elle. La Chine et la Russie prônent un contrôle d'Internet par l'ONU, et participent aux instances de normalisation et de création de noms de domaines non latins. Des accords bilatéraux avec la Russie visent au contrôle des cyber-armes et militent pour le contrôle d'Internet par les états. S'y associent des états démocratiques comme la France, le Royaume Uni et l'Australie, pour des actions de censure limitées à la pédophilie par exemple.
La Chine a déjà fait quelques démonstrations de force : par exemple en 2010, le détournement du trafic de « ejacking » (routeur Internet de dimension mondiale) par la Chine a duré 20 minutes, et a été annoncé ensuite comme une erreur de routage. La Chine pratique aussi des attaques d'espionnage pour trouver des informations ou pour repérer les faiblesse adverses, ou créer des « botnet » (ordinateurs zombis contrôlés à distance à l'insu de leur propriétaire), sans doute avec l'appui des entrepreneurs chinois (les fabricants de routeurs par exemple).

**3. une puissance à relativiser.**

Cette menace est-elle réelle, ou la Chine est-elle victime d'un discours occidental hostile ? En effet, les protestations des Etats Unis montent depuis 2012, B. Obama a fait des accusations directes et une fuite a révélé le contenu d'un rapport sur des attaques militaires possibles pour prévenir la menace chinoise. En fait, d'autres menaces existent venant des Etats-Unis (voir l'affaire de la NSA), de la France, et d'Israël. Et en Chine, de jeunes hackers pratiquent une cybercriminalité active contre des acteurs économiques et politiques, sans être arrêtés.
En définitive, la Chine est aujourd'hui un acteur majeur du cyberespace, puissant, capable d'attaques, mais reste une puissance en construction, qui n'a pas encore tous les outils nécessaires.

Anne Calvet