http://abonnes.lemonde.fr/technologies/article/2013/12/17/le-droit-de-la-guerre-envahit-le-cyberespace_4335695_651865.html

Le droit de la guerre envahit le cyberespace

LE MONDE | 17.12.2013 à 14h40 |Par **Yves Eudes**

Au sein de l'OTAN, la « cyberguerre » fait désormais partie intégrante de la réflexion tactique et stratégique, et sa codification juridique est déjà en bonne voie. Onze pays membres de l'Alliance atlantique, dont les Etats-Unis, ont créé à Tallinn (Estonie) un « Centre d'excellence » technique et juridique consacré à la cyberdéfense. Il est ouvert depuis 2008, mais sa montée en charge est très progressive.

L'une des missions du centre est de réfléchir à la façon dont le droit de la guerre va s'appliquer dans le cyberespace. Pour cela, il a réuni une équipe de juristes spécialisés, américains et européens, qui ont déjà produit une masse de textes théoriques et de recommandations.

Ils envisagent, par exemple, de fixer un *« seuil d'intensité »* au-delà duquel une cyberattaque peut être considérée comme un acte de guerre. Ainsi, une cyberagression massive, provoquant ou non des dégâts matériels, contre un membre de l'OTAN pourrait justifier le déclenchement du mécanisme de sécurité collective de l'Alliance : tous ses membres entreraient dans le conflit pour venir en aide au pays attaqué.

Les juristes tentent aussi de déterminer quels types de contre-mesures seraient légitimes pour faire cesser une attaque, et quels types de contre-attaques seraient jugés excessives ou disproportionnées.

Par ailleurs, les experts du centre souhaitent inciter les Etats membres de l'OTAN à faire la distinction, comme dans les conflits classiques, entre les cibles militaires et les infrastructures civiles, qui doivent être protégées autant que possible. Cela dit, si des civils, y compris des « hacktivistes » (hackers à motivation politique) participent à un acte de cyberguerre, ils deviennent une « cible légitime ». Par ailleurs, ils remarquent que les dommages collatéraux infligés à des installations civiles lors d'une cyberguerre seront sans doute inévitables

– une forme de justification par avance. Ils rappellent enfin que l'espionnage, sur Internet ou ailleurs, n'est pas contraire au droit de la guerre.

SIMULATIONS

Le centre de Tallinn possède aussi des missions techniques, notamment la formation de militaires des pays membres. Pour cela, il a organisé ces deux dernières années plusieurs simulations de cyberattaques en grandeur nature – la dernière en date a eu lieu en novembre.

Une équipe de pirates, en réalité des experts civils et militaires, s'est installée dans les locaux du centre. Puis, pendant deux jours, elle a lancé des attaques complexes et diversifiées contre des centres informatiques militaires situés dans les pays participants, qui doivent improviser leur défense en temps réel.

Ces simulations se sont révélées utiles, car leur bilan est alarmant : la majorité des centres visés résiste mal aux attaques les plus sophistiquées et n'arrive pas à partager efficacement leurs informations avec leurs homologues. En revanche, l'équipe internationale chargée de protéger le réseau interne de l'OTAN, basée en Belgique, s'est bien défendue contre les attaques venues de Tallinn. Cinq nouveaux pays membres de l'Alliance, dont la France, devraient bientôt rejoindre officiellement le Centre d'excellence. Des officiers français sont déjà sur place.

▪ **Yves Eudes**
Grand reporter

Cyberguerre

- L'armée chinoise accusée de pirater les transporteurs de l'armée américaine
- Le FBI enquête sur des cyberattaques probablement menées depuis la Russie
- L'armée française bientôt sous surveillance chinoise ?

- Cinq officiers chinois « wanted » pour piratage
- Une première réunion internationale pour réguler l'usage des « robots tueurs »
- Une fondation pour soutenir les lanceurs d'alerte