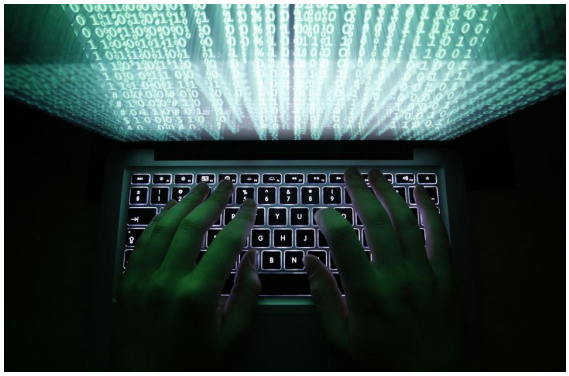
Existe-t-il un droit de la cyberguerre ?

Existe-t-il un droit de la cyberguerre ?

Le ministère de la Défense récuse l'avoir organisé en urgence, mais ce colloque tombe à pic. Les 2 et 3 novembre 2015, le nouveau site de Balard, «l'Hexagone», accueille une série de conférences sur le thème «Droit et Opex» (opérations extérieures, la guerre donc), autour de deux thèmes clés : la judiciarisation croissante des conflits et l'adaptation du droit aux nouvelles menaces, aux «zones grises».



A l'instar des bombardements français en Syrie dont la légalité a soulevé de nombreuses questions.
Ces bombardements se sont accompagnés d'actions d'un nouveau genre. Selon Le Monde, «une opération informatique du cybercommandement de l'état-major» a permis de «remonter jusqu'au groupe» visé.
Soit une nouvelle application de la doctrine française en matière de «lutte informatique offensive», dans un cadre légal encore flottant.

Pourquoi la question se pose aujourd'hui ?
«La France dispose de capacités offensives [en matière informatique]», a tonné le ministre de la défense, Jean-Yves Le Drian, fin septembre, lors d'un autre colloque, consacré au «combat numérique».
Le message était clair : la France ne se contente pas de se défendre, elle attaque.
La décision n'est pas nouvelle. Le livre blanc de la Défense de 2008 poussait déjà à l'acquisition de moyens d'attaque, un souhait réitéré cinq ans plus tard à dans le nouveau livre blanc.
En 2013, l'exécutif plaidait ainsi pour «un effort marqué» en matière de cyberdéfense militaire : «Les engagements de coercition seront conduits de façon coordonnée dans les cinq milieux (terre, air, mer, espace extra-atmosphérique et cyberespace).»

Un nouveau champ de bataille est né.
« La guerre de demain devra combiner le cyber avec les autres formes de combat », écrit Le Drian dans le numéro de novembre de la Revue Défense Nationale.
«Pour nos forces armées, le premier enjeu est désormais d'intégrer le combat numérique, de le combiner avec les autres formes de combat.» L'attaque est ainsi devenue une priorité en France, mais pas seulement.
La prise de conscience de 2008 est provoquée par une série d'événements : les cyberattaques contre l'Estonie au printemps 2007 lors d'un différend diplomatique avec Moscou, un scénario similaire un après lors de la guerre entre la Géorgie et la Russie, la découverte en 2010 du virus Stuxnet développé pour saboter certaines installations nucléaires iraniennes…
Les Etats-Unis adaptent rapidement leur doctrine. En 2011, le Pentagone annonce se réserver la possibilité de répondre par des moyens conventionnels à une cyberattaque. Cette année, le Pentagone a revendiqué ouvertement mener des cyberattaques dans la nouvelle mouture de sa «cyber stratégie».

Le droit international peut-il s'appliquer ?
La militarisation croissante du cyberespace a mené à une première vague de travaux visant à encadrer ce nouveau recours à la force. Une réflexion a ainsi été lancée par des experts au sein de l'Otan après les attaques contre l'Estonie, pour aboutir, en 2013, au Manuel de Tallinn. Le texte reconnaît que le droit international s'applique aux conflits dans le cyberespace et le décline en 95 règles.
Une opération cyber est ainsi «une agression armée lorsque l'emploi de la force atteint un seuil élevé en termes de degré, de niveau d'intensité et selon les effets engendrés : pertes en vies humaines, blessures aux personnes ou des dommages aux biens.»
La définition est cruciale, puisqu'elle conditionne l'invocation de la légitime défense, donc le recours licite à la force. D'autres principes sont aussi déclinés à propos des cibles, de l'intensité des attaques…

Existe-t-il un consensus entre les Etats ?
Le Manuel n'est que le fruit d'un travail otanien, non contraignant. Une autre démarche, sous l'égide des Nations Unis, a donné des résultats cet été. Un groupe d'experts gouvernementaux a rédigé un rapport visant à prévenir une escalade en cas d'incident. «Il faut faire ce travail avant qu'un vrai pépin existe. Est-ce que ce sera respecté ? Au moins, ces normes sont là» défend le Quai d'Orsay.
Toutes les parties l'ont endossé, représentants chinois et russes compris, alors que le consensus n'a pas prévalu tout au long des négociations, loin s'en faut.
Elles n'ont abouti que deux minutes avant la fin de la dernière rencontre, le 26 juin 2015, peu avant 18h… Les discussions bloquaient sur l'application concrète du droit international au cyberespace. «Les Chinois ne voulaient pas que le droit international humanitaire s'applique, explique le Quai d'Orsay, leur argument phare était : si on codifie les conflits armés dans le cyberespace, alors on les encourage.»
La légitime défense sera retirée du rapport, «elle n'apparaît que dans une référence très indirecte» précise-t-on au ministère des Affaires Etrangères. Sont reconnus «les principes d'humanité, de nécessité, de proportionnalité et de discrimination [entre les combattants et les non-combattants].» Les experts gouvernementaux se sont surtout accordés sur des «normes de comportements» : absence d'attaque contre les infrastructures critiques ou les «équipes d'intervention d'urgence», coopération entre Etats pour renforcer la sécurité des systèmes essentiels.
Plus surprenant, les Etats «devraient s'attacher à prévenir l'utilisation de fonctionnalités cachées malveillantes». Un engagement pour le moins surprenant de la part de Washington, également coauteur du rapport, alors que les Etats-Unis se sont fait une spécialité d'introduire des «backdoors», des portes dérobées, dans certains produits… «Toutes les questions relatives à l'espionnage sont exclues du périmètre du travail du groupe» justifie le Quai d'Orsay.
Un deuxième Manuel de Tallinn sera publié en janvier 2016. Il ne devrait pas traiter le domaine conflictuel. Au niveau européen, les discussions se concentrent sur la protection des données personnelles. Un thème remonté dans l'agenda politique après une décision récente de la Cour de justice de l'UE et surtout les révélations d'Edward Snowden sur l'ampleur de la surveillance dans les démocraties.

Réagissez à cet article
Source : http://www.liberation.fr/futurs/2015/11/03/existe-t-il-un-droit-de-la-cyberguerre_1410778