# Cyber attaques, actes de guerre ?

***Patricia Okouda***
***Master Management du Risque***
***Institut Léonard de Vinci***
*patriciaokouda@yahoo.fr*

## Les cyberattaques subies depuis quelques années, par les nations ou par les entreprises, peuvent-elle constituer un acte de guerre ? Ces nations ou ces entreprises sont-elles en droit de riposter par d'autres cyberattaques ?

Pour l'opinion publique, la guerre est un synonyme de conflit armé.

Le droit international humanitaire est un ensemble de règles internationales d'origine conventionnelle ou coutumière qui visent à limiter les séquelles des conflits armés. Il protège les individus qui ne participent pas aux combats et restreint les moyens et méthodes de guerre.

Il fait partie du droit international qui régit les relations interétatiques. Les quatre Conventions de Genève de 1949 et leur premier Protocole additionnel de 1977 composent les principaux traités applicables aux conflits armés internationaux. Quelques éléments d'éclaircissement sur la notion de conflit armé sont apportés par l'article 2 commun aux Conventions de Genève de 1949 et l'article 1 du Protocole additionnel II.

Mais ce n'est qu'à partir de 1995 qu'une véritable définition est née. En effet, lors du procès de Dusan Tadic, une décision du Tribunal pénal international pour l'ex-Yougoslavie a produit une définition claire d'un conflit armé. Cette juridiction a considéré qu'un « conflit armé existe chaque fois qu'il y a recours à la force armée entre États ou un conflit armé prolongé entre les autorités gouvernementales et des groupes armés organisés ou entre de tels groupes au sein d'un État ».

Les conflits armés internationaux sont définis à l'article 2 commun aux Conventions de Genève de 1949. Cet article indique que la Convention s'applique en cas de « guerre déclarée ou de tout autre conflit armé surgissant entre deux ou plusieurs États, même si l'état de guerre n'est pas reconnu par l'une ou l'autre des parties ». Il est de ce fait sous-entendu qu'une déclaration de guerre n'est pas indispensable pour la qualification d'un conflit en conflit armé international.

Or, une cyberattaque est un acte malveillant envers un dispositif informatique via un réseau cybernétique. Elle peut provenir de groupements de pirates informatiques, d'organisations terroristes, d'escrocs isolés mais aussi d'armées et d'organisations

gouvernementales. Les ordinateurs et l'internet sont utilisés afin de neutraliser, c'est- à-dire comme une arme.

Au vu de ces éléments, les cyberattaques peuvent constituer un acte de guerre.

Depuis quelques années, ce type d'attaques pullule dans le monde. En novembre 2010, le site internet de la Royal Navy, marine britannique, a été victime d'une attaque revendiquée par un groupe de hackers roumains, appelé TinKode. La technique utilisée par les pirates est appelée attaque par injection SQL : elle exploite la faille d'une application pour obtenir l'accès à des informations sensibles.

En mai 2011, Lockheed Martin, entreprise importante du secteur de l'armement aux États-Unis, subit une cyberattaque massive dont l'origine n'est toujours pas officiellement connue. Tous les systèmes informatiques de la société ont été bloqués pendant plusieurs heures et tous ses codes de sécurité ont été subtilisés.

Un mois plus tard, plusieurs centaines de comptes Gmail appartenant à des hauts fonctionnaires américains, des rebelles chinois, des responsables de plusieurs pays asiatiques, des militaires et des journalistes ont été piratés. Selon Google, cette cyberattaque vient de Jinan où sont localisés un commandement militaire chinois et une école formée avec l'appui de l'armée, qui avait déjà été accusée d'avoir pénétré les serveurs de Google l'année précédente.

L'été 2012, sur une période de soixante jours, près de quatre-vingts millions de dollars sont dérobés dans une série de cyberattaques touchant des banques européennes mais aussi nord-américaines et sud-américaines.

Mais la première cyberattaque recensée ciblant une structure étatique durant plusieurs semaines s'est passée en Estonie. Dès le 27 avril 2007 et pendant plus d'un mois, les sites gouvernementaux, des banques et des médias ont enduré des attaques les rendant inaccessibles. La plupart des institutions estoniennes ayant opté pour une bureaucratie sans papier, intégralement informatique et reliées entre elles par l'internet, ce pays se trouve très vulnérable à ce type d'attaques. Se protéger contre ces cyberagressions a été très onéreux tant pour le gouvernement de l'Estonie que pour les entreprises du secteur privé qui avaient été ciblées.

Le procédé d'attaque consistait à connecter un maximum d'appareils à un seul réseau et ainsi provoquer une saturation de celui-ci. Cette méthode du botnet est fréquemment utilisée pour sa discrétion en terme de traçabilité. Elle est pilotée par une personne unique contrôlant plusieurs ordinateurs contaminés par celle-ci. Comme il y a une abondance d'appareils, le choix du traçage IP est à écarter.

Étant donné les techniques très compliquées employées lors de ces attaques, seul un groupe organisé possédant un large soutien financier a pu accomplir une telle action. Il est admis par le gouvernement d'Estonie et par plusieurs experts en sécurité cybernétique qu'un réseau de pirates mené et financé par le Kremlin est à la source de ces attaques.

Des blogs russes avaient été utilisés pour convier des pirates patriotiques à aider à punir l'Estonie après la décision du gouvernement estonien de déplacer la statue d'un soldat de l'Armée rouge, symbole de plus de cinquante ans de tutelle soviétique.

La défense choisie par l'Estonie a d'abord été d'augmenter les capacités de trafic des sites internet pour faire face au flux massif de connexions. Par la suite, les connexions vers le réseau extérieur ont été détournées, ce qui revient en quelque sorte à débrancher l'Estonie de l'internet.

Un simple technicien, et non le gouvernement, a pris l'initiative de suspendre l'accès internet du pays pour faire face à l'attaque.

Comme nous l'avons vu précédemment, ces cyberattaques ont des conséquences colossales. Il ne s'agit pas de spéculer sur la solution miraculeuse d'un individu, comme ce fut le cas en Estonie, mais plutôt sur les politiques de réponses des nations.

Ont-ils le droit de recourir à la force armée ?

Il existe un principe d'interdiction du recours interétatique à la force armée. Les Nations Unies règlent en principe pacifiquement et de manière consensuelle les conflits. La Charte des Nations Unies dispose ainsi dans son article 2 paragraphe 4 que : « les membres de l'Organisation s'abstiennent, dans leurs relations internationales, de recourir à la menace ou à l'emploi de la force, soit contre l'intégrité territoriale ou l'indépendance politique de tout État, soit de toute autre manière incompatible avec les buts des Nations Unies ».

L'article 51 de la Charte des Nations Unies rappelle cependant une exception à ce principe : la légitime défense. Dans ce cas, le pays agressé pourra agir à sa guise, jusqu'à l'intervention du Conseil de sécurité, et dans la mesure où sa réaction est proportionnelle à l'agression subie.

Le principe de la sécurité collective est un autre argument soulevé pour lancer une attaque. Selon l'article 5 du Traité de l'Atlantique Nord signé à Washington, « les parties conviennent qu'une attaque armée contre l'une ou plusieurs d'entre elles survenant en Europe ou en Amérique du Nord sera considérée comme une attaque dirigée contre toutes les parties, et en conséquence elles conviennent que, si une telle attaque se produit, chacune d'elles, dans l'exercice du droit de légitime défense, individuelle ou collective, reconnu par l'article 51 de la Charte des Nations Unies, assistera la partie ou les parties ainsi attaquées en prenant aussitôt, individuellement et d'accord avec les autres parties, telle action qu'elle jugera nécessaire, y compris l'emploi de la force armée, pour rétablir et assurer la sécurité dans la région de l'Atlantique Nord. Toute attaque armée de cette nature et toute mesure prise en conséquence seront immédiatement portées à la connaissance du Conseil de sécurité. Ces mesures prendront fin quand le Conseil de sécurité aura pris les mesures nécessaires pour rétablir et maintenir la paix et la sécurité internationales ».

Les nations, et non les entreprises, semblent donc avoir le droit de riposter par d'autres cyberattaques.

Pour une société victime d'un hacker, il existe des recours juridiques pour punir le voleur et obtenir réparation. En matière de vol de données, la loi Godfrain du 5 janvier 1988 érigeant une répression globale de la criminalité informatique, dispose que « le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans de prison et de 45 000 mille euros d'amende ».

Les établissements touchés par le piratage peuvent de ce fait se tourner vers la justice pour tenter d'obtenir réparation.

En l'état actuel des choses, il paraît sensé d'examiner la capacité d'un pays à conduire des attaques informatiques au même titre que de lancer des armes de destruction massive. Les cyberattaques sont bien désormais un élément de dissuasion sur l'échiquier mondial de la géopolitique. Étant donné les forces en présence et les pays impliqués, ces cyberattaques ne déboucheront vraisemblablement jamais sur une déclaration de guerre traditionnelle par les armes matérielles.

Néanmoins, Il conviendrait d'approfondir les problématiques de moralité et surtout d'escalade plus ou moins démesurée des ripostes qu'engendrent ces cyberattaques.