**NA C1.2**

**ACTIVITÉ DE MÉDIATION ORALE :**

**Comme membre d’une association pacifiste, vous participez à des interventions dans les centres scolaires pour encourager la prise de conscience contre les guerres et en particulier contre les cyberguerres.**

**Après avoir lu le texte ci-dessous, vous devez faire un petit exposé oral sur le concept de cyberguerre et ses principales caractéristiques à un groupe d’étudiants de 13 à 14 ans.**

**10 minutes de préparation et 2 minutes d’exposé oral.**

**La définition de la « cyberguerre »**

Des débats ont été menés sur l’expression même de la « cyberguerre ». Peut-on employer le mot « guerre » dans un contexte cyber ? La difficulté est liée à la conception traditionnelle de la guerre : Elle implique un conflit armé sur un théâtre d’opération, menaçant possiblement des vies humaines [6]. Est-ce que cette conception est adaptée aux actes offensifs d’espionnage et de sabotage menés dans le cyberespace ?

Le professeur Thomas Rid par exemple a publié un article scientifique controversé en 2011 et deux ans plus tard un livre du même titre provocatif : « *Cyber war will not take place* » (la cyberguerre n’aura pas lieu) [7]. Selon lui, il n’y avait pas encore de cyberguerre et il n’y en aura pas dans le futur. Il admet que des cyberattaques peuvent revêtir une certaine violence, mais que celle-ci serait toujours restreinte par sa nature inhérente indirecte. [8] Finalement, les actes de la cyberguerre ne constitueraient que des versions plus sophistiquées des conduites de la guerre classiques (sabotage, espionnage et subversion).

Force est de constater que, jusqu’à aujourd’hui, on n’a pas encore vécu une cyberguerre « autonome ». Les cyberattaques sont déjà une réalité concrète, mais comme on verra plus tard, elles s’intègrent toujours dans un contexte plus large d’un conflit étatique classique, armé ou non. La « cyberguerre » n’est donc qu’un élément, qui accompagne une guerre « traditionnelle» ; c’est un mode d’action parmi d’autres qui fait partie de la stratégie des parties au conflit et qui a le potentiel de bouleverser la conduite de la guerre traditionnelle [9]. Cependant, l’emploi de la notion de « cyberguerre » a un intérêt, celui-ci étant plutôt pédagogique. Il est facilement accessible et permet au large public de se rendre compte des enjeux importants liés à l’utilisation des technologies modernes. [10]

Quel est donc le contenu d’une action, qu’on peut qualifier comme « cyberguerre » ? Les attaques informatiques peuvent prendre des formes diverses – or, toute attaque ne constitue pas *ipso facto* une attaque de cyberguerre. La notion de « cyberguerre » doit être lue de manière restreinte et distinguée d’autres catégories d’attaques informatiques, qui sont d’une ampleur moins importante ou poursuivent d’autres buts. Suivant la proposition du « *Center for Security Studies Zürich* », on peut ainsi classer les attaques informatiques en fonction de leur objectif et de la gravité de leurs effets [11] : Il y a des actes de *cyberhacktivisme* (la modification ou la destruction du contenu en piratant un site web) ou de *cybercrime* et *cyberespionnage*(visant notamment le secteur privé des grands entreprises), qui ne ciblent à priori pas directement un Etat et ne se déroulent pas dans le cadre d’un conflit interétatique.

Or, un Etat peut être affecté par des actes de *cyberterrorisme* (une attaque menée par un acteur non-étatique afin d’intimider le gouvernement et la population d’un pays, causant un dommage concret dans le monde réel) et par l’attaque la plus grave, la *cyberguerre*. Cette dernière met directement en cause l’intégrité et la sécurité d’un Etat, de sa propriété et de ses citoyens [12].

Si on est face à une cyberguerre, celui-ci vise toujours à déstabiliser l’adversaire dans sa maîtrise de l’information. L’information est donc « le centre de gravité du conflit » et elle peut être manipulée de trois manières [13] :  en perturbant et interrompant le fonctionnement des systèmes informatiques ou en falsifiant leur contenu (guerre contre l’information) ; en récupérant des informations, donc par des actes d’espionnage comme dans le cas récent de l’attaque contre le gouvernement allemand (guerre pour l’information) ; et dernièrement, en manipulant les systèmes informatiques afin de faire de la propagande ou diffuser par exemple des fausses informations (guerre par l’information). Sans rentrer dans les détails techniques, ces modes d’actions sont mis en œuvre soit par un déni de service (la saturation d’un serveur par un grand nombre de demandes instantanées, afin de provoquer son inaccessibilité), soit par la récupération ou modification des données confidentielles (par exemple par un cheval de Troie) [14].

**Les difficultés liées aux réponses à la cyberguerre**

Comment les Etats peuvent-ils faire face à la cyberguerre ? La réponse à cette question nécessite de s’interroger d’abord sur les difficultés et limites de la lutte contre la cyberguerre, qui sont le produit des particularités de ce type de conflit.

La difficulté majeure de la cyberguerre, c’est qu’il est extrêmement difficile d’identifier son auteur. Les attaquants peuvent facilement brouiller leurs pistes en ayant recours à des serveurs relais, ce qui rend l’imputabilité d’un acte à son acteur presque impossible. Concernant les incidents en Estonie et Géorgie, on soupçonne que les attaques étaient menées par des hackeurs russes, sans être capable de prouver leur identité de manière certaine [21]. Deuxièmement, une cyberguerre peut aussi être de nature « asymétrique », opposant donc un Etat à un acteur non-étatique. Ces derniers agissent de manière autonome, sans être contrôlés par un Etat. Comment identifier les buts qu’ils poursuivent et comment leur imposer des représailles effectives ? [22]

Cependant, l’enjeu de savoir comment répondre à une cyberguerre est d’une importance majeure: Une cyberguerre peut avoir non seulement des conséquences directes dans le monde virtuel, mais aussi des effets considérables dans le monde réel. Il y a donc un risque des effets « en cascade » [23]. Afin d’empêcher ce risque de se réaliser, un Etat peut soit adopter une stratégie plutôt défensive (développer des logiciels antivirus, respecter des règles de sécurité…), soit une stratégie offensive (rechercher et développer des armes virtuelles lui-même). [24] Le domaine est tellement jeune, que les organismes et stratégies ne sont qu’en train de se mettre en place. En France, par exemple, il existe depuis 2009 l’ANSSI (l’Agence Nationale de la Sécurité des Systèmes d’Information), agissant dans une perspective défensive et surtout dans le domaine civil en cas d’attaque des systèmes informatiques français [25]. L’OTAN a créé le « *centre d’excellence de cyberdéfense coopérativ*e » à Tallinn, qui a pour mission d’améliorer les capacités et la coopération entre les pays membres en domaine de la cyberdéfense. [26] Les Etats-Unis sont plus offensifs dans leur stratégie et ont créé en mai 2010 le « *US Cyber Command* », ce qui marque l’entrée officielle de la cyber stratégie dans les forces armées [27].

*Source : Ecrit par Maren Rimbach* *http://www.isd.sorbonneonu.fr/* *17 mars 2018*