MODEL UNITED NATIONS FRANCE

MARCH 16TH-18TH | STRASBOURG

DISEC

DÉSARMEMENT ET SÉCURITÉ INTERNATIONALE

STUDY GUIDE

Réguler les actes de Cyberguerre

Strasbourg, Mars 2018

Model United Nations France
Stras'Diplomacy
47 avenue de la Forêt-Noire
67000, Strasbourg, France
Web: www.munfrance.com

Auteurs: Agathe Courtet, Renaud Mouzin

Design graphique: Corentin Martin-Loos, MUN France

Table des matières

L'Assemblée Générale des Nations Unies – Première Commission – Désarmement et Sécurité Internationale

La Première Commission traite des questions de désarmement et de sécurité internationale. Elle a été créée avec pour fonction de formuler des recommandations dans le domaine du désarmement. Chaque année, à l'issue de ses délibérations, elle transmet ses recommandations à l'Assemblée Générale, dont elle est un organe subsidiaire, au même titre que les cinq autres Grandes Commissions, afin que tous les états membres puissent voter de nombreuses résolutions sur les thèmes qu'elle aborde, allant de la lutte contre la prolifération nucléaire jusqu'au contrôle de la démilitarisation de l'espace extra-atmosphérique.

Il est toutefois à noter que les résolutions adoptées en Assemblée Générale ne disposent aucunement de pouvoir coercitif. A ce titre les états ne peuvent pas imposer une ligne directrice ou même des sanctions à l'intérieur de celles ci, à la différence du Conseil de Sécurité des Nations Unies.

Introduction à la cyberguerre

"La cyberguerre est bien déclarée", Hamadoun Touré, Secrétaire Général de l'Union Internationale des Télécommunications (UIT)

Si la cyberguerre se caractérise par des affrontements en réseau entre certains pays, associations ou individus, il parait extrêmement compliqué de la cerner précisément : comment définir et poursuivre la cyberguerre si elle ne se manifeste pas, comme la plupart des guerres classiques, sous forme de violence armée ou si elle n'est pas dirigée par des groupes politiques ? A ce titre, certains expliquent, comme Michel Baud, qu'il n'y a en France pas de véritable définition de la cyberguerre, allant même jusqu'à penser qu'il s'agisse d'un terme « fourre-tout ». A contrario, et de manière sans doute plus empirique, le Général Marc Watin-Augouard écrit dans l'introduction du livre « La première cyber-guerre mondiale ? » que celle ci se caractérise par l'introduction des armes cybernétiques dans la conduite de la guerre, c'est à dire la « guerre via le cyber ». Cette analyse vient ainsi trouver un point d'encrage sans doute plus concret dans les rapports de force actuels impliquant une puissance tout au moins régionale. C'est à cet effet que l'on pourrait éventuellement appliquer à la cyberguerre tout un domaine juridique tel qu'explicité plus tard dans ce Study Guide, dans la 6ème partie.

Quoiqu'il en soit l'ONU, sous l'égide des états, ne saurait donner une définition claire et précise de ce qu'est la cyberguerre, sans aucun doute du fait de la réticence des puissances mondiales elles mêmes à qualifier des actes qu'elles seraient susceptibles de reproduire et dès lors de leur peur que soient intégrés aux actes de guerre ceux du domaine cyber, ces premiers étant largement encadrés et condamnés par le Chapitre VII des Nations Unies.

On ne peut évoquer la cyberguerre sans parler des TIC (Technologies de l'Information et de la Communication) qui constituent tous les instruments de communication tels que la télévision, le téléphone, les ordinateurs et réseaux privés, publics ou venant de satellites. Ces instruments technologiques sont utilisés pour communiquer mais aussi pour organiser, accumuler ou créer des informations qui constituent la richesse d'une entreprise, d'un individu ou d'une nation entière. Une cyberattaque touche forcément un réseau TIC, tout ceci

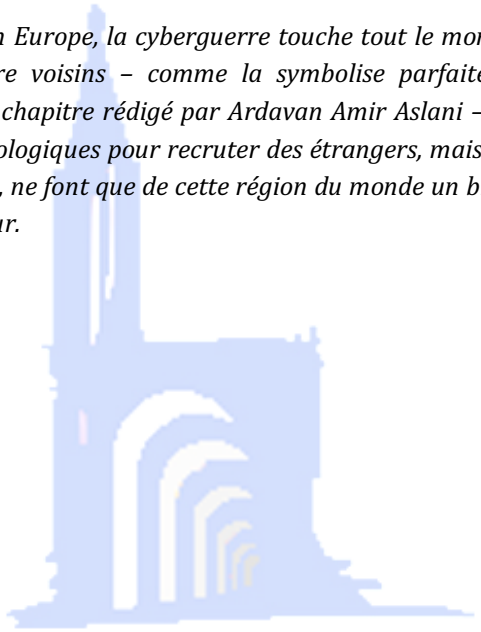
sachant que plus de 3,5 milliards de personnes utilisent l'Internet (avec un taux de pénétration de 81% dans les pays développés) selon l'UIT, organisation des Nations Unies spécialisées dans les TIC, dans un rapport de 2016, sans prendre en compte les pays sous développés dans le calcul.

Pour contrer les cyberattaques, certains pays membres ont créé individuellement des services de cybersécurité. La cybersécurité peut être définie comme la mise en place de systèmes technologiques visant à protéger les ordinateurs, réseaux, programmes ou données d'éventuelles cyberattaques ayant pour but de les endommager, de les voler ou de les vendre. On qualifie les cyberattaques d'actes de cyberterrorisme lorsqu'elles sont orchestrées par des groupes politiques et non des Etats à proprement dit et qu'elles suscitent des dommages importants à l'encontre de l'Etat concerné, l'opinion publique ou bien ses citoyens quel que soit leur pays de résidence.

Il existe donc une distinction entre les cyberattaques provoquées par des Etats et celles provoquées par des organisations aux buts politiques. La lutte contre la cyberguerre s'opère grâce à des moyens de défense mis en place par des agences potentiellement spécialisées des différents états. Par des moyens de prévention ou de contre-attaques numériques, les pays tentent de riposter contre les attaques dans le cyberespace. Or la dissuasion technologique est très importante, tout comme la dissuasion nucléaire dans les guerres physiques, car les pays orchestrant des cyberattaques jouent souvent sur l'appartenance et la revendication d'un groupe de cyberterroristes à ce pays et non à une indépendance de cette organisation, assurant une riposte brutale du ou des pays visés.

La guerre informatique ne concerne plus seulement les amateurs de TIC mais elle revient sous toutes les formes, dans un contexte politique, économique et militaire, à l'échelle mondiale. D'après cette chronologie d'événements qui suit, on remarque que le front de guerre des conflits du 21ème siècle est technologique. De 2007 à nos jours, on observe autant une prise de position des hackers qui se surnomment les "hacktivistes" ou "hacker-activistes" que des attaques émanant des différentes puissances, tout au moins régionales, et sans conteste particulièrement de la Fédération de Russie, des Etats Unis d'Amérique, de la République Populaire de Chine ainsi que de l'Etat d'Israël.

Que cela soit en Asie, Amérique, au Moyen Orient ou en Europe, la cyberguerre touche tout le monde et s'accentue surtout au Moyen Orient où les oppositions entre voisins – comme la symbolise parfaitement l'opposition « Stuxnet vs Shamoon » pour reprendre le titre du chapitre rédigé par Ardavan Amir Aslani – ainsi que l'utilisation par les groupes islamistes des ressources technologiques pour recruter des étrangers, mais aussi pour lancer de puissantes cyberattaques contre leurs opposants, ne font que de cette région du monde un brasier d'autant plus susceptible de prendre encore davantage d'ampleur.



Evènements important concernant la cyberguerre : (liste non exhaustive et à lire de bas en haut)

***-8 septembre 2017** : Equifax, société de crédit américaine aux 143 millions de clients se voit piratée, laissant présager aussi bien usurpations d'identités que vols des données bancaires*

***-5 mai 2017** : A quelques heures de la fin de la campagne du second tour des présidentiels, 71 848 courriels d'En Marche ! sont piratés puis publiés par Wikileaks. Déjà précédemment durant la campagne certains sites, notamment ceux du PS et d'EM ! avaient fait l'objet de tentatives de piratage. La piste russe n'est pas formellement identifiée, ni écartée pour autant.*

***-Mai 2017** : Le rançongiciel (logiciel de chantage contre des rançons sous peine de divulgation d'éléments compromettants) Wanacry fait plus de 200 000 victimes dans 150 pays en un seul jour. Le Service national de santé britannique (NHS – National Health Service) a été touché, empêchant le bon fonctionnement des hôpitaux, comme de grandes entreprises, comme Renault ou l'opérateur espagnol Telefonica qui ont aussi été frappés.*

***-27 décembre 2016** : Piratage de l'OSCE attribué à la Russie (plus exactement l'APT28 (également connu sous les alias de Pawn Storm, Sofacy ou Fancy Bear) et réputés pour leurs liens avec les services spéciaux russes) durant le mois d'octobre, susceptible d'avoir dérobé courriers électroniques, dossiers et mots de passe. A noter que ces dossiers sont ultra-sensibles puisque l'OSCE, organisme « indépendant », participe activement au règlement des conflits est-ukrainiens.*

*-**2016** : 2 piratages lors de la campagne présidentielle américaine de certains systèmes du parti démocrate par des hackers russes : WikiLeaks publie notamment le 22 juillet une première partie des correspondances soit 44 000 emails et 18 000 pièces jointes. Des emails, notamment ceux de M. Podesta, sont publiés tous les jours à partir du 7 octobre jusqu'au jour des élections.*

***-21 octobre 2016** : Le virus Mirai qui « « enrôlait » des centaines de milliers d'objets connectés à Internet pour qu'ils mènent des attaques coordonnées » paralyse massivement le web américain, empêchant ses principaux services de fonctionner.*

***-Juillet 2016** : Le New York Times est visé par des pirates de Moscou, en vain.*

*-**2016** : Les données de 57 millions d'utilisateurs d'Uber sont piratées, ce dernier cédant 100 000 dollars aux pirates afin que ceux ci ne révèlent pas l'affaire au grand public.*

*-**11 janvier 2015** : Le groupe Fallaga, se présentant comme un groupe de "cyber activistes", pirate plusieurs sites web d'organisations, de commerces, de collectivités ou d'établissements scolaires français.*

*-**2 janvier 2015 :** Deux millions d'abonnés du site de TF1 voient leurs données piratées par des hackers détenant leur RIB et d'autres informations sensibles.*

*-**26 décembre 2014 :** Les sociétés PlayStation et Xbox sont victimes d'une panne après une cyberattaque. Les joueurs ne peuvent plus se connecter aux services en ligne PlayStation et Xbox.*

*-**21 décembre 2014 :** Des hackeurs dérobent des documents internes comme des plans de réacteurs nucléaires sud-coréens à la Korea Hydro & Nuclear Power Corporation, puis les publient sur Internet.*

*-**19 décembre 2014 :** Icann, le régulateur mondial d'internet, annonce que des pirates informatiques ont réussi à pénétrer dans leurs ordinateurs.*

*-**18 décembre 2014 :** Une usine métallurgique allemande subit une cyberattaque provoquant de lourds dégâts matériels*

*-**18 décembre 2014** : Icann est victime d'un piratage informatique*

*-**Décembre 2014 :** La Corée du Nord (DPRK) est soupçonnée d'avoir menée une cyberattaque contre l'entreprise Sony par la CIA.*

*-**9 octobre 2014 :** Ulcan, hacker franco-israélien revendique un piratage des sites internet des chaînes d'information France-Info et France-Inter.*

*-**2 octobre 2014 :** JP Morgan Chase annonce que 76 millions de foyers et 7 millions de PME parmi ses clients ont été piratés lors d'une attaque informatique dans le courant du mois d'août de la même année.*

*-**Aout 2014** : Révélation quant au virus Snake qui aurait infiltré les bureaux du 1er ministre ukrainien. Une soixantaine d'ordinateurs auraient aussi été infectés depuis 2012 rendant accessible la totalité de leur système, touchant notamment des ambassades ukrainiennes. Attaque imputée à la Russie.*

*-**11-17 juillet 2014** : Plus de 1000 sites internet israéliens (dont 10 ministères) sont hackés. Anonymous évoque une opération appelée #OpSaveGaza.*

*-**16 Mars 2014** : Alors qu'il s'agit du jour du référendum quant à l'autodétermination de la Crimée, le site créé par les autorités séparatistes pour suivre le scrutin a été bloqué. Un peu plus tôt, c'est le site de l'OTAN qui fut attaqué par le groupe CyberBerkout (supposé être plus ou moins directement téléguidé par le Kremlin) et inaccessible plusieurs heures durant.*

*-**12 février 2014 :** Une attaque par déni de service frappe de multiples serveurs aux Etats-Unis et en Europe. C'est la plus grande attaque informatique par déni de service la recensée à ce jour.*

*-**27 novembre 2013** : La chaîne américaine de grande distribution Target est victime d'une attaque informatique lors de laquelle des hackeurs se sont procurés les coordonnées bancaires de plus de 40 millions de personnes.*

*-**15 février 2013 :** Facebook subit une attaque informatique d'envergure, cependant Facebook assure que les données personnelles des utilisateurs n'ont pas été compromises. Le réseau social avait alors annoncé : "Nous avons remédié au problème dans tous les appareils infectés, nous avons informé la police et commencé une vaste enquête qui se poursuit à ce jour".*

*-**2 février 2013 :** Twitter est touché par une vague d'attaques informatiques. Ils n'admettrons finalement qu'en octobre 2017 que l'ensemble des 3 milliards de comptes furent touchés. Plus encore, sur 4 personnes poursuivies par les USA dans cette affaire, 3 sont russes dont 2 travaillant directement au sein du FSB.*

*-**Septembre 2012 :** Six grandes banques américaines sont victime d'une attaque à l'aide d'un virus développé par un group de hackers antisionistes. En octobre le même virus a attaqué une grande banque française.*

*-**Aout 2012 :** Aramco, un groupe pétrolier d'Arabie Saoudite, révèle avoir été victime d'une attaque informatique d'envergure. Ainsi, 30 000 postes informatiques de l'entreprise ont été infectés par un virus informatique extérieur, les détruisant et stoppant leur système durant 2 semaines. Au même moment est aussi touché la compagnie gazière Qatarie RasGas.*

*-**2011 :** Explosion d'un dépôt de missiles iranien attribuée par les médias américains à une attaque virale. En avril de la même année, l'Iran avait du déconnecter son terminal pétrolier de Kharg d'Internet suite à une cyberattaque. Cependant, la même année, les iraniens réussissent à neutraliser un satellite espion de la CIA grâce à une technologie de brouillage de pointe au laser, qui lui aurait supposément été fournie par la Russie. De même, quelques jours plus tôt, un ingénieur iranien a alors affirmé qu'ils avaient réussi à pirater la fréquence d'un drone américain et à le faire se poser au sol.*

*-**27 avril 2011 :** Sony est victime du piratage de 12 700 numéros de cartes de crédit non américaines issues d'une base de données ancienne.*

*-**07 mars 2011 :** Bercy et le Trésor sont victimes d'une opération de piratage informatique d'envergure. Plus de 150 ordinateurs du ministère sont alors infiltrés et des documents piratés. La méthode des espions est classique et suit la logique du virus 'Cheval de Troie'.*

*-**2011 :** Cyberattaque contre de nombreux sites internet et réseaux gouvernementaux japonais. De plus, un virus réussit à infecter les postes de contrôle de drones américains déployés en Afghanistan.*

*-**Septembre 2010 :** Stuxnet et Flame, 2 virus conçus par les Américains et Israéliens, s'attaquent à des centaines de centrifugeuses iraniennes situées dans les centrales nucléaires de Natanz et Bouchehr dans le but de produire des effets analogues à ceux d'un bombardement.*

*-**Mars 2010 :** Google Chine s'écroule.*

*-**12 janvier 2010 :** Google menace de quitter la Chine à cause d'agressions informatiques massives envers des chinois militants pour les droits de l'homme.*

*-**2010 :** Fidèles au concept de « guerre hors limites » développé par les colonels Qiao Liang et Wang Wiangsui, l'opération "Shadow Network", perpétrée par la Chine, a lieu. Cette cyberattaque de grande envergure permet à la Chine de voler des informations classifiées à l'Inde mais aussi à l'Office du Dalaï Lama.*

*-**Octobre 2007 :** Opération Orchard : un virus israélien s'attaque aux systèmes de défense de la Syrie, les rendant dysfonctionnels afin d'apporter à Tsahal plus de sécurité lors de leur attaque du réacteur nucléaire syrien d'Al-Kibar.*

*-**27 avril 2007 :** Cyberguerre en Estonie. Le pays fut entièrement paralysé. Cette offensive aurait été lancée par la Russie qui durant plusieurs semaines a lancé des attaques par déni de service (DdOS), bloquant les sites gouvernementaux, les banques, les médias, les services d'urgence, etc. De même 85 000 ordinateurs ont été piratés.*

*-**2006 :** L'opération "Shady RAT" a lieu. Il s'agit d'une série d'attaques informatiques qui touchent de nombreuses organisations, dont l'ONU, des administrations américaines et notamment son industrie d'armement. Plus de 70 organisations auraient été touchées, l'attaque ayant supposément duré plus de 5 ans.*

*-**2003 :** L'opération Titan Rain est une série de cyberattaques sur le système informatique Américain qui aurait duré 3 ans, visant principalement des organismes variés, notamment militaires, ou les contractuels y étant affiliés.*

Situation actuelle

Lorsque l'on observe la chronologie de la cyberguerre, on remarque qu'elle ne fait que s'aggraver de jour en jour. Alors que les conflits éclatent au Moyen-Orient et en Europe de l'Est, la cyberguerre se manifeste elle aussi, tantôt en tant qu'outil de ces mêmes guerres, tantôt, à contrario, en tant que discrète et impunie menace d'une superpuissance envers une autre. Cette guerre technologique et non physique se base sur l'information, la censure et le contrôle d'interfaces publiques. Les hackers tentent de faire passer des messages aux groupes de personnes ou états qu'ils visent. Le fait de s'introduire dans un réseau privé, de s'emparer d'informations confidentielles, de faire ressortir une faille dans les systèmes de sécurité nationaux montre une vulnérabilité des gouvernements à protéger leurs données. Certains choisissent de fermer leurs portes en bloquant l'accès à certains sites internet, comme la République Populaire de Chine, tandis que d'autres ripostent et tentent de localiser l'origine de ces cyberattaques, c'est le cas par exemple des États-Unis.

En effet, alors que certains Etats se concentrent sur une approche offensive, la Chine est connue pour son système de censure et de surveillance, plus préventif. Le Great Firewall, ou Grande Muraille virtuelle est constituée d'une multitude de filtres qui bloquent l'accès à des sites, et particulièrement aux réseaux sociaux, en raison de leur contenu. Le département central de la propagande du parti liste les sujets interdits, à charge pour les portails d'information ou la presse de faire preuve d'autocensure sous peine de sanctions (suspension de la licence ou du site internet par exemple). Des dizaines de milliers de cyberpoliciers patrouillent le web à la recherche d'infractions afin de sanctionner et de procéder à la suppression des informations. Ils sont assistés de « commentateurs », chargés de propager la bonne parole du gouvernement dans les discussions en ligne. Réputé infranchissable, la Grande Muraille virtuelle connaît pourtant ses failles : en mars 2016, Google avait réussi à contourner le pare-feu national, bien qu'involontairement, pendant plus de deux heures. L'incident a cependant permis de démontrer la réactivité des autorités chinoises. La Chine connaît cependant elle aussi des outils plus offensifs : des chercheurs ont découvert en 2015 l'existence de ce qu'ils ont nommé le « Great Cannon », ou Grand canon. Le système a permis de mener des cyberattaques paralysantes envers plusieurs sites œuvrant pour la liberté de l'internet chinois. Le Grand canon bloque le trafic afin de lancer des attaques contre un lot très spécifique d'adresses ; mais pourrait aisément être utilisé à des fins plus néfastes.

La situation, au plan des négociations internationales, stagne depuis quelque temps car malgré les efforts des Nations Unies pour proposer des résolutions sur ce conflit, les Pays membres ne collaborent que sur certains points et, n'ayant pas les mêmes manières de procéder, il peut tout simplement être difficile pour les services secrets nationaux et internationaux de collaborer, si ce n'est par pure mauvaise foi et bellicisme que cette coopération est plus qu'imparfaite.

Ainsi, la course à l'armement est lancée à l'échelle internationale, et la question du contrôle des cyberarmes anime les discussions entre Etats, l'idée étant de tarir les potentiels conflits à la source. Il existe certains outils, tels que l'arrangement de Wassenaar signé en 1996 qui prévoit un contrôle des biens et technologies « à double usage », utilisés à des fins belliqueuses comme pacifiques ; or seuls 41 pays en sont signataires. Des outils supplémentaires sont donc nécessaires. Une autre éventualité a fait l'objet de discussions afin de dissuader les attaques : la possibilité d'un « hack back », constitutive d'une réponse privée, rapide efficace des sociétés face à leurs cyberattaquants. Elle permettrait aux entreprises de récupérer les données dérobées mais aussi de s'attaquer aux infrastructures adverses. Un autre de ses avantages serait son cadre assez confidentiel. Or selon David Martinon, haut fonctionnaire français, «Une telle riposte privée constitue un facteur de forte déstabilisation, voire d'anarchie. (…) Cela revient à faire du second amendement de la constitution américaine une règle de droit international. Et donc d'inciter tout le monde à s'armer.»

Acteurs impliqués (pays, organisations, individus)

La cyberguerre est évidemment une guerre mondiale touchant la plupart des pays. Il est toutefois à constater qu'une autrement plus majeure implication des pays du Conseil de Sécurité (France, Royaume Uni, Etats Unis, Chine et Russie) domine le domaine cyber. L'importance de certains autres pays n'est toutefois aucunement à négliger, à commencer par l'Israël ou l'Inde, la Corée du Nord, le Canada, le Pakistan, Taiwan, l'Afrique du Sud, le Brésil, le Mexique, etc.

Les actes de cyberguerre, souvent orchestrés par des organisations politiques mais non nécessairement supervisés par leurs gouvernements, sont les principaux acteurs de ce conflit. Les Pays Membres, eux, encaissent les cyberattaques touchant leur gouvernement, leurs citoyens, leur économie ou leurs entreprises.

Des Organisations non-gouvernementales sont aussi impliquées dans la cyberguerre. Cyber Peace Foundation est par exemple la principale organisation traitant le problème. Mais aussi de nombreuses autres s'attèlent à s'imposer dans ce domaine, telles que que HANS, Larson Security ou NGO Pulse.

Les organisations responsables des cyberattaques peuvent varier, fluctuant d'individuels tel qu'Ulcan, hacker franco-israélien ultra-sioniste, de groupes affiliés à des régions, comme Fallaga, groupe de hackers tunisiens, ou encore des organisations internationales : ce sont le cas des Anonymous, ou dans un tout autre domaine d'action, Al-Quaïda ou ISIS

Des organisations gouvernementales sont susceptibles de lancer des cyberattaques faisant bien sûr parti des acteurs de la cyberguerre, comme la NSA (National Security Agency aux États-Unis) et bien d'autres. On considèrera ici que le gouvernement d'un pays membre à l'origine d'actes-cyber hostiles prendra l'entière responsabilité des actes de l'une de ses organisations gouvernementales.
Toutefois, outre cette vision très empirique de l'agence gouvernementale nationale « traditionnelle », se développe parallèlement des pratiques d'une toute nouvelle forme. Il s'agit en effet de la mise en place de « cyberarmées » dont l'Allemagne a été le premier des 28 pays membres de l'OTAN à mettre en place sa propre cyber armée, une force séparée au côtés de la Marine, de l'armée de Terre et de l'Air. Composée de 260 « hackers » d'élite, elle aura pour

mission d'assurer la protection des infrastructures d'armement face aux attaques informatiques. Elle comptera à terme plus de 13 500 personnes et sera pleinement opérationnelle d'ici 2021. L'initiative de l'Allemagne a rapidement été suivie. Certaines attaques, notamment le virus développé par un groupe de hackers antisionistes ayant touché une grande banque française mi octobre 2012, après avoir touché 6 grandes banques américaines, ont ici poussé la France, et parallèlement certains Etats, à réagir, et à se doter à leur tour de leur propre cyberarmée. Aujourd'hui la France compte 3200 personnes à son service dans ce domaine. La plupart des pays développés s'équipent tour à tour d'une force similaire, suivis de près par certains pays du tiers monde : c'est le cas du Bénin notamment. D'autres pays n'hésitent pas à mettre en avant le côté plus offensif de ce dispositif : c'est le cas de la Corée du Nord qui n'a elle pas hésité à affirmer qu'elle s'était dotée d'une armée de milliers de cyber-militaires capables de mener des attaques meurtrières.

Finalement, des organisations des Nations Unies comme l'ONUDA (Bureau des affaires de désarmement) ou l'ONUDC (Office des Nations Unies contre la Drogue et le Crime) militent contre la cyberguerre. Leur rôle est très limité par les pays membres et leur législation malgré de nombreuses résolutions pour leur donner plus de ressources. Europol, sur le plan européen, est quant à lui autrement plus efficace, avec un département dédié entièrement à la gestion de risques du domaine cyber.

De même, se cachent parfois derrière des « cyberterroristes » des Etats, à l'image des attaques perpétrées par différents groupes tels que Pawn Storm, The Dukes, APT28, Fancy Bear, Sofacy/Sednit Group ou encore Tsar Team visant en priorité des cibles militaires aux Etats-Unis, des objectifs en Pologne, en Géorgie, Bulgarie, Hongrie ou en Ukraine, mais aussi des journalistes américains ou des opposants à Vladimir Poutine

Importance du sujet

Il est de première importance d'aborder ce sujet autant pour son retentissement actuel incomparable que par l'évidente nécessité d'intégrer et d'encadrer ces nouvelles façons de faire la guerre, qui concerne non seulement les pays membres, mais aussi la sécurité des civils, l'économie et plus largement la paix mondiale. Des organisations se servent certes bien de la technologie pour promouvoir leurs idées politiques mais en font également usage pour punir anonymement ceux qui seraient en désaccord avec ces mêmes idées.

Au vue de la chronologie des évènements, on constate que la situation n'a fait qu'empirer depuis le début du 21ème siècle et il apparaît certain que celle ci ne s'estompera pas en l'état actuel de la (non) régulation de ces actes d'un nouveau type.

Voici une liste chronologique non exhaustive des solutions proposées par les Nations Unies mais qui se sont avérées relativement inefficaces.

-4 janvier 1999: L'Assemblée Générale des Nations-Unies adopte la résolution A/RES/53/70 (proposée par la Russie). C'est la première résolution jamais adoptée sur le sujet de la cyberguerre. La résolution vise principalement à établir une collaboration entre Pays Membres et une communication efficace entre ceux-ci.

-22 janvier 2001: L'Assemblée Générale adopte la résolution A/RES/55/63 qui vise à renforcer

les mesures prises dans la première résolution citée. En plus, cette résolution insiste sur le fait que le public soit au courant des interventions étatiques et associatives visant à lutter contre l'utilisation frauduleuse d'objets technologiques d'information.

-22 janvier 2001 : L'Assemblée Générale adopte la résolution A/RES/56/121 qui rappelle les mesures prises dans les résolutions susmentionnées. La résolution invite également les Pays Membres à tenir compte des actions de l'ONUDC (Office des Nations Unies contre la Drogue et le Crime) et plus particulièrement sa branche dédiée à la Prévention du Crime et à la Justice Criminelle.

-21 décembre 2009 : L'Assemblée Générale adopte la résolution A/RES/64/21.

-2 décembre 2011 : L'Assemblée Générale adopte la résolution A/RES/66/24 qui vise à renforcer les actions prises dans les résolutions susmentionnées mais aussi à garantir une place au problème des cyberattaques dans l'Agenda de l'ONU.

-31 janvier 2013 : L'Assemblée Générale adopte la résolution A/RES/57/239 visant à développer un climat de cybersécurité pour l'ensemble des Pays Membres. Une annexe est ajoutée à cette résolution, garantissant une définition commune de termes clefs tels que "l'éthique" ou la "démocratie".

Il est cependant nécessaire d'imaginer un encadrement du droit de la cyberguerre voir même d'un droit de la guerre par le domaine cyber.

Le premier, et sans doute le plus important des enjeux, est bien sûr la potentielle qualification des actes de cyberguerre d'actes de guerre. En effet, et c'est évidemment un sujet particulièrement délicat et périlleux pour les états ayant recours aux cyberattaques et qui en font l'objet, de nombreuses réflexions tendent à aller vers une requalification des actes de cyberguerre en acte de guerre au sens du droit international. Cette requalification entrainerait sans aucun doute possible une totale refonte des rapports de force dans le domaine cyber, que ce soit au regard des normes établies par le droit coutumier international comme l'interdiction du recours à la force codifié dans le paragraphe 4 de l'article 2 de la Charte des Nations Unies ainsi que les 2 exceptions prévues à cette interdiction, c'est à dire la légitime défense et l'intervention armée suite à une résolution votée en Conseil de Sécurité. Dès lors, si jamais les actes de cyberguerre venaient à se fondre dans les actes de guerre, nul doute que les rapports de force occidentaux/orientaux se verraient profondément modifiés et surtout seraient autrement plus délicats puisque la moindre ingérence ou cyberattaque pourrait logiquement déboucher à une riposte, parfaitement légale au regard du droit international, fondée sur la légitime défense (article 51 de la Charte des Nations Unies).

Ce faisant, il paraît aujourd'hui relativement improbable que les P5 laissent se produire une telle redéfinition. Cependant, l'ONU n'est évidemment pas la seule organisation internationale comprenant un encadrement du droit de la guerre. Il s'agit bien sûr du Traité de l'Atlantique Nord qui vient instaurer en son article 5 que « 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 .». Si la cyberguerre était ainsi fondue au régime de l'attaque, celle ci pourrait dès lors déboucher à une riposte de l'ensemble des états membres de l'OTAN envers le pays agresseur.

A ce titre, l'OTAN s'est penchée sur la question dès 2009 en instaurant un Groupe d'experts internationaux indépendants pour examiner si les lois internationales existantes s'appliquaient aux questions concernant la cybersécurité, et le cas échéant dans quelle mesure. 3 ans suivirent pour aboutir au Manuel de Tallinn sur le droit international applicable à la cyberguerre. Les experts participants au projet ont conclu qu'un principe « le jus ad bellum et le jus in bello s'appliquent au contexte cyber ». Le Manuel ne traitant toutefois pas des cyberactivités qui se produisent en deçà de l'agression armée, le Centre d'excellence de l'OTAN a lancé un projet de suivi de 3 ans intitulé Tallinn 2.0. et qui vient aborder les problématiques liées à la souveraineté des Etats, à la responsabilité étatique, au droit diplomatique et consulaire, mais aussi au droit aérien, au droit de la mer, de l'espace, des télécommunications, aux droits de l'Homme, etc.

Depuis, nombreuses sont les organisations régionales qui développent leur propre stratégie en la matière, L'Union africaine, par exemple, a publié le projet de Convention de l'Union africaine sur la cybersécurité en Afrique. L'Union européenne, elle, a récemment publié une communication conjointe sur la Stratégie de cybersécurité de l'Union européenne, le premier document d'orientation de l'UE dans ce domaine qui reflète le point de vue de ses États Membres en matière de cybersécurité.

L'autre domaine du droit international à envisager dans le cadre de la cyberguerre est bien entendu celui relatif au Droit International Humanitaire (DIH).

Il n'est généralement pas établi de différenciation entre les situations de conflit armé et d'autres situations dans lesquelles des cyber-opérations menacent la sécurité d'États, d'entreprises ou de ménages, ce qui provoque une certaine confusion quant à l'applicabilité du DIH à la cyberguerre. Certains États, comme les États-Unis, le Royaume-Uni ou l'Australie ont déclaré que le DIH s'appliquait à la cyberguerre, bien que ces prises de position publiques ne détaillent pas encore des questions telles que le seuil d'intensité à partir duquel il y a conflit armé. D'autres Etats comme la Chine refusent quant à eux son applicabilité, alors que d'autres encore comme la Russie n'ont pas pris position sur la question. La cyberguerre pose une préoccupation humanitaire essentielle : l'impact que ce type de guerre pourrait avoir sur la population civile, notamment parce que les cyber-opérations pourraient gravement toucher les infrastructures civiles, de plus en plus vulnérables du fait de leur dépendance croissante aux systèmes informatiques : c'est le cas d'un certain nombre d'installations d'une importance cruciale telles que centrales électriques, centrales nucléaires, infrastructures médicales, barrages, systèmes de traitement et de distribution de l'eau, chemins de fer et infrastructure de contrôle aérien, etc. Il n'existe pas à l'heure actuelle, d'exemples d'une particulière gravité dans lesquels la population civile aurait été gravement touchée par des attaques de réseaux informatiques pendant un conflit, cependant il serait erroné d'exclure le risque de scénarios catastrophe comme les collisions entre avions, le dégagement de radiations de centrales

nucléaires, ou le rejet de substances toxiques d'usines chimiques, quand bien même que ces scénarios semblent peu vraisemblables. Le DIH ne s'applique que si les cyber-opérations sont effectuées dans le contexte d'un conflit armé et en lien avec ce conflit. Cependant, un certain nombre d'opérations qualifiés de cyberguerre ne sont pas effectuées dans le contexte d'un conflit armé (l'attaque par le virus Stuxnet d'un site d'enrichissement d'uranium de Natanz, en Iran, est par exemple restée jusqu'à présent une attaque isolée). Il devient alors crucial de se pencher sur la question de la protection des civils, potentielles victimes des actes de cyberguerre ; notamment lorsque ces actes ne font pas partie des offensives d'une guerre classique.

Enfin, reste en suspend la question de l'applicabilité des instances pénales internationales aux hackers ayant perpétrés certains actes d'une particulière gravité à l'échelle internationale.

Conseils aux délégués dans l'écriture de résolutions

Afin de cerner les très multiples enjeux contenus dans ce sujet et en faire ressortir une résolution, il s'agit tout d'abord de cerner ou justement de ne pas cerner, selon que votre pays y est intérêt ou non, toutes les différentes facettes que pourraient contenir en leur définition des termes tels que ceux de cyberguerre, cyberterrorisme, cyberattaque, cyberdéfense, etc.

Ainsi, et puisque le sujet traite ici de cyberguerre, insinuant donc qu'il concerne plus des rapports de force étatiques, il s'agit de se concentrer en priorité sur son éventuelle régulation (une régulation par des recommandations, ce comité n'étant pas coercitif), ou à contrario sur une farouche opposition à cette régulation et un déni des différentes tentatives de fusion avec le droit international de la guerre ou humanitaire. De même, et puisqu'il s'agirait de ne pas trop juridiciser le sujet, il s'agit éventuellement de combattre certaines pratiques d'états membres ou au contraire d'étendre les domaines de coopération.

Si bien sûr l'on s'attardera en priorité sur la cyberguerre au sens strict du terme, le cyberterrorisme ou cyberactivisme malveillant ne seront pas à négliger et cela dépendra encore une fois de l'intérêt de vos états à développer une résolution autour d'une plus grande coopération internationale envers sa condamnation ou non, et plus généralement des principes contenus dans la Charte des Nations Unies allant à leur encontre. Cette coopération internationale pourrait aussi bien sur s'étendre à l'action des différentes ONG.

Bibliographie :

- La première-cyberguerre mondiale, ouvrage collaboratif sous la direction de Xavier Raufer et aux éditions MA

https://www.itu.int/fr/mediacentre/Pages/2016-PR30.aspx

https://unchronicle.un.org/fr/article/en-qu-te-de-la-cyberpaix-g-rer-la-cyberguerre-par-la-coop-ration-internationale

http://www.lenetexpert.fr/cybercriminalite-retour-les-principales-attaques-informatiques-enfrance-monde/

http://www.huffingtonpost.fr/2014/12/20/cyber-attaque-sony-coree-du-nord-enquete-etatsunis_n_6359064.html

http://www.rfi.fr/technologies/20140724-israel-palestine-cyberguerre-anonymous-hackers/

http://tempsreel.nouvelobs.com/societe/20141009.OBS1719/ulcan-revendique-le-piratagede-france-info-et-france-inter.html

http://www.itu.int/wsis/docs/background/resolutions/57-53.pdf

http://www.huyghe.fr/dyndoc_formation/doc2_4b59891862bfe.pdf

http://www.bpi.fr/de-la-cyberstrategie-a-la-cyberguerre-1

http://future.arte.tv/fr/cyberguerre

http://revdh.revues.org/984

http://blog.nordnet.com/securite-2/dossiers-securite/les-etats-unis-declarent-la-cyberguerre.html

http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7458&context=jc

http://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyb

http://www.lemonde.fr/pixels/article/2015/10/20/cyberespionnage-les-soupcons-contre-moscou-se-precisent_4793264_4408996.html

http://www.lemonde.fr/pixels/article/2015/06/09/piratage-de-tv5-monde-l-enquete-s-oriente-vers-la-piste-russe_4650632_4408996.html

http://www.lemonde.fr/pixels/article/2014/08/13/l-ukraine-et-la-russie-au-bord-de-la-cyberguerre_4470184_4408996.html

http://unchronicle.un.org/fr/article/en-qu-te-de-la-cyberpaix-g-rer-la-cyberguerre-par-la-coop-ration-internationale/

http://eeas.europa.eu/policies/eu-cyber-security/cybsec_comm_fr.pdf

http://lexpansion.lexpress.fr/high-tech/les-mercenaires-de-la-cyberguerre_1623549.html

http://www.lemonde.fr/international/article/2016/12/28/l-osce-victime-d-une-attaque-informatique_5054744_3210.html

http://www.lepoint.fr/monde/piratage-de-la-campagne-americaine-ce-que-l-on-sait-13-12-2016-2089994_24.php

http://www.lemonde.fr/pixels/article/2016/10/21/une-cyber-attaque-massive-perturbe-de-nombreux-sites-internet-aux-etats-unis_5018361_4408996.html

http://www.un.org/fr/sections/un-charter/chapter-vii/index.html

http://www.idpi.fr/actualites/disruptions/les-strategies-etatiques-face-a-la-cyber-guerre/

http://www.lejdd.fr/International/Actualite/En-pleine-cyber-guerre-froide-597955

http://www.lemonde.fr/pixels/article/2017/12/14/trois-hommes-plaident-coupable-de-la-creation-du-puissant-virus-mirai_5229535_4408996.html

http://www.lemonde.fr/pixels/article/2017/11/22/piratage-massif-d-uber-les-reponses-a-vos-questions_5218688_4408996.html

http://www.lemonde.fr/pixels/article/2017/10/04/yahoo-la-cyber-attaque-de-2013-a-affecte-l-ensemble-des-3-milliards-de-comptes_5195728_4408996.html

http://www.lemonde.fr/pixels/article/2017/03/15/yahoo-quatre-inculpations-prevues-dans-le-cadre-de-la-cyberattaque-de-2014_5094519_4408996.html

http://www.lemonde.fr/pixels/article/2017/09/08/les-donnees-personnelles-de-143-millions-d-americains-potentiellement-piratees_5182543_4408996.html

http://www.lemonde.fr/idees/article/2017/05/17/les-macronleaks-une-attaque-sans-precedent_5128735_3232.html

http://www.lemonde.fr/pixels/article/2017/06/02/macronleaks-l-enquete-pointe-vers-un-piratage-simple-et-generique_5137945_4408996.html

http://www.lemonde.fr/pixels/article/2017/07/31/wikileaks-publie-l-integralite-des-macronleaks_5167002_4408996.html

http://www.lemonde.fr/pixels/article/2017/05/15/logiciel-de-racket-la-situation-semble-stable-selon-europol_5127878_4408996.html

http://www.lemonde.fr/pixels/article/2016/08/31/les-donnees-piratees-de-dropbox-en-2012-refont-surface_4990293_4408996.html

http://www.lemonde.fr/pixels/article/2016/05/30/les-informations-de-millions-de-comptes-myspace-en-vente-en-ligne_4928733_4408996.html

http://www.lemonde.fr/pixels/article/2016/08/24/des-pirates-informatiques-visent-le-bureau-de-moscou-du-new-york-times_4987154_4408996.html

http://ultimaratio-blog.org/archives/8434