72ème Assemblée générale des Nations unies - Cybersécurité - Le rôle et la responsabilité des acteurs privés dans le renforcement de la stabilité et de la sécurité internationale du cyberespace - Intervention de M. Jean-Yves Le Drian, ministre de l'Europe et des affaires étrangères

(New York, 18 septembre 2017)

Mesdames et Messieurs les Ministres, Monsieur le Commissaire

Mesdames et Messieurs,

Je tiens tout d'abord à vous remercier d'avoir répondu en nombre à l'invitation de la France à cet évènement sur le rôle et la responsabilité des acteurs du secteur privé dans le renforcement de la sécurité du cyberespace.

Au cours de ces dernières années, l'espace numérique, que l'on appelle parfois plus simplement «cyberespace», s'est imposé comme un nouveau lieu d'opportunités économiques et de transformations sociales.

Mais nul ne peut l'ignorer : le monde numérique fait aussi face à des vulnérabilités nouvelles ; elles sont susceptibles de remettre en cause les principes d'ouverture et de liberté qui fondent le cyberespace ; elles ont également des conséquences néfastes sur les opportunités économiques qu'offre la révolution numérique. En réalité, nous assistons à une prolifération des menaces dans le cyberespace : ce phénomène représente un défi fondamental et il n'en est qu'à ses débuts ; il s'intensifiera au cours des prochaines années, cela ne fait guère de doutes. Les cyber-attaques qui ont frappé la communauté internationale au printemps dernier, qu'il s'agisse de WannaCry ou de NotPetya, ont servi de signal d'alarme : quand le bon fonctionnement des hôpitaux est menacé, quand des données critiques deviennent soudainement inaccessibles, quand des acteurs économiques de premier plan sont touchés, il est clair que nous avons affaire à une menace commune qui affecte la stabilité et la sécurité internationales.

Face à ces menaces, les États doivent affirmer leur volonté de répondre aux enjeux de cybersécurité par la coopération et par le droit. Je tiens à cet égard à saluer les négociations conduites sous l'égide des Nations unies entre experts gouvernementaux ; elles ont permis, dès 2013, de reconnaitre l'applicabilité du droit international existant au cyberespace et, en 2015, de s'accorder sur un certain nombre de normes de comportement responsable des États dans ce

domaine.

Néanmoins - et comme l'a malheureusement démontré l'échec du dernier cycle de négociations du groupe gouvernemental d'experts de l'ONU en juin 2017 - la régulation interétatique n'est pas en mesure d'apporter à elle seule une solution efficace et durable à ces nouveaux défis de sécurité.

C'est l'un des bouleversements induits par la révolution numérique : l'irruption du numérique comme outil et comme espace de confrontation confère au secteur privé, et notamment à un certain nombre d'acteurs privés systémiques, un rôle et une responsabilité inédites dans la préservation de la paix et de la sécurité internationales. Cela est vrai à plusieurs égards, s'agissant de la cyber conflictualité :

- premièrement, ce que l'on nomme le «champ de bataille» numérique est en grande partie constitué de produits commerciaux grand public, y compris pour les attaques de grande envergure, qui en exploitent les défauts de fabrication ;

- deuxièmement, les «armes» numériques, et j'entends par là les logiciels intrusifs ou destructifs sont pour partie produites par des entreprises privées sur un marché qui, contrairement aux marchés de l'armement classique, est très difficile à réguler ;

- troisièmement, des services de «mercenariat» apparaissent, qui proposent à leurs clients des services offensifs de contre-attaque cyber, selon une logique de légitime défense privée - ce qu'on appelle communément le «hack-back», je vais y revenir dans un instant.

En l'absence de régulation, la poursuite de ces activités est susceptible de nuire à la préservation d'un écosystème numérique global sécurisé ; ces actions ont aussi un fort potentiel déstabilisateur sur les relations interétatiques. La réponse à ce défi doit être inclusive. Il faut donc que les États engagent entre eux, mais aussi avec le secteur privé et le monde de la recherche, de nouveaux travaux afin de définir des formes de régulation originales adaptées à l'évolution du monde numérique. Dans ce contexte, notre responsabilité et notre intérêt sont de défendre les cadres d'action et les règles de droit édictés collectivement, en nous engageant pour le renforcement du rôle du système onusien dans cette régulation, tout en faisant preuve de créativité multilatérale pour élaborer une forme de gouvernance mondiale.

Je tiens à être clair : notre objectif n'est pas de brider l'innovation ou la liberté d'entreprendre. Au contraire, il s'agit de définir ensemble des mesures permettant de renforcer la stabilité, la coopération et la confiance de tous les acteurs dans le cyberespace. C'est aussi une condition indispensable à la réussite économique.

À mon sens, cela passe, au moins, par trois axes d'efforts qui doivent être poursuivis parallèlement :

Le premier axe, c'est le renforcement de la sécurité des produits et des services numériques ;

l'enjeu est de s'assurer qu'ils ne puissent pas être détournés de leur usage initial pour conduire des attaques informatiques. Le problème se pose aujourd'hui de façon accrue avec la multiplication des objets connectés pouvant servir de vecteurs d'attaque. Face à ce défi, il est pertinent de poser un principe de responsabilité de sécurité des acteurs privés dans la conception, l'intégration, le déploiement et la maintenance de leurs produits et service numériques. Cette responsabilité, qui pourrait prendre la forme d'une obligation de moyens pour les entreprises de garantir la sécurité au long terme de leurs produits numériques, incomberait aux producteurs comme aux distributeurs et aux intégrateurs.

Le deuxième axe concerne la lutte contre la prolifération et la commercialisation d'outils, logiciels ou techniques malveillants dans le cyberespace. En effet, comme pour le désarmement conventionnel, le contrôle des exportations de capacités cyber offensives représente un enjeu de sécurité majeur. Dans ce domaine, des progrès ont déjà été permis par l'inclusion, en 2013, des «logiciels d'intrusion» dans la liste des biens à double usage de l'Arrangement de Wassenaar ; c'est le premier jalon d'une régulation du commerce mondial des outils offensifs cyber. Le travail accompli dans ce cadre doit être approfondi afin d'aboutir à un engagement des États pour le contrôle de leurs exportations des outils et techniques offensifs cyber, tout en prenant en compte les intérêts légitimes des entreprises de cybersécurité et du monde académique.

Enfin, le troisième axe d'effort doit permettre l'encadrement de certaines pratiques particulièrement déstabilisatrices, comme le hack-back qui consiste, pour un acteur privé, à s'arroger le droit de mener une contre-attaque dans le cyberespace, dans une logique de «légitime défense privée» ; une telle notion de «légitime défense privée» est très contestable par le biais qu'elle induit s'agissant de l'exercice de la contrainte légitime qui doit rester le monopole des États. La France considère en effet que l'utilisation de telles capacités offensives par des acteurs privés, agissant pour eux-mêmes ou pour le compte d'autres acteurs non-étatiques, fait peser un risque d'instabilité systémique dans le cyberespace. En effet, de telles actions entrainent un risque d'escalade d'autant plus dangereux que le risque d'attribution erronée se pose de la même manière pour le secteur privé que pour les États.

Cela ne signifie pas que les acteurs privés doivent être démunis face aux menaces informatiques. En réalité, ils disposent déjà d'une panoplie de mesures fondées sur des technologies défensives, voire sur certaines techniques de cyberdéfense dites «actives» mais non intrusives. En revanche, en raison des externalités négatives qu'elles sont susceptibles de générer, les capacités intrusives devront rester interdites.

Mesdames et Messieurs,

Les trois chantiers que je viens d'esquisser constituent une première ébauche de réponse pour faire face ensemble aux défis que représentent la sécurité et la stabilité du cyberespace. Ces trois axes représentent une première vague de propositions ; elles devront être encore détaillées, affinées, discutées entre les États mais aussi avec les acteurs privés. À mon sens, le G20 pourrait constituer un forum adapté pour aborder ces sujets de régulation internationale qui, comme vous le voyez, sont au croisement d'enjeux de souveraineté et d'enjeux économiques pour lesquels une étroite coopération avec le secteur privé est par conséquent primordiale. Et je souhaite que l'évènement qui nous rassemble aujourd'hui en marge de la 72ème Assemblée générale des Nations unies, fournisse l'occasion d'un premier échange de

vues afin de proposer des pistes d'actions que nous pourrons porter conjointement dans les enceintes appropriées.

Le commissaire tout à l'heure faisait référence au fait que nous nous sommes connus sous d'autres responsabilités, et précisément les responsabilités du ministre de la défense de la France que j'ai eues pendant 5 ans m'amène à conforter encore plus le raisonnement que je viens de tenir ici sous ma nouvelle casquette de ministre des affaires étrangères. Merci de votre attention./.