



Vers un ordre international pour le cyberspace ?

Depuis la création d'Internet, les États-Unis ont acquis une influence croissante dans le domaine du cyberspace. Les conséquences de l'affaire Snowden ont néanmoins offert aux puissances émergentes l'occasion de faire entendre leur voix dans ce domaine.

L'hégémonie américaine au cœur du débat

En 2011, les États-Unis ont énuméré leurs propres « *normes de comportement* » dans le cyberspace au premier rang desquelles figurent la sécurité, la liberté d'expression et le minimum de contrôle de la part d'institutions supranationales. Cette position s'explique par les capacités de surveillance et d'intervention accrues dont ils disposent.

Washington affiche dès lors une ferme réticence à l'idée d'encadrer le comportement des États dans le cyberspace. Dans ce domaine, les États-Unis contestent l'application du droit international car l'absence de normes contraignantes ne peut que conforter leur hégémonie technologique et militaire.

De profondes dissensions demeurent donc quant à la gouvernance du cyberspace. En avril 2015, les BRICS ont lancé un appel pour une démocratisation accrue de l'ICANN (*Internet Corporation for Assigned Names and Numbers*), qui prône notamment plus de transparence et une réforme radicale du processus décisionnel. L'autorité régulatrice du *Web* est en effet suspectée d'entretenir des liens étroits avec le gouvernement américain.

Une fragmentation du Net



Entre démocratie et « *rideau de fer numérique* », chaque État semble suivre sa propre voie idéologique. Les nations occidentales prétendent, au nom des valeurs démocratiques, assurer la sécurité des systèmes sans contrôler le contenu. Les lois sur le renseignement soulèvent néanmoins d'importants débats.

D'autres modèles de gouvernance cherchent au contraire à renforcer leurs prérogatives nationales à des fins de contrôle. Sous le nom de « *Bouclier doré* », les autorités chinoises ont institué un système verrouillé, dont les passages vers l'Internet mondial sont restreints et surveillés.

En 2006, une résolution soutenue par la Russie devant l'Assemblée générale de l'ONU appelle au désarmement du cyberspace en transposant le droit de la guerre conventionnelle au domaine électronique. Elle a obtenu l'approbation de 177 pays et une unique opposition de la part des États-Unis. Les cyberattaques effectuées par la Russie à l'encontre de l'Estonie en 2007 et de la Géorgie en 2008 révèlent néanmoins le caractère peu contraignant de cette résolution.

Le Brésil se positionne comme le champion du multilatéralisme et comme le partisan d'une troisième voie. Brasília est en effet plus ouvert à une gestion mutualisée par un organisme multilatéral sous l'égide de l'ONU.

La fonction normative des acteurs non-étatiques, source de dissensions

Les entreprises du e-commerce et les activistes jouent aussi un rôle important dans la définition de l'architecture du cyberspace. L'affaire Snowden a mis en lumière les accords tacites établis entre le gouvernement américain et les entreprises du Net comme *Google* et *Facebook*. À la suite de ces révélations, certaines entreprises d'Europe occidentale ont par exemple délaissé les sociétés d'hébergement de données américaines au profit de sociétés européennes.

Selon Daniel Ventre, spécialiste français du cyber, le statut des « cyber-guerriers » pose également de sérieux problèmes aux acteurs de la Défense. En effet, dans l'hypothèse d'une attaque menée par des « cyber-mercenaires » recrutés par un État tiers, le choix de la riposte face à ces « combattants de cette guerre d'un nouveau genre » serait particulièrement délicat.

Une résolution de l'ONU de décembre 2013 a chargé un nouveau groupe de travail composé d'experts gouvernementaux d'établir un rapport sur les « normes, règles ou principes de comportement responsables des États ». Selon le média en ligne Politico, ce document, actuellement en cours d'élaboration, reprend la plupart des normes préconisées par Washington. Toutefois, la Russie et la Chine bloqueraient certaines mesures, notamment l'application de l'article 51 de la Charte des Nations Unies à ce domaine, qui légitimerait l'emploi de la force en cas de cyberattaque.