Cyber Strategy :

définir un horizon stratégique dans

l'environnement cyber

Executive Summary

Chaire de Cyberdéfense et Cybersécurité Saint-Cyr, Sogeti, Thales

Sébastien-Yves Laurent
Professeur des Universités

* Présentation

Sébastien-Yves Laurent est professeur des Universités à la Faculté de droit et de science politique de l'Université de Bordeaux. Il enseigne également à Sciences Po Paris, Sciences Po Bordeaux et à l'École de Guerre Économique. C'est un consultant et analyste spécialiste des enjeux de sécurité globale. Il est le fondateur de l'International Summer School Defence-Security-Cyber (DSC) (http://dsc.u-bordeaux.fr/) et le co-fondateur du groupe de travail « Mètis » (Sciences Po Paris).

Parmi ses publications récentes : *Atlas du renseignement. Géopolitique du pouvoir* (Paris, Presses de Sciences-Po, 2014) ; *Pour une véritable politique publique du renseignement* (Paris, Institut Montaigne, 2014) ; *Transformations et réformes de la sécurité en Europe* (Bordeaux, Presses universitaires de Bordeaux, 2015).

* Executive Summary :

L'objet de cette étude est une analyse critique et prospective des enjeux de gouvernance dans les trois couches du cyber avec un focus particulier sur la dimension de cybersécurité.

* Elle vise ainsi à aider à la définition d'un horizon stratégique pour les acteurs étatiques et privés.

* On a fait ici le choix d'une approche de *comprehensive analysis* permettant de rassembler dans la même analyse les acteurs régaliens et les acteurs privés et en resituant la problématique de la cybersécurité et des différentes gouvernances dans leur environnement normatif et économique.

* L'horizon stratégique fixé dans cette étude repose sur l'identification de 2 caractéristiques durables de long terme, de 10 invariants et de 5 facteurs d'incertitudes qui permettent de bâtir 3 scénarios. L'ensemble du travail s'appuie sur 20 tableaux, graphes et cartes.

* Il est bâti en 4 parties :

1. La construction progressive du cyberespace par ses structures et ses usages
2. L'état actuel de l'environnement cyber
3. Un environnement cyber fait d'incertitudes multiples
4. L'horizon stratégique : des avenirs à géométrie variable.

* Malgré l'arrivée tardive des Etats dans un environnement cyber qui n'a pas été conçu pour eux, on assiste à de multiples balkanisations. Cette caractéristique explique l'importance du principe de gouvernance multistakeholder qui est très dominante dans l'environnement. Celui-ci est faiblement régulé avec la large dominance d'un *soft law* technique sur le *hard law*. Au total, on conclut à une gouvernance relativement forte des couches physiques et logicielles par rapport à une gouvernance de la couche sémantique qui est très faible. De ce point de vue l'Europe est un isolat, favorable aux Internautes mais un espace de forte contrainte juridique pour les acteurs économiques du numérique. L'environnement est caractérisé par des visions très antagonistes entre les grandes et principales moyennes puissances sur ce que doit être le cyberespace de demain.

* Pour les acteurs étatiques et non-étatiques, mettre en œuvre une stratégie dans le cyber suppose de comprendre :

- (1) la transversalité de l'environnement car le cyber innerve tout et de ne pas le limiter à sa dimension la plus visible qui est l'aspect informationnel ;
- (2) les caractéristiques et les ressorts de la gouvernance *multi-stakeholder* où acteurs publics et privés doivent tenir compte de leur caractéristiques respectives et de leurs contraintes spécifiques ;
- (3) l'idéologie à l'œuvre dans le réseau mondial qui sert encore à mobiliser les différents acteurs ;
- (4) la composante socio-politique de l'environnement cyber qui a des effets majeurs, que ce soit sur un plan technologique ou économique.

* En fait, il n'y a pas d'autonomie du cyber par rapport aux autres aspects stratégiques. L'environnement cyber participe désormais d'une approche globale de la stratégie. Les acteurs économiques et régaliens s'affrontent dans l'environnement cyber dans le cadre de leurs rapports de forces généraux. Cet environnement particulier est devenu un terrain privilégié : il est particulièrement attractif car il permet de créer des

dommages et des préjudices de façon discrète sans possibilité d'attribution. De ce point de vue, on peut estimer que l'environnement cyber est désormais le terrain majeur d'affrontement indirect. L'in-attribution favorise les stratégies indirectes pour tous les acteurs ayant un certain seuil (bas) de maîtrise technologique. Le développement de l'environnement cyber est d'une certaine façon un égalisateur relatif de puissance.