La note du CERPA
N°219
05 / 2019

Chargée d'études Claire Desdouits

Le partenariat public privé dans le domaine de la cyberdéfense au Royaume-Uni

Depuis 2003, le Royaume-Uni a mis en place une stratégie nationale en matière de sécurité de l'information en plaçant la cyberdéfense comme l'une de ses priorités nationales. Depuis, un arsenal technique a été déployé pour faire du Royaume-Uni le pays « le plus sûr pour vivre et travailler en ligne »[1], et ce avec une volonté de collaboration entre les secteurs publics et privés.

La cyberdéfense au centre de la politique gouvernementale britannique

Depuis le début des années 2000, le Royaume-Uni finance de nouveaux programmes dans le domaine de la cyberdéfense. En 2010, David Cameron, a annoncé le lancement du *National Cyber Security Program (NCSP)* avec un budget prévu de 860 millions de livres pour la période 2011-2016. Cette enveloppe, principalement destinée aux activités de sécurité et de renseignement du *Gouvernment Communications Headquarters (GCHQ)* ainsi qu'aux activités cyber du *Ministry of Defence (MoD),* est en constante augmentation puisqu'elle atteint les 1,9 milliard de livres pour la période 2016-2021[2].

Au niveau mondial, entre 85 et 90 % du marché de la cyberdéfense est tenu par des entités privées[3]. Les entreprises sont au cœur de la sécurité de l'information et leur action dépasse les frontières étatiques. Néanmoins, certains aspects sont considérés comme d'intérêt national et relèvent donc de la responsabilité de l'Etat[4]. Alors que le NCSP de 2011 préconisait de se concentrer exclusivement sur le secteur privé, celui de 2016 dénonce l'échec du marché dans la réduction de l'insécurité sur internet et propose une approche plus coopérative avec le gouvernement. Cette collaboration repose notamment sur le partage du savoir et de l'expertise en matière de cyberdéfense pour rendre la lutte plus efficace. C'est dans ce contexte qu'est lancé le *Cyber Security Information Sharing Partnership (CiSP)*, une plateforme numérique de partage d'informations en temps réel entre les secteurs privés et publics. De même, en 2016, le *National Cyber Security Centre (NCSC)* est créé à Londres. Rattaché au *Government Communications Headquarters (GCHQ),* cet organisme est l'interface entre le gouvernement et l'industrie et centralise l'ensemble des activités et des informations relatives à la cyberdéfense.

Le place du Royaume-Uni dans un marché mondial en croissance

Le marché mondial de la cyberdéfense est en constante expansion. Alors qu'il ne valait que 3,5 milliards de dollars en 2004, il atteint les 137 milliards en 2017 et les statistiques prévisionnelles annoncent une augmentation de la valeur du marché de 10 à 15 % d'ici 2021[5]. Parmi les membres du G20, le Royaume-Uni est pionnier dans le secteur digital qui représente 16 % de son produit intérieur, 10 % de ses emplois et 24 % de ses exportations[6]. D'après la *Cyber Security Export Strategy* de 2018, les exportations britanniques dans le domaine devraient atteindre les 2,6 milliards de livres en 2021. Par ailleurs, parmi les 50 entreprises de cyberdéfense les plus importantes dans le monde en 2018, 7 sont britanniques comme *BAE Systems, PwC* ou *KPMG*.

L'industrie de la cyberdéfense est traitée comme un service voué à l'exportation et à l'expansion de l'influence du Royaume-Uni sur la scène internationale[7]. Le pays souhaite se démarquer dans le domaine, notamment au travers de la mise en place de la *Global Conference on Cybersecurity* aussi nommée *London Process.* Le rôle du gouvernement britannique est désormais d'étendre son expertise à l'international de façon à dessiner le futur global du marché de la cyberdéfense.

Le Royaume-Uni a su s'adapter au développement rapide de la nouvelle menace cyber. Le gouvernement a devancé ses voisins en engageant une coopération accrue avec le secteur privé et souhaite désormais étendre son expertise à l'international. L'objectif affiché est celui d'influencer à long terme les évolutions du marché mondial de la cyberdéfense.

Ces propos ne reflètent que l'opinion de l'auteur.

1 https://www.ncsc.gov.uk/
2 Carr M. & Tanczer LM. « UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions", *Journal of Cyber Policy*, 10/12/18.
3 P. Rosenzweig "Cybersecurity and Public Goods. The Public/Private "Partnership"" 2012.
4 Smekalova M. & Gourlay K. "Mitigating cyber risks: is there room for two", *Royal United Service Institute (RUSI)*, 17/04/19.
5 "2018 Cybersecurity Market Report" *Cybersecurity Venture.*
6 Carr M. & Tanczer LM. « UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions", *Journal of Cyber Policy*, 10/12/18.
7 *Idem.*