



L'industrie de la cyberdéfense israélienne : une coopération public-privé réussie

Dès le milieu des années 1990, les autorités israéliennes se sont emparées de la problématique cyber pour la placer au centre de leur réflexion stratégique. Les efforts pour développer la cyberdéfense se sont d'abord focalisés sur le domaine militaire tandis que les risques encourus par les systèmes d'information civils étaient peu pris en compte. Depuis, un tissu industriel de cybersécurité s'est développé et a noué des liens privilégiés avec les pouvoirs publics, ce qui place Israël au rang des leaders mondiaux de la cyberdéfense.

L'impulsion gouvernementale décisive dans le domaine de la cybersécurité israélienne

Les menaces cyber sont prises très au sérieux en Israël. Les pouvoirs publics recensent des centaines de milliers de cyberattaques par jour sur le territoire. Les risques sont multiples, concernent les mondes civil et militaire et peuvent aller du simple vol de données à la neutralisation des installations énergétiques. Partant, les initiatives du secteur privé, encouragées par le gouvernement, permettent de compléter l'arsenal de défense cyber à destination de la sphère civile.

En 2010, le Premier ministre Benjamin Nethanyahu lance la *National Cyber Initiative* et crée l'*Israeli National Cyber Bureau (INCB)*, rattaché à son cabinet, qui dispose d'un budget annuel d'environ 130 millions de dollars. L'*INCB* a pour but de renforcer la sécurité civile et militaire des infrastructures du pays en favorisant le financement de la recherche et développement (R&D) dans le domaine cyber et en stimulant la coopération entre les milieux universitaires, industriels et militaires.

L'*INCB* est à l'origine de projets d'envergure dont l'objectif est de renforcer le rayonnement israélien sur le marché mondial de la cyberdéfense via une coopération public-privé ambitieuse. Ainsi, la ville de Beer-Sheva accueille, au sein du pôle technologique *CyberSpark*, la plupart des unités de lutte informatique de l'armée, des cursus universitaires dédiés, des centres de recherche, des firmes nationales de cyberdéfense ainsi que des géants internationaux tels que *IBM*, *Oracle* ou *Lockheed Martin*. Le partenariat pour la cyber-innovation entre l'université Ben Gurion et l'entreprise KUD international LLC, le *Beer-Sheva Advanced Technological Park*, est quant à lui un succès. *Deutsche Telekom*, *Elbit Systems* et *EMC* l'ont récemment intégré.

Une dynamique industrielle nationale qui doit assurer un rayonnement mondial

Actuellement en plein essor, le marché de la cyberdéfense et de la cybersécurité israélien est constitué de 430 entreprises auxquelles s'ajoutent 40 centres de R&D¹. Il représente un relais de croissance de taille. Or, si le marché de la défense nationale est porteur, il demeure restreint. Afin de survivre et de croître, les industries de cyberdéfense doivent se tourner vers le secteur privé et s'exporter.

Trois des plus grandes entreprises nationales de défense, *Israel Aerospace Industries (IAI)*, *Elbit System* et *Rafael*, ont développé leurs compétences en matière de cybersécurité à destination du monde privé, initialement grâce à la commande militaire. L'entreprise *Rafael*, à l'origine du système de défense anti-missile *Iron Dome*, s'est récemment tournée vers des activités de cybersécurité, avec l'appui du gouvernement. En 2015, elle a lancé une offre commerciale pour assurer la sécurité des systèmes qui régissent le secteur des transports ou encore de l'eau. Le gouvernement israélien aide ses entreprises à nouer des partenariats avec d'autres pays dont le Japon, l'Italie et l'Inde, tant pour la recherche que pour l'exportation de solutions qui visent à sécuriser les systèmes d'information des États et des entreprises. *IAI* a pour sa part réussi à obtenir le soutien financier de Singapour pour y ouvrir un centre de R&D.

En 2014, l'*INCB* estimait à 3 milliards de dollars le montant des exportations réalisées par les entreprises nationales, Israël étant alors sur la seconde marche du podium dans le domaine, derrière les États-Unis et devant le Royaume-Uni.

Si les acteurs privés et publics de la cyberdéfense sont complémentaires, les compétences sont, elles, rares et disputées. L'armée dispose d'une réserve opérationnelle dans le domaine du cyber mais subit malgré tout la concurrence des entreprises de cybersécurité qui recrutent les experts formés dans ses unités. Le gouvernement israélien s'est saisi de la question et multiplie les cursus scolaires et académiques pour développer les savoir-faire et pour atténuer la fuite des cerveaux.

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

¹ Cf. Kévin Martin, *Cybersécurité : ambitions israéliennes et positionnement des acteurs défense* Défense&Industries n°6, 1er février 2016.