L'économie de la cybersécurité en Israël

Olivier DANINO
Chaire de cybersécurité & cyberdéfense Saint-Cyr, Sogeti, Thales

Mars 2017 – Article III.29

Lorsque les Israéliens ont commencé à s'intéresser à la sécurité de leurs systèmes d'information, ils se sont d'abord concentrés sur leurs infrastructures militaires. La priorité donnée à l'armée s'est donc faite au détriment de la protection des systèmes d'information du civil. C'est ce retard que les dirigeants israéliens cherchent à combler depuis quelques années. Pour y parvenir, ils ont sollicité l'ensemble des forces vives du pays. L'industrie de la cybersécurité s'est donc vue largement mise à contribution. Lorsque Netanyahou a été réélu en 2009, il a lancé une série d'initiatives visant à renforcer tous les acteurs travaillant sur les enjeux du cyber et sur la question de la cybersécurité en Israël. L'État joue donc un rôle moteur et c'est sur ce point que nous allons insister dans ce document.

I. La vision israélienne de la cybersécurité

Les dirigeants israéliens parlent souvent de 3e révolution industrielle lorsqu'ils évoquent le cyber. Le professeur Eviatar Matania, directeur de l'*Israel National Cyber Bureau*, déclarait ainsi : « *We think the cyber revolution is the third revolution after the agricultural and industrial one, and it's going to change all of our lives* »[1]. Ce changement concerne effectivement tout le monde étant donné que nos sociétés et nos économies sont de plus en plus dépendantes des systèmes d'information. Une faille de sécurité peut ainsi avoir de lourdes conséquences pour un État, pour son armée, pour ses entreprises ou pour sa population. C'est pourquoi, la question de la sécurité de ces systèmes d'information est essentielle. Israël considère clairement ce point comme un enjeu stratégique. Il s'agit de ne pas dépendre d'outils fabriqués à l'étranger et d'assurer ainsi l'indépendance du pays. C'est également une question purement économique vu

[1] Financial Times, « Israel cyber-security expertise lures growing of share investment », 12 janvier 2016, disponible en ligne, https://www.ft.com/content/dfa5c916-b90e-11e5-b151-8e15c9a029fb

que les besoins en cybersécurité sont croissants pour les entreprises et pour les États. D'ailleurs, pour les Israéliens, aucun pays ne peut prétendre à une croissance économique durable dans le futur sans développer ce secteur d'activité.

Israël se distingue toutefois en mettant tout en œuvre pour devenir un leader mondial du cyber et se placer ainsi comme un acteur incontournable. Lors de son discours annuel aux Nations unies en 2016, le premier ministre israélien déclarait ainsi : « *If hackers are targeting your banks, your planes, your power grids and just about everything else, Israel can offer indispensable help. Governments are changing their attitudes towards Israel because they know that Israel can help them protect their peoples, can help them feed them, can help them better their lives* »[2].

L'aspect économique n'est donc pas le seul point qui motive le souhait d'Israël d'être un leader mondial dans le domaine du cyber. La dimension diplomatique entre aussi largement en ligne de compte. Benjamin Netanyahou pense en effet que les collaborations économiques permettent de tisser de véritables liens entre États en créant des intérêts communs et sont donc, au final, vecteurs de paix et de reconnaissance. En contribuant à la sécurité du cyberespace mondial, et en nouant des partenariats partout où Israël le peut, le gouvernement israélien considère donc qu'il lutte contre son isolement sur la scène internationale.

Si le Premier ministre Netanyahou a placé le cyber au cœur de ses choix stratégiques, il s'inscrit cependant dans une politique suivie par tous les dirigeants israéliens depuis le milieu des années 1990. Le gouvernement d'Ariel Sharon, par exemple, a adopté le 11 décembre 2002 un document qui concerne la protection des infrastructures critiques en Israël[3]. Encore en vigueur aujourd'hui, ce texte reste un élément central dans le dispositif israélien. Les gouvernements successifs dirigés par Netanyahou ont toutefois pris de nombreuses initiatives visant à soutenir et renforcer l'industrie de la cybersécurité en Israël et cela a été clairement bénéfique à l'économie israélienne.

II. La place de l'industrie de la cybersécurité dans l'économie israélienne

L'économie israélienne est particulièrement dynamique. En 2015, le taux de croissance s'élevait à 2.5%. Les estimations pour 2016 tournent autour de 3% et pour 2017 autour de 3.3%. En comparaison à d'autres pays de l'OCDE, le niveau de chômage en Israël reste bas, 5.25%, et la dette publique est maîtrisée (73% du PIB). Si ces quelques chiffres ne doivent pas faire oublier les points négatifs - le taux de pauvreté atteint 25%, largement au-dessus de la moyenne de l'OCDE, sans compter un secteur de l'immobilier qui ne cesse de s'enflammer dans certaines villes du pays - il n'en reste pas moins que la croissance est au rendez-vous depuis 13 années consécutives.

---

[2] Prime Minister's Office, « PM Netanyahu's Speech at the United Nations General Assembly », 22 septembre 2016, disponible en ligne, http://www.pmo.gov.il/English/MediaCenter/Speeches/Pages/speechUN220916.aspx

[3] Pour plus d'informations sur la stratégie israélienne voir DANINO Olivier, « la stratégie cybernétique de l'Etat d'Israël », in *Cyber : la guerre a commencé, Sécurité Globale*, n°24, été 2013, pp. 15-24.

Elle est portée en partie par l'industrie des nouvelles technologies qui participe pour un peu plus d'un tiers au PIB israélien. 20% de ces entreprises des nouvelles technologies se consacrent à la cybersécurité. Selon un rapport de l'*Israel Venture Capital Research*, il y aurait en Israël près de 430 compagnies de cybersécurité[4]. Ce chiffre a presque doublé en 10 ans (250 en 2006) et il est près de 20 fois plus important qu'il y a 20 ans (20 en 1996), à une époque où les dirigeants israéliens portaient surtout leur attention sur les systèmes d'information de l'armée. Toutefois, toutes ces compagnies spécialisées en cybersécurité n'ont pas de revenus constants et/ou sont encore en cours de développement. Un peu plus de la moitié des entreprises, 55%, a un chiffre d'affaire régulier parmi lesquels 9% uniquement a un revenu annuel dépassant les 10 millions de dollars. Ce qui signifie que près de 45% des entreprises spécialisées en cybersécurité ne proposent pas encore de produits sur le marché et/ou n'ont pas encore fait leurs preuves. Certaines d'entre-elles disparaitront même assez rapidement mais sans conséquences majeures étant donné que le taux de création/disparition de ces compagnies reste particulièrement élevé en Israël[5].

Les entrepreneurs prennent donc des risques pour imposer leurs produits et c'est ce qui explique en partie le dynamisme israélien. D'ailleurs, une entreprise californienne de veille, qui propose une liste des 500 compagnies les plus dynamiques et les plus innovantes au monde, *Cybersecurity Ventures*, recensent 26 entreprises israéliennes dans son classement annuel. En entrant dans le détail, on constate qu'une seule de ces compagnies se situe dans le top 5, 2 dans le top 20 et 9 dans le top 100. En comparaison, la France n'en a que 6 dans le top 500 (dont Thalès) mais aucune n'arrive avant la 105^{e} place[6].

Si ces entreprises sont actives sur le marché local israélien, elles s'imposent aussi sur le marché mondial. En 2013, les exportations israéliennes en matière de cybersécurité s'élevaient à 3 milliards de dollars soit 5% du marché global. Ces chiffres ont doublé en un an plaçant Israël en 2^{e} position derrière les États-Unis. Même si 2015 a été une année moins faste, les exportations étaient tout de même de 4 milliards de dollars. Les dirigeants israéliens ont également mis en place une stratégie visant à capter les capitaux mondiaux dans le domaine de la cybersécurité. Cela a été efficace vu qu'entre 2013 et 2015 le pourcentage d'investissements étrangers en Israël a doublé. En captant de 11% à 20% des investissements mondiaux du secteur privé, Israël est devenu en 2015 le 2^{e} pays le plus attractif après les États-Unis.

III. La mise en place d'un écosystème favorable au développement de l'industrie de la cybersécurité

---

[4] Le site de l'IVC Research Center est très complet. Le rapport de 2016 y est disponible gratuitement : http://www.ivc-online.com/ivc-16/html/index.html

[5] La moyenne depuis 16 ans est de 52 créations d'entreprises spécialisées en cybersécurité par an ; 66 par an pour les 4 années qui viennent de s'écouler.

[6] Ce classement est disponible en ligne sur le site de Cybersecurity Ventures : http://cybersecurityventures.com/cybersecurity-500/

Si les Israéliens se sont dotés très tôt d'organisations « cyber », il manquait clairement une institution centrale en charge de tout le cyberespace civil[7]. La création de l'*Israel National Cyber Bureau* (INCB), en juillet 2011, est venue combler ce vide. Tous les acteurs civils du cyber – administrations gouvernementales, industriels, chercheurs, universitaires, enseignants – ont désormais un interlocuteur unique et central. L'INCB impulse une dynamique générale et participe au financement de projets (sans en être pour autant systématiquement à l'origine). L'INCB collabore également étroitement avec l'armée et le ministère de la Défense. L'*Israel National Cyber Bureau* joue ainsi un rôle de relais entre civil et militaire alors même que la frontière entre ces deux mondes est déjà poreuse en Israël. Depuis 2012, le ministère de la Défense dispose d'une administration centrale du cyber dont le rôle est d'encadrer et de coordonner les partenariats entre l'armée, les services de sécurité israéliens et les entreprises de cybersécurité. C'est un processus dans lequel tout le monde gagne vu que d'un côté le ministère de la Défense trouve des réponses techniques à ses problématiques spécifiques et que de l'autre les industriels accèdent à des financements privés ou publics pour leur R&D afin de développer les outils dont les militaires ont besoin.

Le soutien à la R&D constitue d'ailleurs un des piliers de la stratégie adoptée par le gouvernement israélien. L'INCB et le ministère de l'Industrie ont financé, par exemple, le projet « Kidma » dont l'objectif était de faire progresser la R&D en Israël afin de répondre aux besoins du marché local et mondial de la cybersécurité tout en favorisant dans le même temps l'entreprenariat en Israël[8]. L'INCB a également financé avec le ministère de la Défense le projet « Masad » dont l'objectif était de soutenir la R&D dédiée à la mise sur le marché de produits pouvant servir à la cybersécurité de l'armée et des infrastructures civiles[9]. C'est ce que les Israéliens appellent un projet dual : militaires comme civils doivent pouvoir utiliser les mêmes outils.

Conscient que les fonds alloués à la R&D ne suffisent pas, le gouvernement israélien a engagé une politique active pour inciter les entreprises étrangères à investir en Israël. La création du CyberSpark relève de cette volonté d'attirer les capitaux et les compagnies étrangères spécialisées en cybersécurité en Israël. Pour les dirigeants israéliens, cette industrie ne peut se développer pleinement et durablement sans ouverture vers l'extérieur. Cela pose toutefois certaines questions. Depuis plusieurs années, le gouvernement israélien se demande quelles règles adopter en matière d'exportation cyber étant donné la sensibilité de certains produits. Après 3 ans de discussion, le gouvernement israélien a codifié en 2016 la réglementation

---

[7] Les Israéliens ont mis en place au départ des structures spécialisées avec des prérogatives ciblées. Par exemple, pour répondre à la question de la protection des infrastructures critiques du pays, le Comité ministériel de la sécurité nationale a entériné en décembre 2002 le texte B/84 dont l'une des dispositions est la création de l'AGSI. L'agence est placée sous la tutelle directe des services de renseignement intérieur israélien le Shin Beth.

[8] Le bureau du Premier ministre a mis en ligne une fiche à propos de ce programme : http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Kidma%20Program.pdf

[9] Le bureau du Premier ministre a également mis en ligne une fiche à propos du programme « Masad » : http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Masad%20Program.pdf

régissant les exportations de l'industrie de cybersécurité sur la base « tout ce qui n'est pas spécifiquement interdit est autorisé »[10].

L'ouverture vers l'international vise à garantir des débouchés à l'industrie israélienne de la cybersécurité mais aussi à nouer des partenariats grâce auxquels les Israéliens pourront améliorer leurs connaissances et en acquérir de nouvelles. Israël a engagé des projets sur tous les continents : Stefanini (Brésil) et Rafael, Israël et le Nigéria pour lutter contre la cybercriminalité, Elbit System (pour 22 millions de dollars) et Israel Aerospace Industry (pour 40 millions de dollars) en Asie, coopération accrue avec les États-Unis (industries et renseignement), coopération renforcée avec Singapour (liens commerciaux et cybersécurité), accord avec l'Allemagne (nanotechnologie et cybersécurité). Ces quelques exemples ne concernent que l'année 2016.

Si l'État joue un rôle essentiel, il existe toutefois en Israël deux incubateurs dont il faut souligner l'existence. Un incubateur est une organisation dont le but est d'aider au développement et au succès de compagnies pas encore intégrées sur le marché qu'elles ciblent (mentorship, financements, partenariats, R&D). JVP Labs aide ainsi au développement de compagnies spécialisées en cybersécurité et en big data. JVP Labs a accompagné de grandes entreprises comme CyberArk ou Magnafire. C'est toutefois un incubateur sous licence du ministère de l'Economie contrairement à Team8 qui a été fondé par deux anciens de l'unité 8200. Team8 a récolté environ 23 millions de dollars en 2015 grâce à des partenariats avec des multinationales comme Nokia, AT&T, Accenture ou Alcatel-Lucent. Ce sont donc des sommes issues de fonds privés, qui complètent les investissements engagés par l'État, qui sont directement réinvesties dans l'économie israélienne de la cybersécurité.

IV. Le facteur humain : l'importance de la formation et des interactions entre spécialistes

Si Team8 est l'exemple parfait d'Israéliens qui ont fait le choix de monter leurs entreprises après avoir fait leur service militaire dans une unité cybernétique, ce n'est pas un exemple unique. Un quart des entrepreneurs israéliens dans le secteur de la cybersécurité sont des hommes et des femmes ayant effectué leur service militaire au sein d'une unité cyber de Tsahal.

---

[10] Il s'agit là d'une citation directe du Premier ministre israélien lors de la conférence CyberTech qui s'est déroulée à Tel-Aviv le 26 janvier 2016. L'intégralité de cette intervention est disponible en ligne sur : http://mfa.gov.il/MFA/PressRoom/2016/Pages/PM-Netanyahu-addresses-the-CyberTech-Conference-26-January-2016.aspx Les Israéliens ont en réalité aligné leur réglementation en matière de cybersécurité aux règles qui régissent les exportations militaires. Les compagnies spécialisées en cyber se retrouvent donc assimilées aux industries de l'armement. Voir AZULAI Yuval, « Cyber cos concerned about export restrictions », *Globes*, 14 janvier 2016, disponible en lignes http://www.globes.co.il/en/article-cyber-security-cos-concerned-about-export-restrictions-1001095244 et pour une analyse purement juridique du sujet voir MANSPEIZER Michele, « Should Israel legislate the export of cyber security ? », *Law offices*, 6 mars 2016, disponible en ligne http://www.law-m.co.il/single-post/2016/03/06/Should-Israel-Legislate-the-Export-of-Cyber-Security

Quasiment un autre quart, 22%, viennent des hautes technologies ou sont des hackers reconvertis. 18% sont des anciens employés de grandes entreprises IT[11]. Malgré ce vivier, le besoin en ressource humaine reste problématique en Israël. L'industrie de la cybersécurité croît tellement vite qu'elle peine à recruter suffisamment de personnes hautement qualifiées. Tsahal rencontre d'ailleurs les mêmes difficultés. C'est pour répondre à ces deux enjeux que le gouvernement israélien a décidé d'investir massivement dans la formation de sa jeunesse.

Parmi les initiatives engagées, deux projets se distinguent particulièrement des autres. « Magshimim » est un programme de 3 ans devant permettre à des jeunes âgés de 16-18 ans d'acquérir les bases en informatique (langage, programmation, fonctionnement des réseaux etc..). Lancé au départ pour 400 jeunes, le gouvernement israélien a décidé en 2013 d'en faire un programme national devant s'adresser à plus de 4800 jeunes. Un autre exemple illustre les efforts israéliens en matière de formation. « Gvahim » est un programme beaucoup plus restreint, clairement orienté « cybersécurité », dont l'objectif est d'enseigner à des jeunes de 16-18 ans les modes de défense et d'attaque dans le cyberespace. L'armée est très présente dans ce programme. Ces deux exemples montrent à quel point les dirigeants israéliens sont sensibles à l'idée de proposer un enseignement technique de haute qualité et exploitable rapidement par les industriels et surtout par les militaires.

L'État finance également des bourses d'études et de recherche[12]. Là où l'exemple israélien est intéressant, c'est que ces bourses concernent aussi bien des étudiants en sciences dures qu'en sciences humaines. La connaissance technique est donc autant valorisée que les compétences d'analyse touchant à la dimension humaine du cyber. Ces recherches interdisciplinaires sont la marque de fabrique de l'université de Tel Aviv. L'université de Haïfa (Technion) et l'université Ben Gourion de Beer Sheva dispensent, elles, un enseignement plus technique, avec une spécialisation plus marquée en cybersécurité pour l'université Ben Gourion. Ce n'est d'ailleurs pas un hasard si le gouvernement israélien a décidé d'installer son CyberSpark à Beer Sheva.

Ce projet annoncé en 2014, estimé selon certaines sources à près de 9 milliards de dollars, s'adresse aussi bien aux Israéliens qu'aux étrangers. Pour le Premier ministre israélien, il est primordial de favoriser un écosystème dans lequel tous les acteurs du cyber puissent se rencontrer et échanger rapidement. L'industrie de la cybersécurité doit au final profiter de toutes ces interactions humaines et de cette symbiose. La création du CyberSpark vise donc à réunir sur le même site géographique des industriels israéliens et étrangers, des centres de recherche privés et publics, des institutions publiques, de nouvelles structures universitaires autour de l'université Ben Gourion, les services de renseignement israélien et l'ensemble des unités cybernétiques de Tsahal dont le déménagement à Beer Sheva s'étale jusqu'à 2021. Le gouvernement israélien a mis en place une « tax break » en juillet 2014 afin de favoriser

---

[11] Ambassade de la République d'Inde à Tel-Aviv, « The Cybersecurity sector in Israel, preliminary market analysis », 2015, disponible en ligne https://www.indembassy.co.il/pages.php?id=6666700#.WE0sERrhDRY

[12] En 2012, ces bourses s'élevaient à 13 millions de dollars

l’installation des entreprises à Beer Sheva ainsi que des mesures d’incitation pour encourager les Israéliens à s’installer dans cette ville.

La création du CyberSpark stimule profondément, et dans la durée, l’industrie de la cybersécurité en Israël tout en favorisant le développement économique du sud à travers des projets immobiliers, la construction de centres commerciaux et l’installation de populations jeunes et actives dans cette partie du pays connue pour être moins dynamique que le centre. Le CyberSpark redynamise donc le sud d’Israël. Pour les Israéliens, c’est la preuve que le cyber constitue une révolution industrielle dont les conséquences dépassent ce simple secteur d’activité et dont la croissance entraîne avec elle l’ensemble de l’économie du pays.