



Un aperçu des efforts israéliens dans le domaine cybernétique

*Olivier Danino. Chercheur au sein de l'Institut français d'analyse stratégique (IFAS)
Membre du Cercle des chercheurs sur le Moyen-Orient (CCMO)*

Mars 2015, Article III.21

Depuis plusieurs années, l'Etat d'Israël cherche à devenir un leader mondial dans le domaine cybernétique. Si la stratégie israélienne ne fait pas encore l'objet d'un document officiel de doctrine, sur lequel l'*Israel National Cyber Bureau* (INCB) travaille depuis sa création (le 11 juillet 2011), il n'en reste pas moins que le gouvernement Netanyahu prend plusieurs initiatives qui traduisent clairement la vision d'Israël. Les efforts sont portés sur la formation de la jeunesse, l'industrie de sécurité des systèmes d'information, la recherche privée et publique et les capacités défensives et offensives de l'armée¹.

1 - La jeunesse

La formation des jeunes est un enjeu majeur qui doit permettre à Israël de disposer à termes d'un vivier humain ayant un savoir-faire technique de haut niveau dans le domaine cybernétique. Ce secteur recrute massivement mais il peine à trouver du personnel qualifié. Il en va de même au sein de l'armée où les besoins de certaines unités augmentent rapidement. C'est pourquoi, l'Etat développe des programmes spécialisés pour les 15-18 ans. Le baccalauréat israélien est composé d'une base commune à tous les lycéens qui est complétée par des options permettant une spécialisation du diplôme. Les options informatiques ne sont pas une nouveauté. La programmation, par exemple, était déjà enseignée depuis plusieurs années. Par contre, la mise en place de programmes répondant spécifiquement aux besoins de recrutement de l'armée est plus récente.

Ainsi, fin 2012 – début 2013, le gouvernement israélien a lancé en collaboration avec Tsahal, les services de sécurité, la Fondation Rashi, le ministère de l'Education et l'*Israel National Cyber Bureau*, un programme national pour les élèves de première et de terminale intitulé en hébreu *Magshimim*². Ce programme s'adresse aux habitants de la périphérie du pays (certaines villes côtières en

¹ Pour une analyse de la stratégie cybernétique israélienne voir Olivier DANINO, *La cyberstratégie de l'Etat d'Israël*, Sécurité Globale, n°24, 2013/2, p. 15-24.

² Pour en savoir plus sur ce programme voir le site <https://www.magshimim.net/Default.aspx?KPages=492> (source en hébreu).

particulier) et est axé dans un premier temps sur l'acquisition des bases en informatique (langages informatiques, fonctionnement de l'Internet et des réseaux). Les jeunes qui intègrent ce programme augmentent ainsi leur chance de servir par la suite dans une unité cybernétique de l'armée. La presse israélienne le décrit comme un « *cyberwarfare program* » de haut niveau. Après le conflit qui s'est déroulé entre le Hamas et Israël lors de l'été 2014, plusieurs jeunes inscrits dans ce programme ont demandé à le quitter pour intégrer des unités combattantes.

Cette initiative s'inscrit parmi tant d'autres. Une en particulière qui date exactement de la même époque. Il s'agit du programme *Gvachim*³. Soutenu par les mêmes acteurs institutionnels que *Magshimim*, *Gvachim* ne s'adresse par contre qu'aux élèves du centre du pays et a été implanté uniquement dans dix lycées israéliens. Un an après le lancement de ce programme, un concours parrainé par l'unité 8200 s'est déroulé au sein de ces dix écoles. L'objectif pour les participants était de neutraliser des serveurs tout en protégeant les leurs d'une attaque. L'intérêt de ce concours était double : renforcer l'émulation entre lycéens et permettre à l'armée de détecter les meilleurs élèves.

2 - L'industrie spécialisée dans la sécurité en système d'information (SSI)

Le deuxième pilier, après celui de la formation de la jeunesse, est celui du soutien à l'industrie SSI. Le gouvernement israélien injecte effectivement d'importantes sommes d'argent dans ce secteur d'autant plus qu'il est perçu par les politiques comme créateur d'emplois et de croissance économique. Les sommes allouées par l'Etat sont principalement utilisées par les départements de Recherche et de Développement de ces industries spécialisées dans la sécurité des systèmes d'information. En 2013, ces-dernières se sont vues attribuer près d'un demi-milliard de shekels, soit environ 125 millions de dollars, afin de soutenir leur effort en R&D. Cette décision est conforme aux recommandations faites en 2011 par le Conseil national pour la recherche et le développement suite à la commande par le Premier ministre Netanyahu, en 2010, d'un rapport sur les enjeux du Cyber en Israël⁴.

En soutenant les entreprises de SSI, le gouvernement israélien cherche aussi à satisfaire ses propres besoins. L'idée étant de garantir aux institutions militaires, gouvernementales et aux infrastructures critiques du pays des outils efficaces et sécurisés à l'image du logiciel *Telepath* développé par Hybrid Security. C'est un support qui n'est pas exclusivement réservé à l'Etat, puisqu'il est disponible pour tous, mais qui est utilisé par plusieurs infrastructures nationales en Israël. *Telepath* est capable de détecter des comportements suspects sur l'Internet et sur les Intranets. Plus récemment, en février 2015, Rafael, qui gère notamment les outils de défense du système d'information du « Dôme de Fer », a annoncé développer son offre commerciale en voulant fournir des solutions pour protéger les systèmes SCADA⁵. Certaines offres peuvent être toutefois plus exclusives. Ainsi, en juin 2012, Elbit System a mis en place un simulateur destiné à l'entraînement des agences civiles et militaires en charge de la défense du cyberspace israélien.

³ La presse israélienne (notamment Haaretz et Times of Israel) s'est faite l'écho de ces initiatives dans plusieurs articles dont la très grande majorité est accessible en anglais.

⁴ Pour un résumé des recommandations faites par le Conseil national pour la recherche et le développement voir Lior Tabansky, *Cyberdefense Policy of Israel: Evolving Threats and Responses*, disponible en ligne sur le site de la Chaire de cyberdéfense et Cybersécurité, http://www.chaire-cyber.fr/IMG/pdf/article_3_12_-_chaire_cyberdefense.pdf

⁵ Les systèmes SCADA (*Supervisory Control And Data Acquisition*) sont des systèmes automatiques organisant certaines infrastructures, notamment dans les secteurs de l'eau, de l'électricité et des transports.

Néanmoins, le souhait du gouvernement israélien est de rayonner à l'échelle mondiale. Il ne veut donc pas se contenter de fournir des produits au marché israélien mais bien conquérir des parts de marché à l'international. C'est pourquoi, Israël noue des partenariats avec plusieurs pays à l'instar de l'Italie, du Japon et de l'Inde. Les entreprises de SSI israéliennes sont des acteurs majeurs de ces accords de cyberdéfense. Les collaborations entre Israël et l'étranger concernent également la Recherche et le Développement à l'instar du centre ouvert à Singapour en février 2014. L'agence spatiale israélienne, IAI, participe à ce projet dont l'objectif est de développer des solutions pour détecter une menace en cours dans le cyberspace avant même que celle-ci ne se révèle effective. La R&D n'est pas le seul domaine concerné, les entreprises de SSI proposent également des solutions pour sécuriser les systèmes d'information d'organismes étrangers. En novembre 2014, la division sécurité de MER Group a signé un contrat avec le fond de pension gouvernemental du Mexique. Le projet s'inscrit sur plusieurs années au cours desquels MER Security fournira notamment les outils nécessaires à la protection des systèmes d'information du fond de pension.

Il est important de souligner que la recherche industrielle n'est pas la seule soutenue par le gouvernement israélien qui porte également une attention particulière à la recherche universitaire. L'INCB s'est d'ailleurs joint, dès 2012, au ministère des Sciences et des Technologies pour encourager celle-ci. Près de 50 millions de shekels, soit environ 13 millions de dollars, ont ainsi été engagés pour financer des bourses d'études et de recherche dans plusieurs universités du pays. Les domaines concernés ne sont pas uniquement techniques. L'une des originalités en Israël est effectivement que les enjeux du cyber ne sont pas restreints aux études d'ingénieur ou d'informatique. A l'université de Tel-Aviv, par exemple, des étudiants travaillent sur la psychologie des hackers afin de mieux comprendre leurs mécanismes d'action (individuel ou en groupe).

3 - Tsahal

L'armée israélienne dispose d'un savoir-faire défensif et offensif à travers plusieurs unités spécialisées dont la plus connue reste l'unité 8200. Celle-ci a plusieurs unités sous sa direction, comme l'unité *Hatzav* qui collecte du renseignement en source ouverte, ou encore une unité de commandos d'élite qui intervient directement sur le terrain. Le *Computer Service Directorate* (CSD), appelé en hébreu *Agav atikshouv*, est une autre structure qui s'impose dans le dispositif militaire israélien. Le CSD regroupe trois branches différentes à savoir l'unité C4I, une brigade opérationnelle et l'unité *Lotem*, spécialisée en télécommunication et en technologie de l'information et elle-même subdivisée en plusieurs unités spécialisées⁶.

Néanmoins, la structure militaire israélienne est en constante évolution. En 2009, une sorte d'état-major cyber est créé au sein de l'unité 8200 dont le rôle est de coordonner et diriger les activités de l'armée dans le cyberspace. Les soldats de cet organisme appartiennent aussi bien à l'unité 8200 qu'au CSD. En janvier 2012, dans un souci d'organisation et d'efficacité, le ministère de la Défense israélien se dote d'un organisme central afin de mieux encadrer les partenariats entre l'armée, les services de sécurité israélien et les entreprises privées de SSI.

L'outil cybernétique n'est toutefois pas restreint aux unités spécialisées. Ainsi, par exemple, l'unité *Yahalom*, qui appartient au Génie militaire, utilise lors de ses opérations des robots perfectionnés

⁶ Délégation aux Affaires stratégiques (Olivier Danino), « l'utilisation stratégique du cyber au Moyen-Orient », Ministère de la Défense, mai 2013, <http://www.defense.gouv.fr/das/la-delegation/evenements/restitution-etude-utilisation-strategique-du-cyber-au-moyen-orient-22-avril-2013/restitution-etude-utilisation-cyber-au-moyen-orient-22-avril-2013>

comme le « EyeDrive », un robot tout-terrain⁷. L'une des missions de l'unité *Yahalom* est la recherche de caches d'armes et de tunnels. Elle est notamment intervenue avec le « EyeDrive » lors de l'opération menée par Tsahal dans la bande de Gaza durant l'été 2014. A termes, l'armée israélienne s'est fixée comme objectif de diffuser ce savoir-faire cybernétique à toutes ses unités.

Depuis le milieu de l'année 2012, les officiers supérieurs, principalement ceux de l'infanterie, des brigades d'artillerie et des blindés, doivent d'ailleurs suivre une formation afin que la dimension cybernétique soit prise en compte dans leur commandement. C'est le CSD, à travers l'unité C4I, qui est en charge de ces cours. En février 2014, l'armée a mis en place un deuxième cours destiné à des officiers supérieurs ayant déjà une expérience opérationnelle en cyber défense afin de les sensibiliser davantage aux enjeux et aux risques du cyber.

L'armée israélienne est donc en constante évolution. La réflexion stratégique menée au sein de Tsahal concerne aussi bien la répartition des responsabilités dans l'organisation générale de l'armée que l'acquisition de nouvelles compétences techniques, défensives comme offensives. Mais pas seulement. L'état-major souhaite également que l'ensemble des unités de l'armée intègrent les outils cybernétiques dans leur fonctionnement et que les personnels gradés soient formés aux enjeux du cyber même si ces-derniers ne sont pas directement concernés par ce domaine d'activité.

4 - La création du « CyberSpark »

La création du « CyberSpark » reflète parfaitement les ambitions d'Israël qui ne souhaite pas se contenter de soutenir séparément les secteurs industriels, militaires, de la recherche et de l'éducation mais bien de réaliser une symbiose entre ces différents mondes. L'objectif étant bien entendu le partage d'expérience, l'émulation et la mise en commun d'un savoir-faire propre à chacun de ces secteurs afin d'éviter la dispersion et la perte de connaissance.

Influencé par son expérience aux Etats-Unis, lorsqu'il y était étudiant, le premier ministre israélien a décidé de créer à Beer-Shev'a un complexe dédié au cyber visant à réaliser cette symbiose : le « CyberSpark »⁸. Le projet, annoncé en janvier 2014 et estimé par la presse israélienne à 9 milliards de dollars, doit réunir sur le même site des industriels israéliens et étrangers, des études universitaires, des centres de recherche privés et publics, des institutions publiques et l'ensemble des unités cybernétiques de Tsahal.

Le site choisi pour l'établissement du « CyberSpark » est tout proche de l'université Ben Gourion, elle-même reliée par le chemin de fer israélien à l'université de Tel-Aviv. Ces deux universités sont en Israël deux institutions importantes dans le domaine de la recherche et de l'analyse cybernétique. Plusieurs entreprises ont déjà annoncé leur participation à ce projet comme Microsoft, Deutsche Telekom ou encore Lockheed Martin. En avril 2014, l'INCB, l'université de Ben Gourion et Tsahal ont signé un accord de 8,5 millions de dollars afin d'établir un centre de recherche au sein du « CyberSpark ». Enfin, le premier CERT israélien, créé en novembre 2014 au sein de l'INCB, et basé donc à Tel-Aviv, déménagera ses bureaux pour rejoindre le site de Beer-Shev'a au courant de l'année 2015 ou au début de l'année 2016. Le projet est donc en cours et semble trouver un écho favorable au sein de l'ensemble des acteurs du cyber en Israël, locaux comme internationaux.

⁷ L'armée israélienne a consacré un article complet sur cette unité dans la version française de leur site Internet : <http://tsahal.fr/2012/04/17/yahalom-lunite-delite-qui-fait-face-au-terrorisme-a-laide-dune-technologie-de-pointe/>

⁸ Voir la communication officielle du Ministère des Affaires étrangères, PM Netanyahu opens Cybertech 2014, annonces creation of CyberSpark in Beer Sheba, 27 janvier 2014, <http://mfa.gov.il/MFA/PressRoom/2014/Pages/PM-Netanyahu-to-open-Cybertech-2014-.aspx>

Conclusion

Ce rapide aperçu des efforts israéliens en matière cybernétique montre que le gouvernement Netanyahu a fait de ce domaine d'activité une priorité stratégique. Israël n'est pas uniquement centré sur les capacités de son armée mais aussi sur ceux de ses industries et de sa recherche privée et publique en sachant que les objectifs fixés ne pourront pas être atteints sans une ressource humaine qualifiée et compétente. D'où l'importance donnée à la formation de la jeunesse. Les cours proposés aux jeunes de 16-18 ans sont non seulement spécialisés mais ils répondent clairement aux besoins de l'armée, permettant à celle-ci au final un recrutement de meilleure qualité. A la fin de leur service militaire, à 20 ans pour les femmes et à 21 ans pour les hommes, ces jeunes disposent donc déjà d'un bagage théorique et pratique de très haut niveau pour leur âge qu'ils mettent soit au service de l'Etat soit au service d'entreprises privées spécialisées en sécurité des systèmes d'information. C'est là l'une des forces du modèle éducatif israélien.

Chaire Cyber-Défense et Cyber-sécurité

Fondation Saint-Cyr, Ecole militaire, 1 place Joffre, 75007 Paris
Téléphone: 01-45-55-43-56 - courriel: contact@chaire-cyber.fr; SIRET N° 497 802 645 000 18
La chaire remercie ses partenaires



CENTRE DE RECHERCHE
DES ECOLES DE
SAINT-CYR CDÉQUIDAN



THALES