# Cybersécurité : ambitions israéliennes et positionnement des acteurs défense

Le marché de la cybersécurité est l'objet de nombreuses estimations qui varient considérablement en fonction du périmètre qui lui est appliqué. Par exemple, au Royaume-Uni, l'agence gouvernementale UKTI estime que le marché mondial du secteur de la cybersécurité avoisinait en 2011 les 123 Mds£ (~196 Mds$)[1]. Le rapport *MarketandMarkets* considère de son côté le montant du marché en 2015 à 106,32 Mds$[2]. Enfin, pour la même année, VisionGain l'évalue à 75,4 Mds$[3]. Toutefois, les prévisions s'accordent sur une croissance forte et constante à court et moyen terme.

Depuis 2013, les autorités israéliennes publient également des données relatives au marché de la cybersécurité. Cette communication fait ainsi partie intégrante de la stratégie plus globale visant à renforcer l'image du pays sur la scène internationale en tant que nation leader dans le domaine. Ainsi, à l'occasion de la conférence d'Herzliya en 2014, l'*Israel National Cyber Bureau* (INCB) précisait, selon ses estimations, que l'État hébreu se positionnait au deuxième rang mondial des exportateurs de solutions de cybersécurité[4], derrière les États-Unis. Avec un total cumulé de 3 Mds$, le montant des exportations réalisées par les entreprises israéliennes serait ainsi trois fois supérieur à celui des entreprises britanniques[5], qui ferment le podium des principaux exportateurs. Toujours selon l'INCB, les exportations auraient augmenté d'au moins 10% en 2015[6] pour atteindre environ 3,5 Mds$. Isaac Ben-Israel, responsable de l'*Interdisciplinary Cyber Research Center* (ICRC) de l'Université de Tel Aviv déclarait en juin 2015 : « *Last year [2014], Israeli cyber exports constituted about 8 percent of the global market. This year [2015] it's 10 percent* »[7]. Cependant, les déclarations de l'INCB réalisées en janvier 2016 viennent largement pondérer les chiffres présentés par l'ICRC : « *Based on all accepted estimates, the global market for cyber is about $75 billion, which points to an Israeli share of the market of some 5 percent. And if we look at the market for products only, Israel's share is estimated at 7 percent* »[8].

## Renforcement des compétences nationales et création d'un cluster de cybersécurité

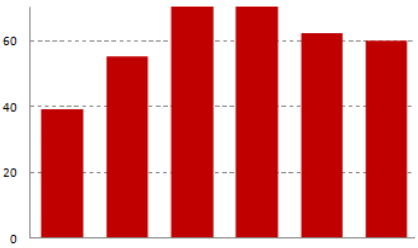
Suite à la *National Cyber Initiative,* lancée en 2010 par Benyamin Netanyahou, l'État hébreu a révisé sa politique en matière de cybersécurité[9], affichant désormais de très fortes ambitions tant sur le plan du renforcement des capacités nationales de cybersécurité qu'en matière d'exportation de solutions. Les recommandations issues de cette initiative, qui entendent promouvoir Israël parmi les cinq "superpuissances cyber" dans le monde, ont été adoptées dans le cadre de la résolution 3611 datée du 7 août 2011[10]. L'un des aspects clés est la création de *l'Israel National Cyber Bureau* (INCB). Placé sous le contrôle du bureau du Premier ministre, l'INCB dispose d'un budget initial (2010-2015) de 2,5 Mds NIS (soit ~ 130 M$/an)[11].

Le mandat de l'INCB couvre le développement de la filière israélienne de cybersécurité. Outre le pilotage de programmes de R&D (*Kidma* notamment[12]), l'INCB prend part au *Beersheba Advanced Technological Park* (ATP). Inauguré en septembre 2013[13], l'ATP illustre la volonté du gouvernement israélien de renforcer en priorité les capacités nationales d'innovation et de R&D dans le domaine de la cybersécurité. Bénéficiant d'un investissement d'environ 8 à 9 Mds NIS sur 5 ans (~2,1 à 2,4 Mds$)[14], l'ATP prend la forme d'un partenariat public-privé comprenant l'Université Ben Gourion (BGU) et l'entreprise KUD international LLC[15]. Le projet vise à transformer la ville de Beersheba en un véritable cluster mondial de l'innovation dans le domaine de la cybersécurité (19 hectares dédiés). L'objectif est de créer une synergie entre les secteurs académique, privé (notamment avec les centres de R&D étrangers) et militaire. Dans ce cadre, l'INCB a noué un partenariat avec l'Université Ben Gourion (BGU) afin de créer un centre de recherche au sein du *CyberSpark* (association initiée par l'INCB et créée par BGU, Lockheed Martin, EMC et Jerusalem Venture Partners en charge de la planification, coordination et promotion du cluster).

Selon le cabinet israélien *IVC Research Center*, la filière nationale de cybersécurité compte 430 entreprises et 40 centres de R&D privés étrangers[16]. Cette dernière, composée en majorité de start-up (création en moyenne de 52 start-up/an depuis 2000) et d'éditeurs de logiciels spécialisés sur des segments relais de croissance (SCADA industriels, Objets connectés, Renseignement d'origine cyber, etc.) profite des politiques nationales (création d'un cluster à rayonnement mondial, captation des IDE, encouragement des investissements de type *Venture Capitals, etc.)* pour se développer très rapidement.

Si l'éditeur de logiciels Check Point Software Technologies (technologies firewall) représente la tête de pont historique de la filière israélienne de cybersécurité (CA 2014 de 1,5 Md$), les groupes de défense Rafael, IAI et Elbit Systems en constituent également des acteurs clés.

**Filière israélienne de cybersécurité**
Nombres d'entreprises créées sur le territoire national




Source : Cabinet *IVC Research Center,* 2016

## Acteurs défense et cybersécurité : quelles stratégies de pénétration ?

Au sein des principaux Etats producteurs et exportateurs d'armement, les industriels de la défense ont progressivement pénétré le marché de la cybersécurité (et plus généralement de la « sécurité ») dans un contexte de contraction des commandes d'équipements de défense. Identifié comme potentiel relais de croissance, le marché de la cybersécurité a vu se positionner les fournisseurs historiques de la défense, avec notamment aux États-Unis, Raytheon, Lockheed Martin et Northrop Grumman (pour ne citer que les principaux), et en Europe, BAE Systems, Airbus Defence & Space, Thales, Safran et Finmeccanica.

En effet, ces acteurs défense disposent d'atouts qu'ils peuvent mettre à profit sur le marché de la cybersécurité, parmi lesquels des capacités d'intégration et de maîtrise d'œuvre de programmes complexes, une relation privilégiée avec le client étatique national et une empreinte internationale. Par ailleurs, le développement d'une offre en matière de cybersécurité par ces derniers peut dériver de « spin-in » de technologies défense et/ou résulter d'une stratégie de croissance externe et/ou de partenariats. Ainsi les groupes de défense ont-ils été ces dix dernières années à l'origine de nombreuses opérations de rachats d'entreprises, avec pour cœur de cible les acteurs de la cybersécurité (PME, ETI et filiales de grands groupes). Cette extension de leur portefeuille de produits/services leur permet d'atteindre de nouveaux marchés, en diversifiant leur portefeuille clients vers d'autres administrations voire des acteurs privés.

La consolidation de leur offre de cybersécurité passe généralement par les axes stratégiques suivants :

- Création d'une ligne d'activités dédiée à la cybersécurité. Par cette stratégie, les acteurs défense visent en priorité le marché Défense domestique, les administrations publiques (nationales et internationales) et les opérateurs d'importance vitale (OIV). De plus, l'intégration de solutions sur étagères, *via* le développement de partenariats avec les leaders mondiaux de la cybersécurité, permet de renforcer cette ligne d'activités.
- Mise en place d'une filiale cybersécurité dédiée, laquelle consolide les activités des acteurs spécialisés rachetés par le groupe de défense. Ce dernier peut ainsi bénéficier de leurs canaux de ventes. Si ces entités nouvellement acquises disposent d'une « marque » forte (très bonne visibilité auprès des clients finaux), celle-ci peut être préservée.
- Adoption d'une stratégie multidomestique avec la création *ex-nihilo* d'une filiale (société de droit local) ou l'acquisition d'un acteur local, qu'il soit consultant ou éditeur de logiciels. De cette manière, les groupes de défense peuvent également nouer des relations directes avec les clients « Défense » étrangers. Ainsi, quand la R&D est réalisée localement, les entreprises se positionnent-elles en tant que « fournisseur domestique » (solutions de souveraineté).
- Insertion de clauses de cybersécurité dans les accords G2G (*Government to Government*). Dans le cadre de contrats d'armement, une offre cyber peut être intégrée. Bien que minoritaire aujourd'hui et résultant de demandes clients, ce type d'offre est voué à croître et à se systématiser.

Néanmoins, rappelons que le nombre important d'acteurs potentiellement victimes de cyber-attaques crée une hétérogénéité des profils de clients finaux, contraignant les groupes de défense à adapter leur stratégie de pénétration aux segments visés. Une étude publiée en 2013 par le *Department for Business Innovation and Skills* britannique (BIS) mettait ainsi en exergue 4 sous-ensembles de marchés[17] disposant de dynamiques propres : Défense & Renseignement, Gouvernement, entreprises transnationales et ETI, PME & consommateurs. Ainsi, le sous-ensemble « Défense » représente-t-il un marché de niche, la demande étant tirée principalement par le secteur civil (administrations publiques et OIV).

En diversifiant leur portefeuille clients vers le secteur civil –généralement par le biais d'une stratégie de croissance externe– les groupes de défense se trouvent en concurrence frontale avec les acteurs historiques de la cybersécurité, au premier rang desquels les éditeurs de logiciels spécialisés et les entreprises de services du numérique (ESN, ex-SSII). Par ailleurs, ils se positionnent sur un marché dont le modèle économique n'est pas toujours adapté à leurs activités historiques. Ainsi, l'association française des éditeurs de logiciels (AFDEL) estime pour sa part que « *Les groupes de Défense, s'ils bénéficient de la taille, de la structure financière et d'une vraie culture de la sécurité des systèmes d'information critiques et des produits gouvernementaux, ne disposent pas de marques reconnues sur ces segments de marché (hors Défense). Ils ne disposent ni des canaux de vente ni de la culture du management propre à l'industrie du logiciel. Ils définissent des stratégies fondées sur le retour sur investissement sur la base des cashflow, là ou un investisseur en capital-risque aura pour objectif de réaliser une plus-value actionnariale. Or, si ce mode de raisonnement est bien adapté au monde industriel, il ne l'est pas pour des sociétés technologiques en forte croissance* »[18].

Cet argumentaire semble faire écho aux dernières décisions prises par les groupes de défense américains. En effet, après avoir racheté à prix d'or des acteurs *pure-players*, Raytheon et Lockheed Martin ajustent depuis leur positionement, en particulier sur le marché civil de la cybersécurité. Suite à la finalisation, en janvier 2016, des acquisitions de Stonesoft et Sidewinder auprès d'Intel Security, Raytheon a précisé que les solutions issues des deux filiales seraient regroupées avec celles de Raytheon Websense, pour former la nouvelle entité ForcePoint. Raytheon poursuit ainsi la consolidation de ses activités de cybersécurité (en 10 ans, le groupe a investi plus de 3,5 Mds$ dans le domaine), désormais regroupées au sein d'une « marque » dédiée, visible des clients finaux. A l'inverse, Lockheed Martin a prévu d'opérer un recentrage sur ses activités défense, avec la vente ou la création d'une spin-off de sa BU *Information Technology*.

La montée en compétences des groupes de défense israéliens dans le domaine de la cybersécurité (Rafael, IAI et Elbit Systems) constitue également une excellente illustration des voies et moyens mobilisés par les fournisseurs historiques des armées pour pénétrer ce marché.

### Rafael et IAI : l'option du « partenariat »

Troisième groupe de défense israélien derrière IAI et Elbit Systems, Rafael se présente comme un acteur historique de la cyberdéfense, revendiquant 15 ans d'activités sur ce segment[19]. L'entreprise a ainsi acquis une expertise de niveau mondial dans le domaine des algorithmes, issue notamment du développement du système de défense aérienne de courte portée *Iron Dome*. Les activités de cybersécurité / cyberdéfense sont consolidées au sein de la branche *Air&C4ISR Systems*, sous l'appellation *Administration Intelligence & Cyber* (dirigée par Ariel Karo).

Cette entité a pour vocation de coordonner les activités cyber existantes et de proposer une stratégie de développement.

Toutefois, l'affichage d'une ligne de solutions de cybersécurité demeure très récente[20]. En mai 2011, Rafael a mis en place une unité en charge du développement de solutions de cybersécurité, localisée sur le site de Leshem (entité de l'ex-division Missiles). Le groupe entend commercialiser ces dernières sous la marque Cyber-Dome[21], ciblant principalement les marchés Défense, Administrations publiques et OIV. Pour ce faire, Rafael développe ses solutions de cybersécurité sur la base de produits / technologies déjà existants (spin-in) tout en multipliant des coopérations au sein du tissu industriel et académique national. En novembre 2014, en partenariat avec mPrest (détenu à 50% par Rafael[22]) et *Israel Electric Corporation* (IEC), le groupe israélien a lancé « *Information grid* », un système de contrôle et de commandement de réseaux de puissance électrique[23]. Cette solution a été exportée pour la première fois, en janvier 2015, au Canada[24]. Par ailleurs, Rafael profite de sa relation étroite avec le gouvernement israélien pour accélérer le développement de ses activités de cybersécurité. Historiquement très dépendante des commandes des forces armées israéliennes (environ 50% de son CA), l'entreprise a remporté, en juin 2015, le marché relatif à la construction du CERT national, opéré sous la direction de l'INCB[25]. En tant que maître d'œuvre, Rafael travaille avec une équipe composée d'IBM, EMC, Cisco et Matrix. Le PDG de Rafael, Yeddida Yaari, déclarait ainsi dans ce contexte : « *Rafael's selection by the Israël government is a strategic development for the company. (…) We are now ready to leverage our expertise in Cyber technology, together with our new partners* »[26].

Premier groupe de défense israélien avec un CA 2014 de 3,83 Mds$, IAI identifie également le segment cybersécurité comme un relais de croissance de premier ordre : « *IAI also sees a great deal of potential in its cyber activities that are designed for both the defense and the commercial markets. This year, the Company has conducted major transactions in its target markets based on its innovative and idiosyncratic capabilities in the cyber field* »[27]. IAI n'aura toutefois dévoilé ses solutions de cybersécurité qu'à compter de 2013. Avec des axes de développement orientés vers les domaines du renseignement, des systèmes d'alerte et de commandement et de contrôle, le groupe a introduit les deux nouvelles familles de solutions TAME[28] et ELS-8910.

En septembre 2015, à l'image de Rafael, IAI a été sélectionné par le gouvernement israélien afin de mettre en œuvre un réseau sécurisé d'échanges de données entre organisations nationales et CERT relatif au renseignement d'intérêt cyber[29]. Par ailleurs, depuis deux ans, IAI a établi un partenariat stratégique avec la PME israélienne Cyberia, et ce, en lien avec les activités réalisées au sein du *R&D Cyber Accessibility*[30] (développement et commercialisation de nouvelles solutions de cybersécurité). Dans ce cadre, Cyberia se voit chargée du développement de prototypes sur la base de nouvelles technologies identifiées par IAI. Les ingénieurs du groupe ont ensuite pour mission de transformer le prototype en solution mature en vue d'une commercialisation. Ce partenariat a permis de développer les solutions Nimbus (interception de données dans le cloud) et CyFi (interception de communications wifi). Plus récemment (janvier 2016), IAI a opté pour le développement d'un partenariat avec le prestataire de services Formula Systems, dans le cadre de l'acquisition de la filiale TSG de Ness Technologies (montant total de 50 M$)[31]. Si cet accord conduit pour l'instant à la mise en place d'une coentreprise, il pourrait néanmoins laisser présager un futur partenariat plus structurant entre le fournisseur de solutions (IAI) et le prestataire de services (Formula Systems).

A l'international, IAI a ouvert en 2014, un centre dédié R&D cybersécurité à Singapour, avec le soutien financier du gouvernement singapourien[32]. Les principaux domaines de recherche traités visent à l'identification des cyber-attaquants, leur géolocalisation et le développement des capacités de détection avancée des anomalies. Nommé « Custodio », ce centre de recherche permet aussi à IAI de renforcer sa présence sur le marché singapourien où le groupe dispose déjà d'un positionnement réussi sur d'autres segments (drones Heron-I et avions de reconnaissance G-550 modifiés). En effet, les clients défense historiques d'IAI sont des prospects idoines pour l'exportation de solutions de cybersécurité. Par exemple, en janvier 2015, IAI faisait état de l'obtention de deux contrats majeurs dans le domaine cyber obtenus auprès de clients défense stratégiques : « *Israel Aerospace Industries (IAI) concludes 2014 with cyber-solution contracts totaling tens of millions of dollars. Two significant contracts were signed with strategic, foreign, defense customers* »[33].

### Elbit Systems : l'option de la « filiale dédiée »

Premier groupe de défense privé israélien avec un CA 2014 de 2,96 Mds$[34], l'intégrateur-systémier Elbit Systems a pris une place prédominante au sein du tissu industriel de cybersécurité israélien. Ce positionnement s'est construit en plusieurs étapes :

- 2009 : développement en interne de solutions issues de technologies existantes (spin-in).
- à partir de 2011 : acquisitions ciblées.
- juin 2015 : consolidation des activités cyber au sein d'une filiale dédiée, Cyberbit.

En 2009, Elbit Systems crée l'entité *Intelligent & Cyber Solutions*[35] (division Elop). Celle-ci développe la technologie WiT (*Wise Internet Technology*)[36], un système de renseignement d'origine cyber utilisé par la police israélienne. En outre, l'entité travaille sur le développement de solutions de cybersécurité relatives aux systèmes de commandement et de contrôle et aux simulateurs dédiés à l'entraînement et la formation. Dans ce cadre, Elbit Systems dévoile en 2012 une nouvelle solution de simulateur cyber[37]. Celle-ci intègre la solution de générateur de trafic développée par l'entreprise américaine Breaking Point (rachetée par Ixia en 2012[38]).

Parallèlement au développement de nouvelles solutions, Elbit Systems met en œuvre, dès 2011, une stratégie de croissance externe ciblée vers le secteur de la cybersécurité, avec la prise de contrôle de la PME C4 Security Ltd, pour un montant de 10,9 M$[39]. Employant 30 salariés, l'entreprise israé-

lienne est spécialisée dans le *reverse engineering*, les systèmes SCADA et l'identification de sources d'attaques. En plus d'étendre son portefeuille de solutions, cette acquisition permet à Elbit Systems de proposer une offre à destination du marché civil. De plus, en mai 2015, Elbit Systems annonçait avoir trouvé un accord avec NICE Systems pour l'acquisition de la branche Cyber & Intelligence (158 M$). Le PDG de la firme israélienne déclarait alors : « *The acquisition of NICE's division is a significant milestone in our strategy to bring Elbit Systems cyber capabilities to the level of global leaders. NICE is a well- known world leader in the cyber intelligence industry, and its business activities and capabilities are complementary to ours. The acquisition will enable us to provide our customers with end-to-end, market leading cyber solutions* »[40]. Spécialisée dans les solutions de renseignement bout-en-bout à destination des forces de l'ordre (interception de communications, analyse et investigation), la division de NICE Systems a réalisé en 2014 un CA d'environ 80 M$.

A la suite, Elbit Systems entreprend de consolider l'ensemble de ses activités au sein d'une filiale spécialisée, Cyberbit. Celle-ci regroupe les capacités internes (soit 215 employés en 2014[41]) ainsi que les activités de la division *Cyber & Intelligence de* NICE Systems. Cyberbit devrait réaliser un CA 2015 de 150 M$ et compter près de 500 employés. L'objectif affiché par Adir Dar, PDG de la filiale cyber, est dorénavant d'installer la « marque » Cyberbit au sein du marché civil sur les segments relatifs à la surveillance et la gestion du réseau : « *Without a doubt, the cyber world is based extensively on branding. We want to develop a leading global brand* »[42].

Cyberbit peut également capitaliser sur l'empreinte internationale d'Elbit Systems (78% du CA 2014 réalisé à l'export). Ainsi, la filiale dispose-t-elle de centres de services régionaux sur les continents asiatique, nord-américain et africain, couvrant de la sorte 20 pays[43]. Dès août 2015, Cyberbit annonce ses premiers succès à l'export (solutions de renseignement auprès d'un client africain et européen)[44]. Parmi les leaders mondiaux dans le domaine des simulateurs cyber[45], sa solution phare a été acquise en 2014 par le gouvernement singapourien via le conglomérat ST Engineering[46] (simulateur cyber destiné à des applications civiles et opéré par la filiale Info-Security de ST Electronics) ainsi que par l'entreprise suisse RUAG Defence[47].

Avec le développement de leurs activités cybersécurité, les groupes de défense israéliens se placent *de facto* en tant qu'acteur pivot de la filière nationale. De plus, au-delà d'une stratégie de croissance externe, Elbit Systems, Rafael et IAI se présentent comme de nouveaux partenaires stratégiques des PME israéliennes spécialisées et des OIV nationaux (IEC par exemple). Enfin, ils contribuent à renforcer l'image d'Israël en tant que pays partenaire en matière de cyberdéfense.

KÉVIN MARTIN
Chargé de recherche, FRS
k.martin@frstrategie.org

**Notes**

1. UKTI, *Cyber security, the UK's approach to export*, septembre 2012.
2. Markets and Markets, *Cyber Security Market Forecast to 2020*, Juin 2015.
3. VisionGain, *Cybersecurity Market 2015-2025,* 26 février 2015.
4. « Israel claims $3B in Cyber Exports; 2nd only to US », *Defence News*, 20 juin 2014.
5. Le gouvernement britannique estime le montant total des exportations de solutions de cybersécurité en 2012 à 850 M£.
6. « Israeli cyber security exports grew 10% in 2015 », *Globes.co.il*, 14 janvier 2016.
7. « Israeli Cyber Exports Double in a Year », *Defense News,* 3 juin 2014.
8. « Israel Claims Surge in Cyber Sales, Investment », *Defense News,* 21 janvier 2016.
9. Lior Tabansky, *Cyberdefense Policy of Israel: Evolving Threats and Responses*, Tel Aviv University, janvier 2013.
10. Advancing national Cyberspace capabilities, Resolution, No. 3611 of the Government of August 7, 2011.
11. *Op. cit.*
12. « Israel launches Kidma 2.0 cyber-security program », communiqué de presse du ministère israélien des Affaires étrangères, 21 décembre 2015.
13. « Advanced Technologies Park inaugurated adjacent to BGU », *Newsletter of Ben-Gurion University of the Negev*, hiver 2014.
14. « Ya'alon : Beersheba will be national cyber capital », *Jerusalem Post*, 10 janvier 2013.
15. www.atp-israel.com/overview.html
16. « Surge in launches of Israeli cyber security companies », *Financial Times,* 26 janvier 2016.
17. Departement for Business Innovation & Skills (BIS), *Competitive analysis of the cyber security sector*, 29 juillet 2013.
18. Association française des éditeurs de logiciels (Afdel), *Livre Blanc cybersécurité : hisser les acteurs français au niveau de la compétition mondiale*, juin 2014.
19. « ''Cyber Dome'' for the SCADA environment », *Israel Defense*, 10 septembre 2015.
20. *Ibid.*
21. « Israel's Rafael to unveil laser-based defense system », *Israel Hig-tech & Investment Report*, février 2014.
22. « Meet Israel's Home-front Hero: Iron Dome », *Haaretz*, 18 juillet 2014.
23. « Israel presents an 'Iron Dome' for 'electricity terror », *Times of Israel*, 11 novembre 2014.
24. « Canadian Firm Adopts Iron Dome Technology for Electrical Smart Grid », *Breaking Israel News*, 25 janvier 2015.
25. « First Published: IBM, EMC, Matrix, Cisco and Rafael to establish the National CERT », *Israel Defense,* 29 juin 2015.
26. « Rafael has been selected to head Israel's national CERT program », *ASD news,* 1er juillet 2015.
27. « IAI publishes its financial statements for 2014 », communiqué de presse *IAI*, 25 mars 2015.
28. « IAI presents latest cyber intelligence and communications solutions », *Globes.co.il,* 20 mai 2013.
29. « IAI to build a professional network for the cyber community in israel », communiqué de presse *IAI*, 2 septembre 2015.
30. « Elta systems, IAI's group and subsidiary, recently introduced advanced cyber accessibility center at a convention held in Prague », communiqué de presse *IAI*, 9 juin 2013.
31. « IAI and Formula Systems agree to acquire TSG for US$ 50 Million », communiqué de presse *IAI*, 14 janvier 2016.
32. « Opening of Custodio's cyber security research center », communiqué de presse de l'*Economic Development Board* de Singapour, 13 février 2014.
33. « IAI awarded cyber solutions contracts totaling tens of millions of dollars », communiqué de presse *IAI*, 5 janvier 2015.
34. Rapport annuel 2014, Elbit Systems.
35. « The fifth theater of Battle: cyberwar », *Haaretz*, 14 janvier 2014.
36. Elbit Systems company profile, 2009.
37. « Elbit Systems unveils new cyber simulator », *Shephard Media,* 7 juin 2012.
38. « Ixia to acquire BreakingPoint Systems », communiqué de presse *Ixia*, 2 juillet 2012.
39. Document 6-K Elbit Systems, *Security Exchange Commission,* 17 août 2011.
40. « Elbit Systems Signs an Agreement to Acquire NICE Systems », Communiqué de presse *Elbit Systems*, 21 mai 2015.
41. « The fifth theater of Battle: cyberwar », *Haaretz*, 14 janvier 2014.
42. « The Cyber Technology Market is Endless », *Israel Defense*, 15 décembre 2015.
43. Site internet Cyberbit, consulté le 8 février 2016.
44. « CYBERBIT has been awarded contracts by a European police force and an African enforcement agency », *Globes.co.il*, 30 août 2015.
45. « Elbit Takes The Lead In Cyberwarfare Training », *Aviation Week*, 17 décembre 2012.
46. « Elbit Systems Provides Singaporean STElectronics (Info-Security) with a CyberSecurity Simulator for Civil Applications », communiqué de presse *Elbit Systems*, 15 septembre 2014.
47. « Elbit Systems Provides RUAG Defence with an Advanced Cyber Security Simulator », communiqué de presse, *Elbit Systems*, 21.12.2015.
48. Breznitz Dan, *The military as a public space – The role of the IDF in the israeli software innovation system,* MIT-IPC, avril 2002.