JANVIER 2019
PUBLICATION CIGREF

Cigref
RÉUSSIR
LE NUMÉRIQUE

CYBER & INNOVATION EN ISRAËL

Learning expedition du Cigref
Novembre 2018

Cyber & Innovation en Israël

Learning Expedition du Cigref en novembre 2018

Janvier 2019

Le Cigref est un réseau de grandes entreprises et d'administrations publiques qui a pour mission de développer la capacité de ses membres à intégrer et maîtriser le numérique. Par la qualité de sa réflexion et la représentativité de ses membres, il est un élément fédérateur et acteur important de la société numérique.

Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative. Il regroupe à ce jour près de 150 grandes entreprises et administrations publiques françaises dans tous les secteurs d'activité. Sa gouvernance est assurée par 15 administrateurs, élus en Assemblée générale. Son activité est animée par une équipe de 10 permanents.

Retrouvez toutes nos publications sur **www.cigref.fr** | Suivez-nous sur Twitter : **@Cigref**

Cigref, **21 avenue de Messine, 75008 Paris**, +33 1 56 59 70 00, **cigref@cigref.fr**

SYNTHÈSE

Une délégation du Cigref, conduite par Jean-Claude Laroche, DSI d'Enedis, Administrateur Cigref, et Président du Cercle cybersécurité du Cigref, a passé quatre jours en Israël du 11 au 15 novembre 2018 sur le double thème de l'innovation et de la cybersécurité. La délégation Cigref était composée d'une vingtaine de représentants d'entreprises membres du Cigref, accompagnés par trois députés membres de la Commission Supérieure du Numérique et des Postes, Mireille Clapot, Christine Hennion, Eric Bothorel, du Secrétaire Général de cette Commission, Ludovic Provost, et de nos partenaires Shushane&Co et Sia Partners.

La délégation a vécu quatre journées intenses, faites de nombreuses rencontres avec les dirigeants de plusieurs *startups* israéliennes, des hauts responsables israéliens comme le Directeur général du *National Cyber Directorate*, l'équivalent israélien de l'ANSSI, le Président de l'*Israël Innovation Authority*, des députés de la Knesset, le directeur du centre de R&D Cyber de l'Université Ben-Gourion à Beer-Sheva.
A l'occasion de sa venue en Israël, notre délégation a eu l'honneur d'être reçue par l'Ambassadrice de France à Tel-Aviv, Hélène Le Gal, au cours d'une réception à laquelle elle avait convié les représentants de plusieurs entreprises françaises de technologie implantées en Israël.

Dans le double domaine de l'innovation technologique et de la cybersécurité, Israël occupe une place très particulière sur le plan mondial. La « *startup* nation », comme elle se qualifie elle-même, a réussi à s'imposer comme un hub incontournable pour la R&D des plus grands groupes technologiques mondiaux et pour les investisseurs. Depuis plus de dix ans, avec une grande détermination, tous les acteurs de la société israélienne, publics et privés, militaires et civils, académiques et économiques, se sont mobilisés pour développer collectivement, autour des technologies numériques et de la cybersécurité, un « écosystème » cohérent et ultra-performant. Même si la situation géopolitique singulière de l'État d'Israël explique sans doute pour partie cette dynamique d'innovation, nous considérons que des enseignements sont à tirer de la manière dont les israéliens s'y sont pris pour créer les conditions de ce succès remarquable, qui a marqué unanimement les membres de la délégation.

REMERCIEMENTS

Nous remercions tous les membres de la délégation Cigref emmenée par Jean-Claude LAROCHE, DSI d'Enedis, Administrateur Cigref et Président du Cercle Cybersécurité du Cigref, pour leurs contributions à cette réflexion commune :

Thierry AUGER– LAGARDERE
Eric AUDY– ENEDIS
Gérard AURIOL - ENEDIS
Franck ATGIE - ENEDIS
Gildas BOUTEILLER - LAGARDERE
Edouard CHALOUHI - LAGARDERE
Paul COHEN SCALI– PMU
Vincent GAPAILLARD– LAGARDERE
Alain GONDOIN - EIFFAGE
Djilali KIES - TDF
Jean-Claude LAROCHE - ENEDIS
Bernard LASSUS - ENEDIS
François PICAND - TDF
Stéphane ROUSSEAU - EIFFAGE

Nous remercions également les parlementaires qui nous ont accompagné :

Eric BOTHOREL, Député des Côtes d'Armor,

Mireille CLAPOT, Députée de la Drôme,

Christine HENNION, Députée des Hauts-de-Seine,

Ainsi que Ludovic PROVOST, Secrétaire général de la Commission Supérieure du Numérique et des Postes

Nous remercions enfin Jean-Pierre CORNIOU (Sia Partners) pour la qualité de son accompagnement et Nelly SOUSSAN (Shushane&Co) pour la parfaite organisation de ce voyage d'étude.

Ce document a été rédigé par Clara MORLIERE (Cigref) avec la contribution de Jean-Claude LAROCHE (Enedis) et Jean-Pierre CORNIOU (Sia Partners).

TABLE DES MATIÈRES

TABLE DES FIGURES

1. Impressions dominantes

Face à l'augmentation et la complexification des cyberattaques, dans un environnement géopolitique tendu, l'« Écosystème » israélien s'est mobilisé sur la recherche et le développement (R&D) des technologies pour créer de nombreuses solutions innovantes et faire évoluer les cas d'usage en vue de lutter efficacement contre la cybermenace. Cet ensemble de démarche a conduit à un foisonnement des *startups* faisant d'Israël la « *startup* nation » leader en cybersécurité.

Israël est un pays assez jeune (70 ans), « petit » (28 fois plus petit que la France) avec 60% de désert et une population de 8,7 millions d'habitants. Le pays possède une croissance de 4% et investit 4,3% de son PIB dans la R&D. Israël est le pays où la R&D repose le plus, proportionnellement aux dépenses consenties, sur un financement privé. Le chômage continue à diminuer, l'économie s'approchant d'une situation de quasi plein emploi.

L'économie israélienne connaît deux secteurs très contrastés :

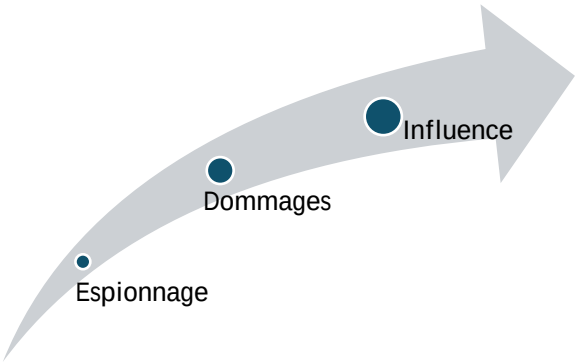
- une partie high-tech très développée qui attire environ 20% des investissements mondiaux dans le secteur des technologies de cybersécurité. Ceci se traduit notamment par l'ouverture de nombreux centres R&D des entreprises technologiques américaines,
- et un secteur avec un des taux de pauvreté les plus élevés de l'OCDE ; c'est pourquoi la cybersécurité est utilisée comme moyen d'intégration et ascension sociale.

Investir dans les technologies est donc un véritable choix de société du gouvernement et du monde économique, qui a conduit au développement d'un ensemble d'acteurs très dynamique partageant des objectifs communs. L'articulation des systèmes éducatifs et militaires avec ce tissu d'acteurs permet d'apporter les compétences et les ressources nécessaires au développement cohérent de cet écosystème.

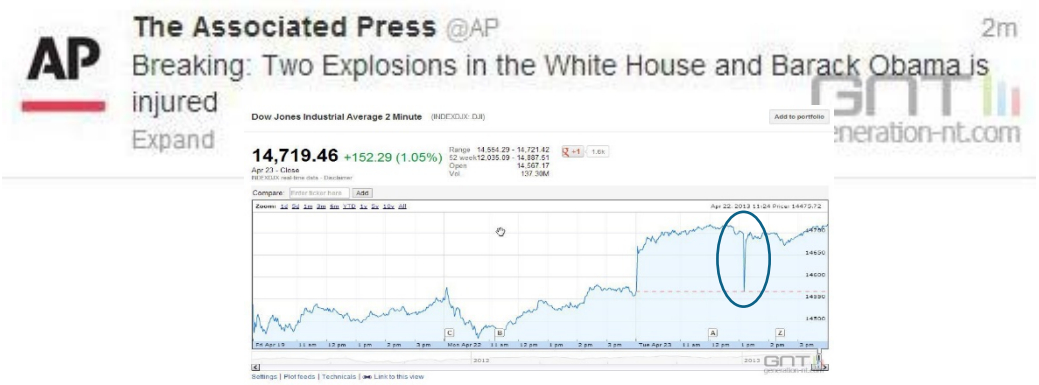
1.1. Multiplication des cybermenaces et solutions de cybersécurité innovantes

La délégation a été frappée par le nombre et la diversité des menaces évoquées lors des interventions mais aussi le nombre de solutions disponibles sur le marché pour y faire face. La multiplicité des solutions proposées, apparaissant souvent redondantes, rend leur lisibilité difficile. Les grands groupes qui souhaitent y trouver des réponses adaptées à leurs besoins ressentent cette difficulté à opérer des choix entre les offres. Il faut souligner qu'une méthodologie de cyberdéfense, en accès libre, a été élaborée et adoptée par les organisations israéliennes.

1.1.1. Multiplication des cyberattaques et leur caractère inéluctable



L'*Israeli National Cyber Directorate*, la direction nationale israélienne de la cybercriminalité, présente la nette évolution des menaces en trois « générations » de cyber-crimes : la première génération amplifiait les moyens de l'espionnage, la seconde visait à produire des dommages et la troisième s'attache à la produire de l'influence. La menace de l'influence s'accroît avec les médias sociaux et la possibilité de manipuler les opinions via les réseaux sociaux. Un exemple significatif fût le piratage du compte Twitter de l'Associated Press qui a eu un impact direct sur le cours des actions de bourse du NASDAQ.



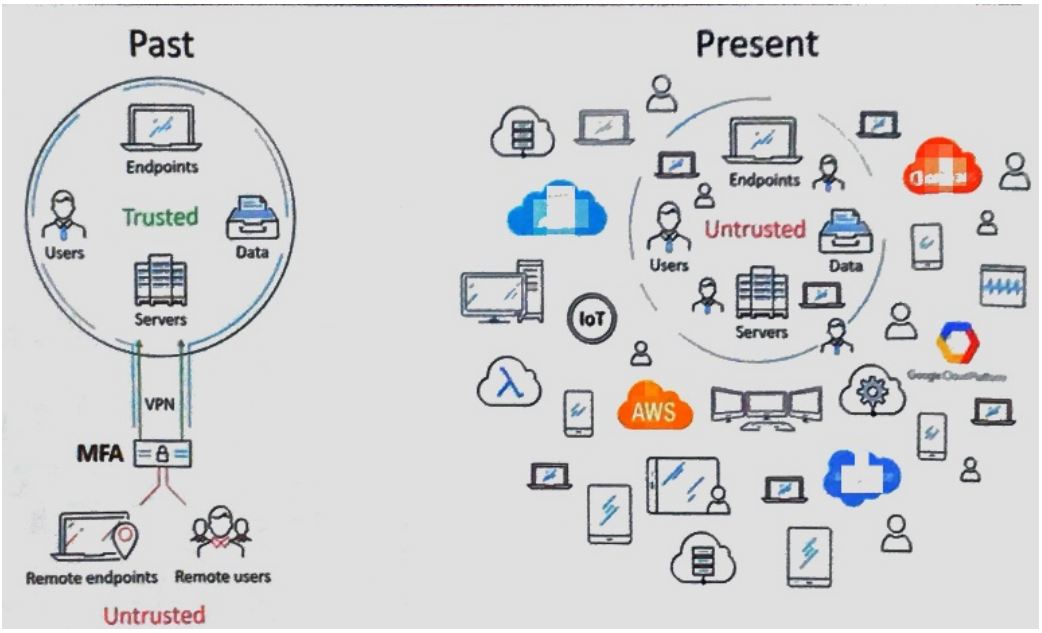
Source : Génération Nouvelles Technologies

Figure 1 : Piratage du compte Twitter de l'Associated Press en 2013

Il semble acquis, pour tous les acteurs, que la question n'est pas de l'éventualité d'une attaque de l'entreprise mais de l'échéance de l'attaque. L'enjeu est de connaître l'échéance d'une prochaine attaque pour en minimiser les dommages. Toutes les entreprises israéliennes d'infrastructures critiques ont été attaquées d'une façon ou d'une autre. Les Israéliens passés par les entités cyber des services militaires ont appris les techniques de cyberattaques et en connaissent ainsi les arcanes : « un cyber-attaquant trouvera toujours une vulnérabilité à exploiter » afin d'entrer dans les systèmes des entreprises, de la même manière que les serrures physiques restent vulnérables. C'est pourquoi les solutions développées se concentrent de plus en plus sur la protection des infrastructures une fois qu'une attaque a été détectée plutôt que sur le fait de construire un « mur » de prévention. La compréhension du comportement des attaquants et de leur pratique des outils de cyberattaque permet de repérer plus facilement les intrusions. La prévention consiste donc à comprendre l'assaillant et à rendre ses attaques inopérantes.

De plus, on constate une extension de la menace : tous les objets connectés et systèmes industriels de l'entreprise ont vocation à intégrer le périmètre du système d'information. La cybersécurité concerne désormais le fonctionnement opérationnel de l'entreprise. La

menace est plus concrète et précise : les attaquants peuvent non seulement altérer les données mais compromettre la sûreté et la continuité de fonctionnement des installations industrielles. Les vulnérabilités de ces technologies opérationnelles sont différentes mais la convergence entre les deux systèmes (système d'information/ système industriel) menace aussi la continuité opérationnelle, et plus seulement l'intégrité des données.



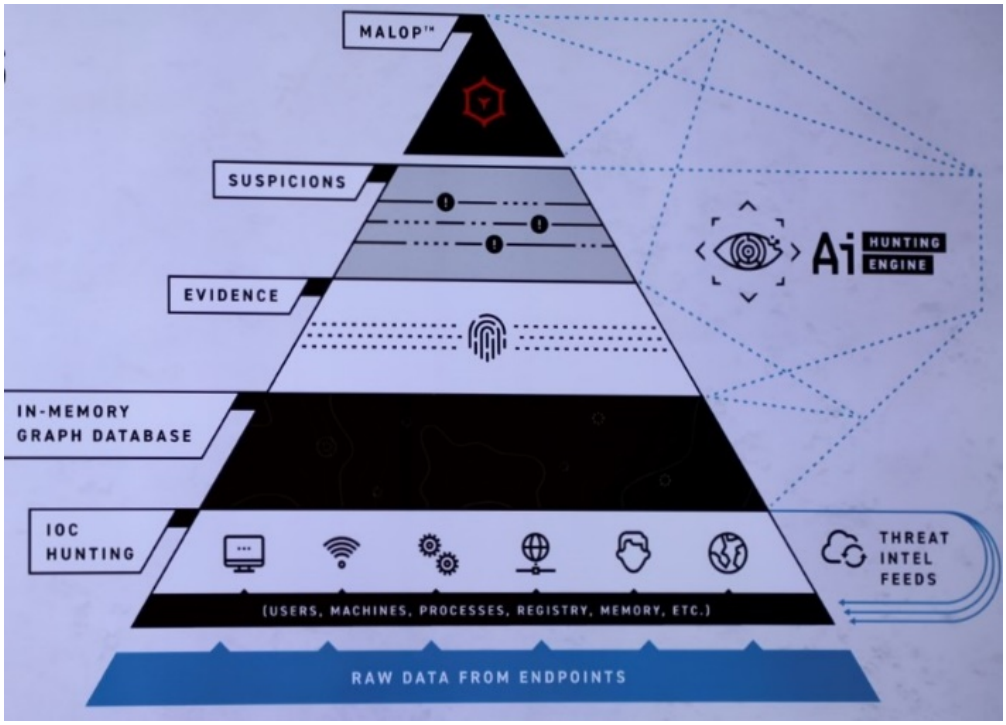
Source : Silverfort

Figure 2 : Complexification des environnements intégrés dans l'entreprise

Pour faire face à l'accroissement inéluctable des cyberattaques, le gouvernement israélien a imposé à ses grandes entreprises équivalentes des Organismes d'Importances Vitales (OIV), de dédier 8% de leurs revenus au budget pour la cybersécurité (la moyenne en France est de 3-4%) pour les ce qui montre l'importance accordée à cette question.

1.1.2. Intégration des solutions aux grands groupes israéliens

Ces enjeux auxquels sont confrontés les acteurs économiques et militaires poussent les *startups* à une recherche permanente de la performance et à son optimisation en utilisant les outils technologiques. Les attaques sont rarement brutales, les agents malins s'installent longtemps avant l'attaque et doivent être identifiés par une pluralité de méthodes concomitantes.



Source : Cybereason

Figure 3 : Étapes de la stratégie anti-intrusion maligne

Les startups auditionnées (cf. partie sur les acteurs rencontrés, page 17) ont présenté des solutions technologiques ayant des capacités diversifiées pour faire face aux cybermenaces. Elles couvrent le spectre entier des actions à mettre en œuvre pour la prévention, la détection et la réaction aux cyberattaques. Certaines développent ainsi des solutions pour :

- Rechercher dans l'open web, le deep et le dark web
- Recherche dans les bases de données du SI de l'entreprise dans une démarche de mise en conformité RGPD
- Analyser les logiciels afin de détecter les parties de code malveillant
- Renforcer les méthodes d'authentification des terminaux pour les sécuriser
- Empêcher l'accès à la mémoire interne des terminaux pour en garantir l'intégrité
- Capter l'activité anormale sur les terminaux de l'entreprise (connectés au réseau ou non)
- Identifier les terminaux infectés pour les isoler du reste du système d'information
- Reconstituer et analyser les étapes chronologiques des attaques.

Face aux présentations des solutions des startups auditionnées, plusieurs questions se sont posées sur les relations entre *startups* et grands groupes israéliens : la question de la sélection des solutions, la question de la maturité des offres proposées ainsi que la question de la dépendance vis-à-vis de ces solutions.

Sélection des solutions

Beaucoup d'entreprises travaillent sur les mêmes problématiques, avec des solutions similaires, et se présentent souvent comme complémentaires. Cette diversité n'est pas un obstacle et répond à la doctrine « "*Better having overlap than gap*" affirmée par le *National*

Cyber Directorate. Un besoin d'identification et de sélection des meilleures solutions se fait alors sentir. Des acteurs français présents en Israël, comme Orange et Thales, effectuent des tests d'évaluation sur les solutions de nombreuses startups, par le biais notamment de *Proof of Concept* avec l'objectif de les intégrer par la suite dans leurs offres.

Maturité des offres

Les offres proposées par les *startups* sont diverses : elles dépendent de leur taille, de leur âge, de leur type de développement ainsi que de leur façon d'aborder les problèmes. Cela complexifie la lisibilité de leur maturité et leur capacité à répondre aux problématiques des grands groupes ce qui nécessite de faire appel à des intermédiaires intégrateurs de ces solutions.

Obsolescence des offres

Le rythme des cybermenaces s'accélère et peut amener rapidement à l'obsolescence des solutions achetées et ainsi donc mettre en difficulté la gestion financière et la gouvernance de ces multiples solutions. Néanmoins, la mise en place des nouvelles solutions devient de plus en plus rapide, ce qui suppose de passer à un mode jetable. La facilité apparente et promue par les *startups* de passer d'une solution à une autre permet d'implémenter les nouvelles solutions en fonction de nouvelles cybermenaces.

Dépendance vis-à-vis des solutions

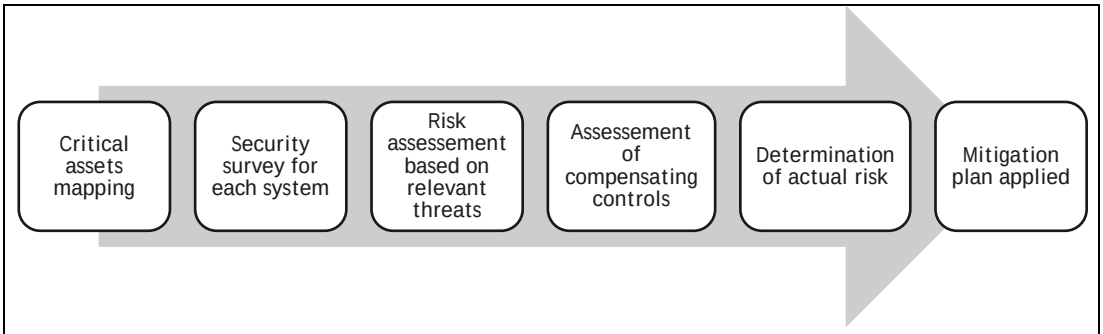
Les systèmes proposés s'intègrent complètement dans les systèmes d'information des entreprises au travers des terminaux (appareils connectés, que ce soient des ordinateurs, des tablettes, des téléphones ou des serveurs). Ces solutions possèdent d'importantes capacités d'analyse et sont très intrusives pour remplir leur fonction de prévention et de protection. Néanmoins, on peut se demander quelle dépendance opérationnelle l'entreprise est capable d'accepter. L'entreprise devrait être en mesure d'auditer les solutions qu'elle implémente afin de vérifier qu'elles font bien ce qu'elles sont censées faire et qu'elles ne font pas ce qu'elles ne sont pas censées faire. Un autre enjeu de la dépendance des entreprises vis-à-vis des solutions est de pouvoir maîtriser l'évolution des solutions critiques, c'est-à-dire de disposer d'un pouvoir de marché sur le fournisseur.

1.1.3. Approche méthodologique pour la protection des systèmes

Les entreprises israéliennes adoptent une approche nationale de la cyber défense. Cette méthodologie partagée est proposée par le *National Cyber Directorate*.

Zoom : Gestion de la cybersécurité d'Israel Railways

L'entreprise de chemins de fer israéliens doit faire face à un grand nombre de cyberattaques. Afin de prioriser les investissements et les actions à entreprendre dans l'entreprise, Israel Railways met en place un ensemble d'actions pour évaluer le risque et établir le plan de réduction des risques.



Source : Israel Railways basé sur la méthode de l'*Israeli National Cyber Directorate*

Figure 4 : Méthodologie de Cyber Défense d'Israel Railways

Le plan de réduction des risques comprend trois piliers de la « cyber-pratique » : *People, Process, Technology*. Dans leurs bonnes pratiques évoquées, ils en recommandent trois :

- **PEOPLE** : Investir principalement sur la sensibilisation et les formations des collaborateurs. Créer des « *cyber-trustees* », aussi appelés « cyber-champions » : des collaborateurs ayant suivi une formation poussée, ce qui permet de placer des personnes sensibilisées au sein des différentes entités de l'entreprise.
- **PROCESS** : Contrôler la *supply chain,* point de vulnérabilité : autoriser et vérifier chaque connexion aux systèmes par les prestataires et fournisseurs, qui sont eux-mêmes évalués avant chaque signature de contrat puis régulièrement pendant la durée des contrats.
- **TECHNOLOGY** : Surveiller les systèmes via des SIEM (*Security Information Management System*) et SOC (*Security Operational Center*) : utilisation de nouvelles technologies militaires et optimisation des systèmes existants.

1.2. De nombreuses avancées technologiques

Les participants, qui étaient déjà venus en voyage d'étude en Israël, ont remarqué la rapidité des évolutions ; ceux qui n'étaient pas encore allés en Israël ont été frappés par le caractère disruptif des innovations présentées. Après un an, l'accélération technologique est visible avec par exemple l'intégration de la 5G.

Les *startups* développent de plus en plus de techniques de cybersécurité et les perfectionnent pour les adapter à tout contexte : on voit maintenant des *Security Operationnal Center* (SOC) complets capables d'être directement utilisables par les utilisateurs finaux. La sécurisation du *Machine learning* est également un sujet important traité par le centre de R&D de l'Université Ben-Gourion du Néguev. Enfin, la multiplication des cas d'usage de la 5G a été montrée par Qualcomm ; sur ce sujet éminemment géopolitique, tous les pays se comparent dans leur avancement.

Israël tente également d'investir dans la recherche technologique reposant sur les sciences fondamentales (chiffrement homo-morphique, informatique quantique). La cryptologie homo-morphique est un vrai sujet prometteur pour des usages étendus du *cloud computing* et la garantie de protection des données sur lesquelles des traitements sont effectués.

1.2.1. Maturité des techniques de cybersécurité et sécurisation du *machine learning*

Les avancées en *machine learning* sont importantes et cette technique ainsi que celle du *deep learning* vont continuer à être développées par les chercheurs pendant encore de nombreuses années d'après la délégation. Certaines *startups* rencontrées ont montré de réelles capacités dans ces domaines. D'après l'intervenant de l'Université Ben-Gourion, le *machine learning* n'est pas très sécurisé, les chercheurs n'ayant pas pensé à y embarquer la cybersécurité ; celui-ci affirme qu'il est donc incroyablement facile de le compromettre. Le centre de recherche de l'Université Ben-Gourion tente alors de trouver des modèles d'apprentissage plus sûrs en établissant un équilibre entre résilience et précision afin d'éviter les attaques visant à leurrer les processus d'apprentissage.

Ces dernières années, la prise de conscience de l'importance de la protection de la vie privée a entraîné une augmentation de la réglementation en Europe ainsi qu'aux États-Unis. En même temps, on cherche à collecter plus de données afin de les analyser. Est-il possible de concilier cela ? Une des *startups* rencontrées, Duality, offre une plateforme permettant de mettre à disposition des données chiffrées afin de faire réaliser des traitements sur ces données chiffrées, et ainsi de faciliter et raccourcir le temps de la collaboration entre les parties (propriétaire des données et prestataire du traitement de l'information).

1.2.2. Déploiement massif et gestion d'objets connectés

Le déploiement massif d'objets connectés et leur gestion telles que les flottes de véhicules connectés à gérer à distance représentent de vrais défis pour les entreprises.

Zoom : Gestion à distance des objets connectés par Harman (filiale de Samsung)

Pour maintenir à niveau un parc de véhicules doté de logiciels (systèmes d'exploitation, microprogrammes, applications et cartes) hétérogènes, la connectivité au *cloud* est essentielle ; elle permet de disposer d'une vue d'ensemble de l'emplacement et du niveau d'utilisation de la flotte, d'en recueillir toutes les informations afin de la superviser et agir en conséquence. Par conséquent, les constructeurs automobiles se devront d'utiliser les solutions « *Over-The-Air* »[1], technologie permettant d'accéder aux données d'une carte SIM à distance afin de déployer de nouveaux services dans le but de mettre à jour les systèmes mais aussi d'atténuer le cyber-risque. En 2013, Harman a acheté **Redbend** qui est spécialisé depuis 70 ans dans la télésurveillance d'objets connectés utilisant la technologie « *Over-The-Air* » et qui est aujourd'hui leader de la gestion logicielle[2] sur le marché de l'automobile. Harman a également acheté **iOnRoad** pour la reconnaissance d'images pour le secteur automobile et **TowerSec**, une *startup* du monde de la cybersécurité du même secteur.

[1] https://fr.wikipedia.org/wiki/Over-the-air_programming
[2] https://www.businesswire.com/news/home/20150122005522/en/HARMAN-Acquire-Red-Bend-Software

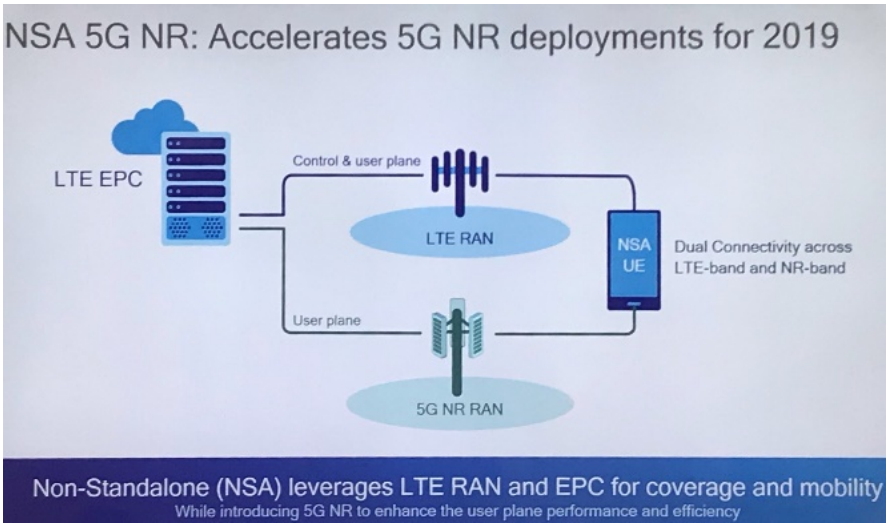
1.2.3. Multiplication des cas d'usage de la 5G

Pour la première fois, des produits seront disponibles rapidement pour la 5G ce qui marque l'avancée de la technologie. Les réseaux 5G sont destinés à générer d'énormes volumes de données avec des contraintes complexes. Ils auront la capacité de supporter de nombreux besoins en bande passante et en temps de latence très courts. Les cas d'usage évoqués sont nombreux et variés, la 5G donnant la capacité de gérer des flottes d'objets mobiles, comme les véhicules autonomes ou les robots de la *supply chain* et des usines.

Le processus d'adoption de la 5G est déjà en cours. La question soulevée est de savoir comment nous saisir de ces outils pour que ces technologies puissent rapidement se développer en France. C'est principalement Orange qui se positionne sur cette technologie et son développement en France.

Zoom : Réseau 5G développé par le centre R&D de Qualcomm

La 5G est le plus gros pari de Qualcomm. Le centre de R&D de Tel Aviv se concentre sur la fabrication des puces ainsi que sur les algorithmes associés pour la 5G. La 5G NR (*New Radio*) répondra à la demande insatiable de haut débit mobile et augmentera la vitesse des données jusqu'à 6 Gigabits/ seconde permettant de connecter les objets entre eux et ainsi de développer de nouveaux marchés verticaux : IoT industriel, voitures et transport autonomes, soins de santé à distance, agriculture intelligente, ville intelligente, etc. Par exemple, la solution « C-V2X » s'appuie sur la 5G et connecte intelligemment l'environnement du véhicule avec l'infrastructure routière et les autres véhicules. Qualcomm travaille avec tous les autres opérateurs 5G pour garantir la compatibilité entre les opérateurs.



Source : Qualcomm

Figure 5 : Utilisation combinée de la 4G et de la 5G pour une meilleure connectivité

1.3. Systèmes éducatifs et militaires à fort impact sur le développement des compétences et de l'écosystème

Au travers des différentes présentations, rencontres et visites, la délégation a été frappée par l'expertise technologique forte démontrée par tous les interlocuteurs. Partant d'une menace liée à son environnement, Israël a fait de la cybersécurité une opportunité de développement non seulement économique mais aussi social, utilisant l'informatique comme un moyen de formation pour les jeunes. Commençant très tôt, dès l'enfance, par une démarche d'« exposition à la technologie », le développement des connaissances et compétences en informatique, codage et logiciels de cybersécurité se poursuit dans les programmes spécialisés extra-scolaires et dans l'armée qui encadre les jeunes et leur donne confiance en eux, facteur clé de réussite professionnelle.

1.3.1. Acculturation des jeunes à la technologie et ascension sociale

Israël inclut dans ses programmes d'éducation une acculturation à la technologie ce qui sert ainsi comme vecteur d'intégration et d'ascension sociale.

Zoom : Intervention du Député Eli Elalouf

Le député Eli Elalouf, président de la commission des affaires sociales, de la santé et du travail, a publié un rapport sur la pauvreté en Israël après avoir consulté 40 spécialistes, y compris des académiciens et des hauts fonctionnaires. Ce rapport a été adopté par le gouvernement en tant que deuxième accord de la coalition politique. L'objectif des recommandations de ce rapport est de sortir les populations défavorisées d'Israël de la pauvreté. Pour cela, le député indique qu'il faut agir dans tous les domaines de la vie : au niveau de l'économie, de la culture, des soins médicaux, des services sociaux, du logement, mais aussi de l'environnement, de la position sociale des pauvres et particulièrement de l'éducation. C'est ainsi que des formations à l'informatique et à la cybersécurité pour les jeunes défavorisés ont été valorisées et déployées à travers tout le territoire. La Fondation Rashi, pionnière dans cette démarche a, par exemple, signé un contrat avec l'armée pour former des milliers d'élèves du niveau du secondaire en vue de les intégrer dans les unités les plus sophistiquées de l'armée.

1.3.2. Encadrement des jeunes

Lors des interventions et visites, la délégation a constaté de façon claire la présence structurante de l'armée pour les *startups* et les entreprises. La période obligatoire dans l'armée permet de donner confiance aux jeunes de 18 ans à 21 ans : ils se rendent compte de ce dont ils sont capables sous un angle extrêmement pratique et non seulement théorique. Cette observation a suscité un intérêt de certains participants au moment de la réflexion parlementaire française sur le développement du service national universel.

Zoom : Service militaire

Actuellement, le service militaire basique en Israël est de 2 ans pour les femmes et de 3 ans pour les hommes. Les recrues sont de plus en plus encouragées à rester plus longtemps (6-7 ans voire y faire carrière). Cet engagement de plus longue durée leur donne la possibilité, de façon plus ou moins explicite, de réutiliser les technologies développées dans l'armée pour les appliquer au domaine civil. Les solutions de l'armée sont tournées vers l'optimisation de ressources (automatisation des alertes à traiter, mobilisation d'assistants virtuels pour optimiser les recherches de preuves des analystes, détection des attaques, etc.), techniques pertinentes aussi pour les entreprises.
L'attachement à la défense d'Israël fait partie de la culture des Israéliens dès l'enfance. L'encadrement renforcé connu au sein de l'armée entraîne le développement d'un état d'esprit commun. Les jeunes y sont exposés aux dernières technologies, bénéficiant de formations (savoir-faire et savoir-être), ils développent un fort esprit de jeu associé à une appétence pour le renseignement, et cet aspect *gamification* permet aussi de fédérer les énergies. Mentalement, les jeunes de 18 ans grandissent très vite pour devenir responsables, matures et capables de travailler en équipe. En sortant de l'armée, les jeunes sont ainsi prêts à intégrer *startups* ou grands groupes.

1.3.3. Détection des profils et sélection des *startups*

L'« Écosystème » israélien a montré sa capacité à détecter des profils compétents et des potentiels d'intelligence. Le jeune âge de nombreux intervenants, et leur confiance en eux lors de leurs présentations, a marqué la délégation. Tous n'étaient néanmoins pas en début de carrière, et la diversité de profils montre également la capacité israélienne à mobiliser tous les talents.

Zoom : Sélection des recrues de l'armée

La logique de recrutement de l'armée s'appuie sur un mécanisme de sélection fondé sur le potentiel d'intelligence, la personnalité et la forme physique. On demande aux candidats de faire face à des scénarios spécifiques permettant d'apprécier notamment leurs qualités humaines. La recette de l'armée israélienne est d'amener à faire travailler les généraux expérimentés avec des jeunes dont on encourage la créativité. Elle dénote un état d'esprit et un respect mutuel qui conduit au succès de la collaboration intergénérationnelle.

Du point de vue des compétences, les disciplines informatique et mathématique sont au cœur du domaine de la cybersécurité. Mais ces compétences doivent être combinées à la psychologie et à d'autres sciences sociales pour être exercées plus efficacement. Le développement de cet ensemble de compétences permet à Israël de disposer des talents dont les entreprises ont besoin.

Zoom : Sélection des *startups* en Israël (mécanisme des fonds d'investissement et de l'Autorité de l'innovation)

L'Innovation Authority choisit de soutenir des entreprises qui ont développé une technologie innovante et qui s'appuient sur une équipe dirigeante solide, disposant d'une bonne connaissance technologique et *business*, et capable d'être facilement coachée. La technologie doit démontrer non seulement son caractère innovant mais aussi un avantage compétitif évident. Le financement peut atteindre 50% des dépenses.

1.4. Choix de société pour développer un *Écosystème*

« *La cybersécurité est une nécessité, c'est une responsabilité d'Etat, c'est un business*. »

Le choix de société effectué par les dirigeants israéliens s'appuie sur une stratégie de défense nationale à la pointe de la technologie. Les Israéliens ont donc fait le choix de maîtriser eux-mêmes les technologies et de ne pas dépendre d'autres pays pour être en mesure de garantir eux-mêmes leur sécurité. Tout l'« Écosystème » s'est ensuite aligné de façon volontariste. L'objectif premier d'une *startup* technologique est de s'appuyer sur l'excellence technologique d'Israël notamment développée au sein de l'armée pour développer des solutions innovantes, les exporter au plus vite à l'échelle mondiale, générer une croissance rapide, puis au bout de quelques années réussir son introduction au Nasdaq et son *exit*. Les stratégies d'exportation au plan mondial et la croissance qu'elles génèrent permettent d'encourager le développement de la R&D, créant ainsi un cercle vertueux. Cette incitation au développement commercial des solutions bénéficie donc au financement des technologies.

1.4.1. Stratégie de défense nationale à la pointe de la technologie

Malgré sa petite taille et sa population, Israël n'hésite pas à s'attaquer à d'importantes problématiques mondiales (telles que les *smart cities)*. La délégation a été frappée par le dynamisme qui se ressent en Israël dans de nombreux domaines, jusque dans l'aménagement du territoire. Il est clair qu'une des causes de ce dynamisme est la peur existentielle « d'être rayé de la carte » par les ennemis du pays, la peur de disparaître.

Compte tenu du contexte géopolitique, le Premier ministre, Benjamin Netanyahou a décidé de prendre directement sous sa responsabilité le sujet de la cybersécurité et a engagé des moyens pour lancer un dispositif complet. En dix ans, Israël est parvenu à se faire reconnaître comme un leader mondial dans ce domaine. L'organisation des services de l'Etat dans ce domaine se caractérise par un *continuum* entre la posture d'attaquant et la cyberdéfense. Ce choix relève aussi du constat que toute innovation non sécurisée est synonyme de menace et qu'une innovation sécurisée est une opportunité. La « condition nécessaire mais pas suffisante » de l'innovation est donc la cybersécurité et le pays anticipe une croissance exponentielle de l'innovation.

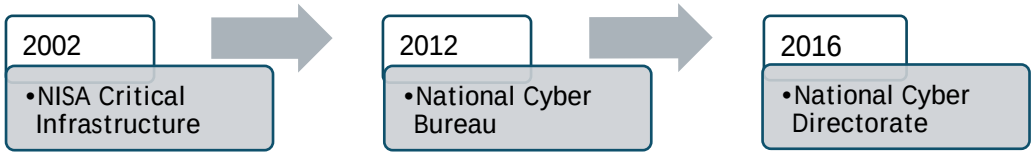
La délégation a pu rencontrer deux acteurs majeurs de l'élaboration de cette stratégie et de sa mise en place : *l'Israeli National Cyber Directorate* et l'*Innovation Authority*.

Zoom : *Israeli National Cyber Directorate*

Le Premier ministre israélien a mis en place en 2016 la Direction nationale israélienne de la cybercriminalité appelé ***l'Israeli National Cyber Directorate*** (INCD). Cette direction a pour mission de sécuriser Israël et de protéger la continuité des activités commerciales notamment en rapprochant le gouvernement et le secteur privé.

Le Directeur du INCD, Yugal Unna, est donc directement rattaché au Premier ministre avec des responsabilités claires auprès des entreprises et des institutions civiles (allant jusqu'à l'ouverture d'un numéro dédié aux cyberattaques pour les citoyens). La répartition des responsabilités suit la logique "*Better have overlap than gap*" : le gouvernement préfère le recouvrement des responsabilités que de laisser des zones non couvertes.

Le rôle du ICND est également de sensibiliser et former les acteurs : les députés du Parlement israélien ont été formés aux enjeux de cybersécurité. Avec l'*Israel Exporte Institute*, l'INCD participe également à l'effort de partenariat et de collaboration avec la communauté internationale autour des sujets de cybersécurité des différents secteurs critiques tels que l'aviation (accord avec Airbus en France), la sécurité intérieure et le domaine médical. La définition du domaine de la cybersécurité est maintenant plus large et le sera de plus en plus : la mission du INCD est aussi de l'anticiper.



Source : *Israeli National Cyber Directorate*

Figure 6 : Évolution des organisations responsables de la cybersécurité en Israël

Zoom : *Innovation Authority*

L'Innovation Authority, dirigée par Ami Applebaum, *Israeli Chief Scientist*, est l'organisation gouvernementale qui pense et finance l'innovation en Israël. *L'Innovation Authority* est le lien entre le secteur privé et le secteur public afin de favoriser l'innovation et développer le foisonnement des *startups* et des initiatives innovantes. C'est une pierre angulaire de l'évolution de la technologie en Israël. A travers l'aide financière du gouvernement à hauteur de 500 millions de dollars, *l'Innovation Authority* lance des appels à projets centrés sur une technologie ou un domaine en particulier. Chaque dollar investi par le gouvernement *via* cette autorité génère à terme environ 5 à 8 dollars dans l'économie israélienne. Les appels à projets s'adressent aux entreprises de toute taille (particuliers, startups ou grands groupes). Cette instance donne seulement un pourcentage du financement au démarrage (50%) afin de contrôler l'avancement et l'adéquation des résultats avec les objectifs. Il s'agit d'un prêt conditionnel : si l'entreprise réussit, elle doit rembourser le prêt par des versements s'élevant à 3 à 5 % de ses revenus ; si l'entreprise échoue, le prêt est effacé.

1.4.2. Alignement de tous les acteurs de l'« Écosystème »

Israël a une réelle capacité à faire fonctionner des « écosystèmes » à tous niveaux à travers l'alignement de tous les acteurs qui apportent leurs compétences respectives, secteurs privés et publics confondus. Un environnement complet est créé en partie grâce à l'aide financière conséquente de l'Etat et aux investissements des multinationales étrangères. Le consensus national sur ces questions a étonné les participants de la délégation par sa réaffirmation constante par tous les acteurs rencontrés.

Les entreprises et les acteurs publics se sont donc fixés un objectif autour des sujets de cybersécurité, associé à un objectif national de survie, afin d'assurer son développement économique. De nombreux facteurs et acteurs ont été mis ensemble pour construire cet « Écosystème » israélien qui dépend :

- de l'armée en tant que vivier de compétences pour les entreprises ;
- du financement de la recherche et développement ;
- des industries fortes, de nombreux centres de R&D d'entreprises internationales et des startups ;
- de compétences qualifiées grâce à la relation entre les mondes académique et professionnel.

Zoom : Exemple du Hub Cybersécurité de Beer Sheva

En 1938, Beer Sheva était un petit village bédouin. Le gouvernement a décidé que Beer Sheva serait la capitale de la cybersécurité en Israël. Dans les deux prochaines années, cette ville en zone défavorisée deviendra le plus grand centre en cybersécurité de la région. Le hub est construit autour de l'université et des instances cybersécurité du gouvernement en particulier le CERT national. Les 40 groupes multinationaux, 10 incubateurs/VC/accélérateurs et les 460 *startups* israéliennes dans la cybersécurité y participeront.

Il semble en effet y avoir un véritable dialogue entre le monde académique et le monde professionnel qui se développe à travers de nombreux partenariats entre entreprises et universités. L'élaboration de programmes avec les universités contribue à la création de centres d'excellence qui permettent de développer les capacités et les compétences dont les entreprises ont besoin au travers de formations académiques et opérationnelles. L'académie est l'un des piliers clés de l' « Écosystème ».

Zoom : Centre R&D de l'Université Ben-Gourion

L'Université Ben-Gourion, seule à délivrer le diplôme d'ingénieur en Israël, est un institut académique très dynamique, la 91ème université au monde en termes de demandes de brevets avec 30% de ces brevets en informatique (placée entre Yale et Princeton).
Le centre de R&D de l'Université Ben-Gourion a deux domaines principaux de recherche : l'informatique (dont 50% sur la cybersécurité et 50% autour de l'analyse des données et de l'intelligence artificielle) et les biotechnologies.
Le centre de R&D est financé par les partenaires sur la base de projets de recherche appliquée, avec un Bureau de Transfert de Technologie de l'Université qui commercialise les résultats des recherches universitaires, ce qui renforce les liens entre université et entreprises. Le centre de R&D compte 150 employés et accueille 33% des 19 000 étudiants de l'université mais aussi des jeunes des programmes de formation en cybersécurité.

Au-delà des compétences et des dispositifs, Israël développe un état d'esprit de collaboration et de soutien entre les différents acteurs pour bénéficier ensemble des opportunités.

La mentalité *business-centric* a été perçue dès le premier jour lorsque l'un des intervenants s'est exprimé ainsi : « *Pour nous, le plus important est la satisfaction client, l'entreprise ferait tout pour le client même s'il fallait traverser les murs* ».

De plus, les relations tissées avec des acteurs étrangers permettent d'enrichir les compétences et le portefeuille de leur « Écosystème » et d'accroître l'attractivité du territoire israélien.

1.4.3. Un *serious business* à visée internationale

La cybersécurité est considérée en Israël comme un « *serious business* » à croissance exponentielle et l'environnement de la cybersécurité en Israël est ultra-commercial. Les *startups* sont orientées très tôt vers le développement de leurs activités à l'international car Israël n'est pas considéré comme un marché en soi. Les *startups* s'exportent ainsi rapidement aux Etats-Unis notamment, même si elles continuent le développement de leurs activités sur leur marché domestique. Cependant, il y a peu de multinationales israéliennes. Ce sont les étrangers et principalement les Etats-Unis qui captent la valeur à travers le rachat des sociétés israéliennes (ex : Waze, Mobileye). Israël se structure ainsi pour passer de la « *startup nation* » à la « *scale-up nation* ».

Lors de toutes les conférences et rencontres à l'occasion du salon HLS & Cyber, les acteurs israéliens ont montré leur volonté de s'ouvrir et partager leurs solutions. Ils cherchent toutes les solutions efficaces quelle que soit la provenance des partenaires (exceptés les pays ne reconnaissant pas Israël ou en étant les adversaires). L'ouverture prononcé à la collaboration des israéliens explique en partie la présence importante de délégations internationales venant à leur rencontre lors du salon HLS & Cyber mais aussi toute l'année parce qu'Israël est un leader dans le domaine de l'innovation et de la cybersécurité. Israël met en place

des politiques pour attirer des multinationales tels que Microsoft, IBM, Checkpoint ou encore Renault, etc.

Zoom : Ouverture à la collaboration internationale lors des conférences HLS & Cyber

Président du HLS & Cyber

« La nécessité d'une coopération internationale est nécessaire, mais est-elle possible ? Les pays peuvent-ils partager et échanger des informations ? Ces obstacles doivent être surmontés pour lutter pour le bien. Israël a beaucoup à offrir. »

Ministre de l'Economie et de l'Industrie

« Israël est le numéro 1 de la R&D et en voit les fruits dans la cybersécurité. Le pays dispose de la meilleure technologie en matière de cybersécurité par nécessité. Pour Israël, il n'y a pas d'autre choix que de travailler au-delà des frontières car les attaquants n'ont pas de frontières. Ce sont les liens et les relations créées lors de la conférence HLS & Cyber qui contribueront à rendre le monde plus sûr. »

Israel Export Institute

« Les conférences HLS & Cyber accueillent environ 90 pays du monde entier. Israël est prêt à partager son innovation avec le monde. L'Israel Export Institute croit en ce slogan: "We do good to the world" et souvenez-vous : "it is a flat word and an unsafe one" »

2. Enseignements clés de la *learning expedition*

2.1. Ce qui est transférable en France

- Une prise de conscience aiguë de la vulnérabilité des systèmes complexes ;
- Une intégration de la sécurité dans tout modèle d'affaires : « Security by design » ;
- Une architecture systémique de la sécurité : on ne contrôle bien que ce que l'on connaît parfaitement ;
- La détection des signaux faibles : une culture de la proactivité ;
- La cybersécurité commence par la prise de conscience et l'engagement des dirigeants ;
- Le développement du SI dans le monde de l'IoT est un déclencheur de cette prise de conscience chez les dirigeants ;
- Penser distribution, intégration et taille de marché est vital pour les *startups*.

2.2. Ce qui est spécifique à Israël

- Le rôle clef de l'armée comme creuset culturel, comportemental et technique ;
- Un sentiment d'urgence partagé par toute la population ;
- Un enthousiasme technique qui démarre dès l'enseignement au collège ;
- Un financement par toutes les grandes entreprises de la technique mondiale et surtout les entreprises américaines ;
- Un terreau de 460 *startups* cybersécurité à vocation mondiale.

3. Recommandations de la délégation

3.1. Enjeux sociétaux pour la France

- Sensibiliser tous les acteurs, qu'ils soient politiques, économiques, professionnels ou académiques, aux enjeux de transformation à venir ;
- Remettre du sens : construire, partager et communiquer un projet collectif avec le sens du bien commun pour aligner les acteurs ;
- Acculturer aux technologies les jeunes au plus tôt mais aussi toute la population pour changer l'acceptabilité du progrès technologique de la société et limiter la fracture sociale ;
- Trouver les leviers d'excellence de l'éducation en France, capitaliser sur les formations existantes, en valoriser les filières ;
- Concentrer ses efforts, augmenter l'attractivité du territoire et retenir les talents et les compétences ;
- S'appuyer sur la sensibilisation éthique de la population européenne (RGDP).

3.2. Enjeux pour les entreprises françaises

- Développer la cyber-résilience de l'entreprise pour faire face à l'accélération et multiplication des cybermenaces ;
- Former, développer les compétences et être attractives pour garder les talents dans l'entreprise ;
- Renforcer la démarche de gestion des risques, la démarche d'audit des solutions choisies et de leur évolution ;
- Repenser l'organisation interne en faisant converger systèmes industriels et systèmes d'information grâce à la donnée et la cybersécurité ;
- Encourager la mise en place de *Proofs of Concept* avec les *startups* et solliciter des intermédiaires intégrateurs de solutions pour les industrialiser ;
- Communiquer auprès de tous les collaborateurs pour les sensibiliser, les acculturer et les rassurer face au développement du numérique ;
- Penser « clients » et « marché mondial ».

4. Acteurs rencontrés

Institutions	**Ambassade de France**	Echanges avec Madame Hélène Le Gal.
	Parlement israélien	Echanges avec le Député Eli Elalouf.
Pouvoirs Publics	***Innovation Authority***	Organisation gouvernementale qui pense et finance l'innovation en Israël (équivalent de la BPI France).
	Israeli National Cyber Directorate	Agence assurant la sécurité du secteur privé et des institutions civiles israélienne sous l'autorité du premier ministre (équivalent de l'ANSSI).
	CERT national	Centre gouvernemental de veille, d'alerte et de réponses aux cyberattaques.
Venture Capital	**Glilot Partners**	Fond d'investissement spécialisé pour les *startups* B2B en cybersécurité et utilisation des données.
Multinationales	**Centre R&D de Qualcomm**	Centre R&D centré sur le développement de la 5G, sa technologie et ses cas d'usage.
	Harman	Leader mondial de la technologie automobile connectée, des innovations audios, des services *cloud* et des solutions *IoT*.
Entreprises israéliennes	***Israël Railways***	Chemins de fer israéliens, rencontre avec la CISO adjoint.
	Verint	Solutions cybersécurité de recherche sur l'*open, deep* et *dark web*.
	Cybereason	Solutions de détection des cyberattaques.
Université	**Université Ben-Gourion de Néguev**	Centre de R&D sur les sujets informatiques et biotechnologies avec des projets de recherche appliquée.
Startups	**CyberX**	Solution de cybersécurité pour l'IoT industriel.
	Duality	Plateforme de collaboration numérique sécurisée pour préserver la confidentialité des données.
	Cognigo	Solution de gestion des données pour conformité au RGPD.
	Silverfort	Solution d'authentification multifactorielle biométrique.
	Intezer	Solution d'analyse génétique des logiciels malveillants.
	SecBi	Solution de détection des menaces avec *machine learning* non supervisé.
	Nanolock	Solution de protection et système sécurisé de gestion à distance des terminaux.
	Minerva	Solutions de sécurité des objets connectés.

À PROPOS DU CIGREF
ACTEUR DE LA SOCIÉTÉ NUMÉRIQUE

Association des grandes entreprises et administrations publiques françaises, le Cigref se donne pour mission de développer leur capacité à intégrer et maitriser le numérique.

RÉSEAU DE GRANDES ENTREPRISES

Association loi 1901 créée en 1970, le Cigref n'exerce aucune activité lucrative. En 2018, il regroupe près de **150 grandes entreprises et organismes français utilisateurs de systèmes numériques**, dans tous les secteurs d'activité.

ACTEUR DU NUMÉRIQUE

Par la qualité de sa réflexion et la représentativité de ses membres, **il est un élément fédérateur et acteur important de la société numérique.**

AU SERVICE DE SES MEMBRES

Sa gouvernance est assurée par **15 Administrateurs**, élus en Assemblée générale. Son activité est animée par une équipe de **10 permanents.**