JANUARY 2019

CIGREF REPORT

CYBER & INNOVATION IN ISRAEL

Cigref Learning expedition in November 2018

Cyber & Innovation in Israel

Cigref Learning Expedition in November 2018

January 2019

Cigref is a network of major French companies and public administrations set up in order to develop its members' ability to acquire and master digital technology. It is a key player and federating body in the digital society, thanks to its high-quality thinking and the extent to which it represents its members.

Created in 1970, Cigref is a not-for-profit body in accordance with the French 1901 Law of Associations. It counts among its members some 150 major French corporations and public administrations across all business sectors. It is overseen by 15 board members who are elected by the General Assembly. Its day-to-day work is carried out by a team of ten permanent members of staff.

Browse all our publications at www.cigref.fr | Follow us on Twitter: @Cigref

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

OVERVIEW

A Cigref delegation led by Jean-Claude Laroche, CIO of Enedis, Cigref Director and Chairman of Cigref's Cybersecurity Circle, spent four days in Israel, from 11 to 15 November 2018, looking at the twin subjects of innovation and cybersecurity. The Cigref delegation was composed of some twenty representatives of Cigref member companies, accompanied by three members of parliament sitting on the Commission Supérieure du Numérique et des Postes (Higher Committee for Digital Technology and Postal Services), Mireille Clapot, Christine Hennion and Eric Bothorel, by the General Secretary of the Committee, Ludovic Provost, and by our partners Shushane&Co and Sia Partners.

The delegation's four-day expedition included numerous meetings with the leaders of Israeli startups, top Israeli officials such as the Director General of the National Cyber Directorate, the Israeli equivalent of the French National Cyber Security Centre, the Chairman of the Israel Innovation Authority, members of the Knesset, Israeli parliament, and the director of the Ben-Gurion University's Cyber R&D centre in Beersheba.

As part of this trip to Israel, our delegation was honoured to be received by the French Ambassador in Tel Aviv, Hélène Le Gal, for a reception to which she had also invited representatives from French tech firms operating in Israel.

In the twin field of technological innovation and cybersecurity, Israel plays a unique role on the global stage. The self-described "startup nation" has managed to carve out a niche for itself as a central R&D hub for the world's tech giants and investors. For over ten years, as part of a highly determined effort, all stakeholders in Israeli society – public and private, military and civilian, academic and economic – have worked together to develop a coherent, thriving ecosystem focused on digital technologies and cybersecurity. While this high rate of innovation can probably at least partly be explained by Israel's one-off geopolitical situation, we think that there are lessons to learn from how Israel paved the way for this remarkable success story, which made an impression on every single member of the delegation.

ACKNOWLEDGEMENTS

We would like to thank all members of the Cigref delegation led by Jean-Claude Laroche, CIO of Enedis, Cigref Administrator and Chairman of Cigref's Cybersecurity Circle, for their contributions to this joint effort:

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

We would also like to thank the Members of Parliament who accompanied us:

Eric BOTHOREL, MP for Côtes d'Armor,

Mireille CLAPOT, MP for Drôme,

Christine HENNION, MP for Hauts-de-Seine,

And Ludovic PROVOST, General Secretary of the Commission Supérieure du Numérique et des Postes.

Lastly, we would like to thank Jean-Pierre CORNIOU (Sia Partners) for his excellent guidance, and Nelly SOUSSAN (Shushane&Co), for perfectly organising this learning expedition.

This paper was written by Clara MORLIÈRE (Cigref) with contributions from Jean-Claude LAROCHE (Enedis) and Jean-Pierre CORNIOU (Sia Partners).

TABLE OF CONTENTS

TABLE OF FIGURES

1. Main observations

Faced with the growing number and increasing complexity of cyberattacks, in a tense geopolitical climate, the Israeli "ecosystem" worked together on the research and development (R&D) of technologies to create numerous innovative solutions and develop use cases to effectively combat cyber threats. This package of initiatives led to a proliferation of startups, making Israeli the "startup nation" and a leader in cybersecurity.

As a country, Israel is quite young (70 years) and small (28 times smaller than France); 60% of it is desert, and it has a population of 8.7 million. The country boasts 4% growth and invests 4.3% of its GDP in R&D. In Israel, private finance accounts for more R&D than any other country, as a proportion of approved spending. Unemployment continues to fall, and the economy is approaching full employment.

The Israeli economy has two very contrasting sectors:

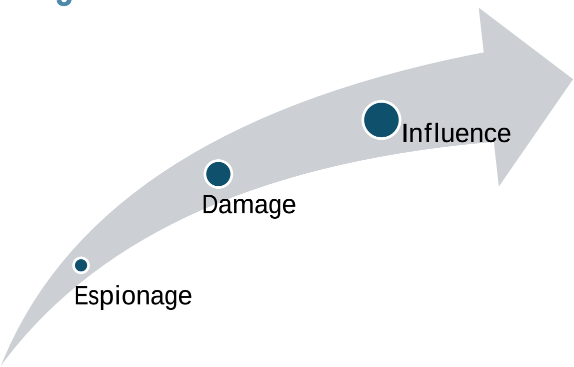
- a highly developed high-tech sector which attracts around 20% of worldwide investment in cybersecurity technology. This is reflected in the opening of numerous R&D centres by US technology companies;
- and a sector with one of the highest rates of poverty in the OECD; for this reason, cybersecurity is used as a means of social integration and mobility.

Investing in technology therefore is very much a societal choice made by the government and the business stakeholders. It has led to the development of a set of very dynamic players sharing common goals. The links forged between the education and military systems and this fabric of stakeholders help generate the skills and resources needed for the ecosystem to grow steadily.

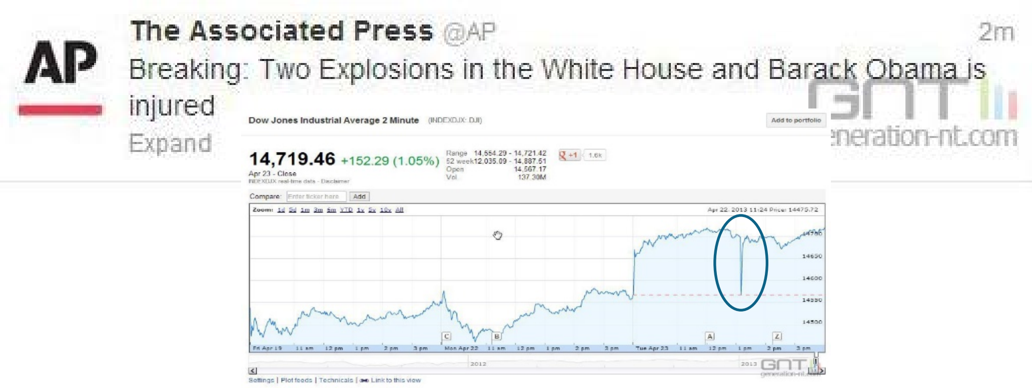
1.1. A growing number of cyber threats and innovative cybersecurity solutions

The delegation was struck by the number and diverse nature of the threats discussed during the presentations, and the number of solutions available on the market to tackle them. There are so many solutions on offer that they often seem redundant, and it is hard to get an overall picture of them. Indeed, large companies looking for solutions that meet their needs find it difficult to choose between them. It should be stressed that an open source cyberdefence methodology has been developed and adopted by Israeli organisations.

1.1.1. Cyberattacks: growing in number and inevitable



The *Israeli National Cyber Directorate* divides the marked increase in threats into three "generations" of cybercrimes: the first generation built on means of espionage, the second aimed to cause damage, and the third seeks to produce influence. The threat of influence has grown in tandem with social media and the ability to use social networks to manipulate opinion. A significant example was the hacking of the Associated Press Twitter account, which had a direct impact on the price of shares on the NASDAQ stock exchange.



The Associated Press @AP 2m
Breaking: Two Explosions in the White House and Barack Obama is injured
Expand

Dow Jones Industrial Average 2 Minute (INDEXDJX: DJI)

14,719.46 +152.29 (1.05%)
Apr 23 - Close
INDEXDJX real-time data - Disclaimer

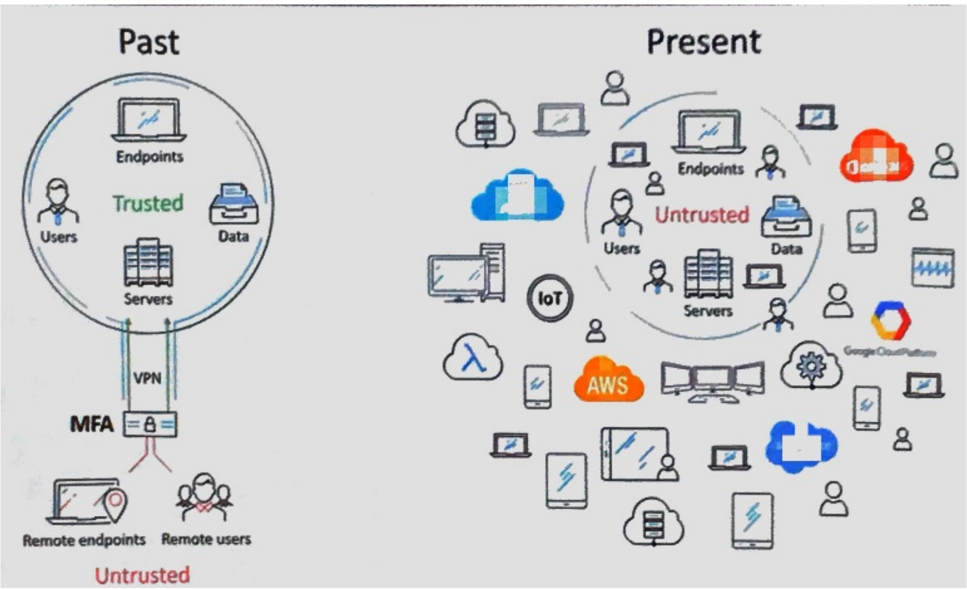
Range 14,554.29 - 14,721.42
52 week 12,035.09 - 14,887.51
Open 14,567.17
Vol. 137.30M

Source: Génération Nouvelles Technologies

Figure 1: Hacking of the Associated Press Twitter account in 2013

Everyone seems to agree that the question is not "if" but "when" a company will be attacked. The challenge is knowing when a future attack will happen in order to minimise the damage. All Israeli critical infrastructure companies have been attacked in one way or another. Israelis who have served with military cyber units have learnt the techniques used for cyberattacks and their mysteries: "a cyberattacker will always find a vulnerability to exploit" in order to penetrate companies' systems, in the same way that physical locks are still vulnerable. That is why the solutions being developed focus increasingly on protecting infrastructure once an attack has been detected rather than on building a defensive "wall". Understanding how attackers behave and how they use cyberattack tools allows to identify intrusions more easily. Prevention therefore entails understanding an assailant and nullifying his attacks.

Moreover, the threat is growing: all company's connected objects and industrial systems are now designed to be brought within the scope of its information system. Cybersecurity now concerns the operational functioning of the company. The threat is more concrete and precise: attackers can not only alter data but also compromise the security and continuity of operation of industrial facilities. The vulnerabilities of these operational technologies differ but the convergence between the two systems (information system and industrial system) also threatens operational continuity, rather than just data integrity, as in the past.



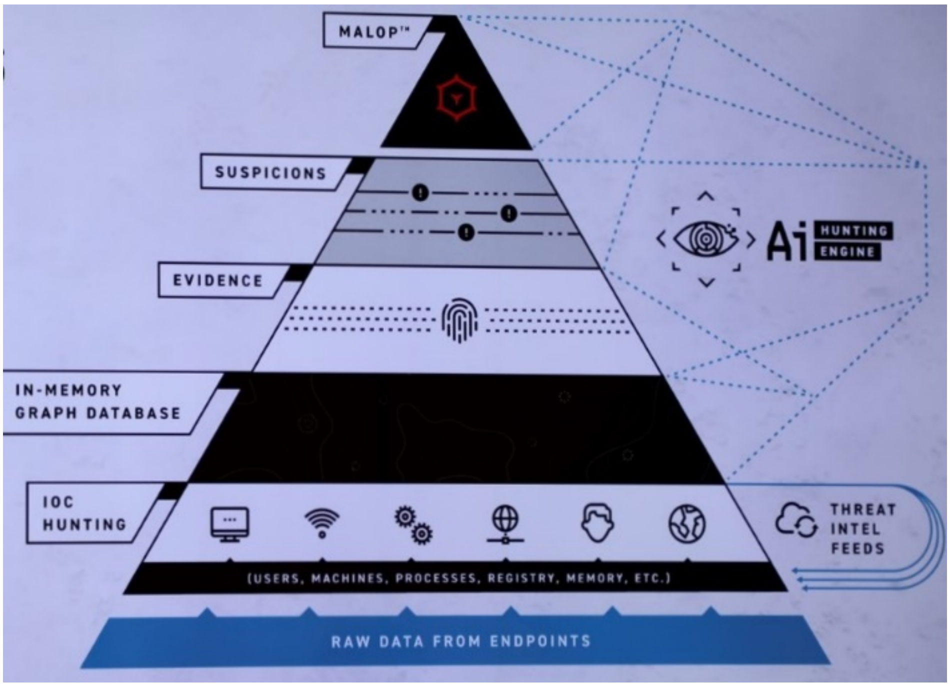
Source: Silverfort

Figure 2: The growing complexity of companies' integrated environments

To address the inevitability of cyberattacks, the Israeli government has forced its large companies, equivalent to France's "operators of vital importance" (OIV), to spend 8% of their revenues on cybersecurity (the average in France is 3-4%), demonstrating the importance attached to this issue.

1.1.2. Integration of solutions by large Israeli groups

The stakes faced by economic and military actors are forcing startups to constantly seek performance gains using technological tools. Attacks are rarely sudden; malicious agents get in long before the attack and have to be identified using a variety of concurrent methods.



Source: Cybereason

Figure 3: Stages in the anti-intrusion strategy

The startups we met (see section on the Stakeholders interviewed, page 16) presented technological solutions boasting a diverse range of anti-cyber threat capabilities. They cover the full spectrum of actions to take in order to prevent, detect and react to cyber threats. Some startups are developing solutions to:

- Search the open, deep and dark webs
- Search in a company's IS databases to take steps to ensure GDPR compliance
- Analyse software to detect malicious sections of code
- Strengthen end-points authentication methods to make them more secure
- Prevent access to end-points' internal memory to protect its integrity
- Detect abnormal activity on a company's end-points (internet-connected or otherwise)
- Identify infected end-points to isolate them from the rest of the IT system
- Reconstitute and analyse the attacks' chronological steps.

The startups' presentations prompted numerous questions about the relationships between them and large Israeli firms: about how solutions are selected, about the maturity of the offerings, and about dependence on these solutions.

Selection of solutions

Lots of companies are working on the same issues, with similar solutions, and often describe themselves as complementary. This diversity is no obstacle and is in line with the "*Better an overlap than a gap*" doctrine espoused by the National Cyber Directorate.

There is therefore a pressing need to identify and select the best solutions. French companies operating in Israel, like Orange and Thales, are testing and evaluating solutions from numerous startups, using Proofs of Concept with a view to integrating them into their offerings.

Maturity of offerings

The startups offer a variety of solutions depending on their size, age, development type and approach to problems. This makes it hard to assess their maturity and ability to solve the issues faced by large groups, hence the need for intermediaries to integrate these solutions.

Obsolescence of offerings

Cyber threats are growing in number, which can quickly render solutions companies buy obsolete and therefore complicate their financial management and governance. Nonetheless, new solutions are being deployed more quickly, which suggests a move to disposability. The apparent ease, promoted by startups, with which companies can move from one solution to another enables them to implement new solutions as new cyber threats arise.

Dependence on solutions

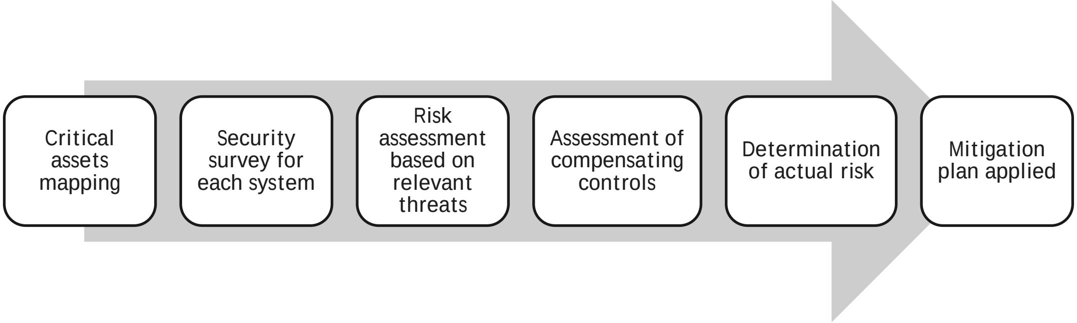
The systems offered are fully integrated into companies' information systems through end-points (connected devices, whether they be computers, tablets, telephones or servers). These solutions have significant analytical capabilities and are very intrusive when fulfilling their prevention and protection functions. Nonetheless, questions might be asked about what level of operational dependence a company is prepared to accept. A company should be in a position to audit the solutions it deploys in order to check they actually do what they are supposed to do and do not do what they are not supposed to do. Another challenge in terms of companies' dependence on solutions is what control they can have over the upgrades of critical solutions, in other words whether they have market power over the supplier.

1.1.3. Methodological approach to system protection

Israeli companies take a national approach to cyber defence. This shared methodology is developed by the National Cyber Directorate.

Focus: Cybersecurity management by Israel Railways

The Israeli rail operator has to address a large number of cyberattacks. In order to prioritise investment and the actions to take in the company, Israel Railways has in place a package of measures to assess risk and determine the mitigation plan.


Critical assets mapping
Security survey for each system
Risk assessment based on relevant threats
Assessment of compensating controls
Determination of actual risk
Mitigation plan applied

Source: Israel Railways based on the Israeli National Cyber Directorate method

Figure 4: The Israel Railways cyber defence methodology

The mitigation plan comprises three "cyber-practice" pillars: *People, Process, Technology*. Among their best practices, they recommend three:

- **PEOPLE**: Investing mainly in raising employee awareness and training. Creating "cyber-trustees", aka "cyber-champions": employees who have completed advanced training, which means that informed staff can be placed in the company's various entities.
- **PROCESS**: Monitoring the *supply chain,* which is a weak point: authorise and check each login to systems by providers and suppliers, who are themselves evaluated before each contract is signed and then regularly throughout the term of contracts.
- **TECHNOLOGY**: Supervising systems via SIEMs (Security Information Management Systems) and SOCs (Security Operations Centres): use of new military technologies and optimisation of existing systems.

1.2. Numerous technological breakthroughs

Participants who had visited Israel on learning expeditions before were struck by the speed of progress; those on their first trip noted the disruptive nature of the innovations presented. After one year, the technological acceleration is visible, for example with the integration of 5G.

Startups are developing more and more cybersecurity techniques and honing them to adapt them to any context: we are now seeing full Security Operations Centres (SOC) that can be used as is by end users. Making machine learning secure is another key topic addressed by the R&D centre of Ben-Gurion University of the Negev. Lastly, the growing number of 5G use cases was demonstrated by Qualcomm. All countries are looking over each other's shoulders in this geopolitically vital field.

Israel is also looking to invest in tech research underpinned by basic science (homomorphic encryption, quantum computing, etc.). Homomorphic encryption is a very promising field for widespread use of cloud computing and for guaranteeing the protection of data used for processing operations.

1.2.1. Maturity of cybersecurity techniques and securing machine learning

Major breakthroughs are being made in machine learning, and this field along with deep learning will continue to be developed by researchers for many years, in the view of the delegation. Some of the startups the delegation met demonstrated real capabilities in these fields. According to the speaker from Ben-Gurion University, machine learning is quite insecure because researchers neglected to embed cybersecurity, he says it is incredibly easy to compromise. The Ben-Gurion University research centre is therefore trying to find securer learning models by striking a balance between resilience and precision in order to avoid attacks aiming to bait learning processes.

In recent years, growing awareness of the importance of privacy has led lawmakers to tighten regulations in Europe and the US. At the same time, people are trying to collect more data for analysis. Can these two aims be combined? One of the startups the delegation met, Duality, offers a platform that produces encrypted data that can then be used for processing operations, thereby making collaborations between stakeholders (data owners and data processing providers) quicker and easier.

1.2.2. Mass deployment and management of connected objects

The mass deployment of connected objects and their management, such as in remotely managed fleets of connected vehicles, pose real challenges for companies.

Focus: Remote management of connected objects by Harman (a Samsung subsidiary)

To upgrade a fleet of vehicles with a range of embedded software programs (operating systems, microprograms, applications and cards), cloud connectivity is essential; it gives an overview of the location and level of use of the fleet, allowing to gather all the information needed in order to monitor it, and to act in response. This means that carmakers will have to use “Over-The-Air”[1] (OTA) solutions, a technology enabling remote access to SIM card data in order to deploy new services and update systems but also mitigate cyber risk. In 2013, Harman bought **Redbend**, which is specialised in the remote monitoring of connected objects using OTA technology and which is now the leader for software management[2] in the car industry. Harman also bought **iOnRoad**, which offers image recognition for the automotive sector, and **TowerSec**, a cybersecurity startup working in the same sector.

1.2.3. Growing number of 5G use cases

For the first time, products will soon be available that use 5G, marking a breakthrough for the technology. 5G networks are intended to generate huge volumes of data with complex constraints. They will be able to support large bandwidth needs and offer very short latency. The use cases indicated are many and varied, as 5G provides the capability to manage fleets of mobile objects, such as driverless cars or robots in supply chain and factories.

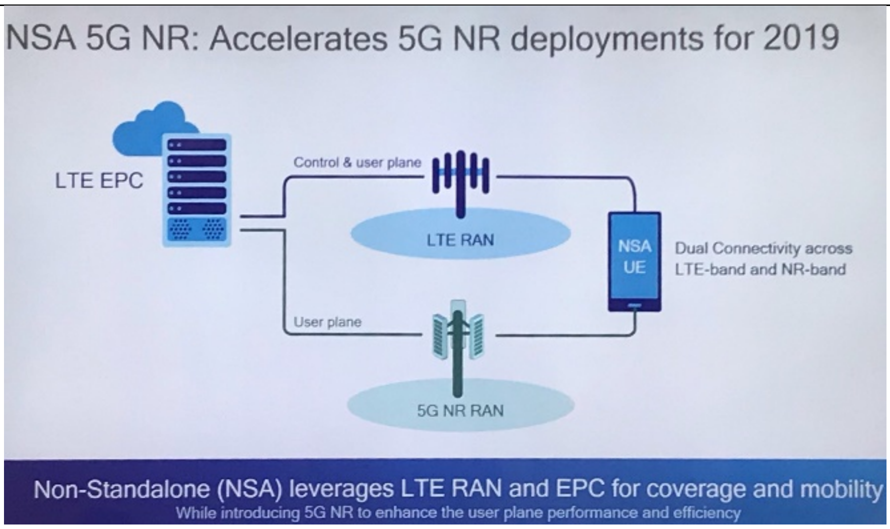
The 5G adoption process has begun. The question that arises is how to grasp these tools so that the technologies can flourish quickly in France. The French telecom operator Orange is at the forefront of 5G development and deployment in France.

Focus: 5G network developed by the Qualcomm R&D centre

5G is Qualcomm’s biggest bet. The Tel Aviv R&D centre is focused on manufacturing chips and on associated algorithms for 5G. 5G NR (New Radio) will meet the insatiable demand for mobile broadband and increase data speeds up to 6 Gb/s, enabling object-to-object connections and the development of new vertical markets: industrial IoT, autonomous cars and transport, remote healthcare, smart agriculture, smart cities, etc. For example, the “C-V2X” solution is underpinned by 5G and intelligently connects the car’s environment with the road infrastructure and other vehicles. Qualcomm is working with all other 5G operators to ensure compatibility between operators.

[1] https://en.wikipedia.org/wiki/Over-the-air_programming

[2] https://www.businesswire.com/news/home/20150122005522/en/HARMAN-Acquire-Red-Bend-Software



NSA 5G NR: Accelerates 5G NR deployments for 2019

Non-Standalone (NSA) leverages LTE RAN and EPC for coverage and mobility

While introducing 5G NR to enhance the user plane performance and efficiency

Source: Qualcomm

Figure 5: Combined use of 4G and 5G for better connectivity

1.3. Educational and military systems with a high impact on the development of skills and of the ecosystem

During the course of the presentations, meetings and tours, the delegation was struck by the great technological expertise demonstrated by everyone they met. Faced with a threat tied in with its environment, Israel has made cybersecurity development into an economic but also a social opportunity, using computing as a way of training young people. Starting very early, in childhood, using a “tech exposure” approach, the development of knowledge and skills in computing, coding and cybersecurity software continues in specialized extracurricular programmes and in the army, which instils discipline in young people and gives them confidence, a key factor in professional success.

1.3.1. Technological acculturation for children and social mobility

Israel includes technological acculturation in its school curriculums; technology thus serves as a means of integration and social advancement.

Focus: Presentation by Eli Elaluf MP

MP Eli Elaluf, Chairman of the welfare, health and labour committee, published a report on poverty in Israel after consulting 40 specialists, including academics and senior civil servants. The adoption of the report was the second decision of the current coalition government. The aim of the report’s recommendations is to raise Israel’s disadvantaged population out of poverty. The MP says that doing this requires interventions in every area of life: in the economy, culture, healthcare, social services, housing, environment, social situation of poor people, and last but not least education. For this reason, IT and cybersecurity training courses for disadvantaged young people have been promoted and rolled out nationwide. The Rashi Foundation, a pioneer in this area, has signed a contract with the army to train thousands of secondary school pupils with a view to helping them join the army's most sophisticated units.

1.3.2. Mentoring of young people

During the presentations and tours, the delegation gained a clear insight into the defining influence of the army on startups and companies. The period of compulsory military service gives confidence to 18- to 21-year olds: they realise what they are capable of from an extremely practical rather than solely theoretical perspective. This observation generated interest from some participants at a time when the French parliament was debating developing universal national service.

Focus: Military service

Currently, basic military service in Israel lasts 2 years for women and 3 years for men. Recruits are increasingly being encouraged to stay on longer (6-7 years) or even to make a career in the military. This longer commitment allows the parties to agree between themselves, whether explicitly or tacitly, to design civil applications that reuse technologies developed in the army. The army's solutions are focused on optimising resources (automation of alerts to be processed, using virtual assistants to optimise analysts' searches for evidence, detecting attacks, etc.), techniques which companies will also find useful.

From childhood, Israelis are taught to value defence. The heightened discipline experienced in the army gives rise to the development of a common mindset. In the military, young people are exposed to the latest technologies, receive training (technical know-how and interpersonal skills), develop a strong spirit of cooperation combined with an appetite for intelligence, and gamification is also a way of harnessing energies. Mentally, 18-year-olds grow up very quickly, becoming responsible, mature and capable of working in teams. When they leave the army, they are thus ready to join startups or large firms.

1.3.3. Talent spotting and selection of startups

The Israeli ecosystem has a proven capacity to detect competent people and spot talent. The young age of many speakers, and their self-confidence during their presentations, were noted by the delegation. However, not all were just starting out in their careers, and the diverse range of profiles also demonstrates Israel's ability to harness all talents.

Focus: The army's selection of recruits

The army's recruitment process is underpinned by a selection mechanism based on intelligence potential, personality and physical fitness. Candidates are asked to tackle specific scenarios which will allow recruiters to assess in particular their human attributes. The Israeli army's technique is to get experienced generals to work with young people, whose creativity is encouraged. It reflects a mindset and a mutual respect that result in the success of this intergenerational collaboration.

From the skills perspective, computer and mathematical sciences are central to the cybersecurity field. But these skills must be combined with psychology and other social sciences if they are to be brought to bear more effectively. The development of this skillset means that Israel has a pool of the talents that businesses need.

Focus: Selection of startups in Israel (mechanism used by investment funds and the Innovation Authority)

The Innovation Authority chooses to support companies that have developed innovative technology and boast a solid management team that has good technological and business knowledge, and can be easily coached. The technology must demonstrate not only that it is innovative but also that it offers a clear competitive edge. Up to 50% financing of expenditure is permitted.

1.4. Choice of companies to develop an ecosystem

"*Cybersecurity is a necessity, a State responsibility, a business*."

Israeli leaders' choice of companies is based on a cutting-edge national defence strategy. Israelis have chosen to be experts in the technologies themselves rather than depending on other countries; they want to take responsibility for ensuring their own security. The whole ecosystem is then brought deliberately into line. The primary aim of a tech startup is to build on Israel's technological excellence, developed in particular in the army, to design innovative solutions, export them quickly to the rest of the world, generate rapid growth, and then after several years float successfully on the NASDAQ before selling up (called "exit"). The global export strategies and the growth that they generate encourage the development of R&D, thus forming a virtuous circle. This incentive to develop solutions commercially has a positive knock-on effect for technology financing.

1.4.1. Cutting-edge national defence strategy

Despite its small size and population, Israel does not shy away from tackling major global challenges (including smart cities). The delegation was struck by the tangible dynamism in Israel, in many fields, down to territorial planning. It is clear that one of the reasons for this dynamism is the existential fear of "being wiped off the map" by the country's enemies, the fear of disappearing.

Given the geopolitical context, Prime Minister Benjamin Netanyahu decided to take direct responsibility for cybersecurity and committed resources to a comprehensive programme. In the space of ten years, Israel has become recognised as a global leader in this field. The State's services in this area are organised on a continuum ranging from the posture of attacker to that of cyberdefence. This choice also points to the conclusion that any insecure innovation constitutes a threat and that a secure innovation is an opportunity. The "necessary but not sufficient" condition for innovation is therefore cybersecurity and the country anticipates an exponential growth in innovation.

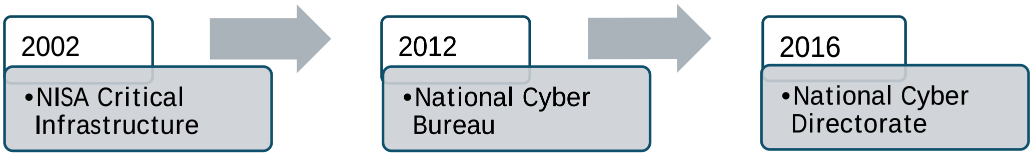
The delegation met with two major players in the development and implementation of this strategy: the Israeli National Cyber Directorate and the Innovation Authority.

Focus: Israeli National Cyber Directorate

In 2016 the Israeli Prime Minister set up the **Israeli National Cyber Directorate** (INCD). It is tasked with keeping Israel safe and protecting business continuity, notably by bringing together the government and the private sector.

The Director of the INCD, Yugal Unna, therefore reports directly to the Prime Minister and has clear responsibilities to companies and civil institutions (including opening a public cyberattack hotline). The distribution of responsibilities is in line with the "*Better an overlap than a gap*" doctrine: the government would rather duties overlap than that there were unprotected areas.

The INCD's role is also to raise awareness and train actors: Israeli MPs have been trained in cybersecurity issues. Along with the Israel Export Institute, the INCD also contributes to the construction of partnerships and collaboration with the international community on cybersecurity issues in a range of critical sectors, including aviation (agreement with Airbus in France), domestic security and the medical sector. Cybersecurity is now defined in broader terms, and these terms will become increasingly wide-ranging: one of the INCD's roles is to plan for this.



Source: *Israeli National Cyber Directorate*

Figure 6: Evolution of organisations responsible for cybersecurity in Israel

Focus: Innovation Authority

The **Innovation Authority,** led by Ami Applebaum, Israeli Chief Scientist, is the government agency that develops and finances innovation in Israel. The Innovation Authority is the link between the private and public sectors, promoting innovation and developing the burgeoning array of startups and innovative initiatives. It is a cornerstone in the evolution of technology in Israel. Backed by government funding worth 500 million dollars, the Innovation Authority issues calls for tender focusing on one technology or one field in particular. Each dollar invested by the government via this agency eventually generates between 5 and 8 dollars for the Israeli economy. The calls for tender are aimed at companies of all sizes (sole traders, startups and large groups). This agency gives only a percentage of the early-stage funding (50%) in order to monitor progress and ensure that results are consistent with objectives. It is given as a conditional loan: if the company is a success, it must repay the loan in instalments rising to 3 to 5% of its revenue; if the company fails, the loan is cancelled.

1.4.2. Bringing all players in the ecosystem into line

Israel has a real capacity to build functioning ecosystems at all levels by bringing into line all players supplying their respective skills, whether from the private or public sector. A full environment is created in part thanks to substantial State subsidies and to the investments made by multinationals. Members of the delegation were amazed by the national consensus on these issues, constantly reasserted by everyone we met.

Companies and public actors have set themselves a goal on cybersecurity issues, linked to a national survival objective, in order to ensure the country's economic development. Numerous factors and stakeholders have been brought together to build this Israeli ecosystem which depends on:

- the army as breeding ground for the skills companies need;
- R&D funding;
- strong industries, numerous R&D centres run by international companies, and startups;
- specialised skills delivered thanks to the relationship between academia and business.

Focus: Example of the Beersheba Cybersecurity Hub

In 1938, Beersheba was a tiny Bedouin village. The government has decided that Beersheba will be Israel's cybersecurity capital. Over the next two years, this town in a poor area will become the region's major cybersecurity centre. The hub is located around the university and the government's cybersecurity agencies, including the national CERT. The 40 multinationals, 10 incubators/venture capital funds/accelerators and 460 Israeli cybersecurity startups will join this cybersecurity hub.

A fruitful dialogue seems to be developing between academia and the business world, manifested in numerous partnerships between companies and universities. Programmes are being constructed with universities, thereby helping to create centres of excellence which, through academic and professional training courses, are nurturing the abilities and skills that companies need. Academia is one of the key pillars of the ecosystem.

Focus: Ben-Gurion University R&D centre

Ben-Gurion University, the only university in the country to grant engineering degrees, is a very dynamic academic institution, ranked 91st in the world in terms of patent requests, with 30% of these requests in the field of computing (ranking it between Yale and Princeton).

The Ben-Gurion University R&D centre pursues two main fields of research: computing (split half and half between cybersecurity and data analysis/AI) and biotech.

The R&D centre is financed by partners on the basis of applied research projects, with a University Technology Transfer Office which markets the results of the institution's research, thereby strengthening ties between the university and business. The R&D centre employs 150 people and teaches not only 33% of the university's 19,000 students, but also young people on cybersecurity training programmes.

As well as skills and initiatives, Israel is developing a mindset of collaboration and support between stakeholders so that everyone can benefit from the opportunities.

This business-centric mentality was clear from day one, when one speaker said: "*For us, the most important thing is customer satisfaction, the company would do everything for the customer even if it meant walking through walls*".

In addition, the relationships forged with foreign players help to enhance the skills and portfolio of their ecosystem, and to grow the appeal of Israel as a whole.

1.4.3. A serious business with an international outlook

In Israel, cybersecurity is regarded as a "serious business" that is growing exponentially, and the cybersecurity environment in the country is ultra-commercial. Startups very quickly focus on growing their businesses internationally because Israel is not regarded as a market in itself. They begin exporting very quickly, to the United States in particular, although they do continue to grow the domestic side of their businesses. However, there are few Israeli multinationals. It is mostly foreign actors and in particular the United States that tap into the value by acquiring Israeli companies (e.g. Waze, Mobileye). Israel is therefore moving from being the "startup nation" to the "scale-up nation".

At all the presentations and meet-ups around the HLS & Cyber Conference, Israeli actors demonstrated their eagerness to collaborate and to share their solutions. They are on the lookout for any effective solutions, wherever their partners are from (except for countries that do not recognise Israel or are enemy states). Israelis' clear openness to collaboration explains in part the significant presence of international delegations beating a path to their door at the HLS & Cyber Conference, and all year round, because Israel is a leader in innovation and cybersecurity.

Israel is implementing policies to attract multinationals such as Microsoft, IBM, Checkpoint and Renault.

Focus: Openness to international collaboration at HLS & Cyber conferences

Chairman of HLS & Cyber

"International cooperation is necessary, but is it possible? Can countries share and exchange information? These obstacles must be overcome to fight for what's right. Israel has much to offer."

Minister of the Economy and Industry

"Israel is the number 1 for R&D and reaps the rewards in cybersecurity. The country has the best cybersecurity technology as a matter of necessity. For Israel, there can be no choice other than to work beyond our borders because attackers do not respect borders. The ties and relationships forged at the HLS & Cyber conference will help to make the world more secure."

Israel Export Institute

"HLS & Cyber conferences are attended by representatives of about 90 countries from around the world. Israel is ready to share its innovation with the world. The Israel Export Institute believes in the following slogan: 'We do good to the world', and remember: 'It is a flat word and an unsafe one'".

2. Main takeaways from the learning expedition

2.1. What is transferable to France

- Acute awareness of the vulnerability of complex systems;
- Integration of security into any business model: “Security by design”;
- Systematic security architecture: you can only control what you know inside out;
- Detection of weak signals: a proactive culture;
- Cybersecurity begins when leaders gain awareness and make commitments;
- IS development in the IoT world is one trigger for this awareness among leaders;
- Thinking distribution, integration and market size is vital for startups.

2.2. What is specific to Israel

- The key role of the army as cultural, behavioural and technical melting pot;
- A feeling of urgency shared by the whole population;
- Technical enthusiasm which begins at school;
- Funding from all global tech giants, especially big American companies;
- A battery of 460 globally-oriented cybersecurity startups.

3. The delegation's recommendations

3.1. Societal stakes for France

- Raise awareness of all stakeholders, in the political, economic, professional and academic spheres, of the future transformation challenges;
- Give meaning: build, share and communicate a collective project aiming to further the common good to get people on board;
- Immerse young people in technologies as early as possible, but also the rest of the population, to change perception on societal technological progress and bridge the digital divide;
- Find drivers of educational excellence in France, capitalise on existing training programme, promote courses of study;
- Focus efforts, increase the country’s appeal and keep talents and skills;
- Build on the ethical awareness of the European population (GDPR).

3.2. Challenges for French companies

- Develop business's cyber resilience to address the fast-growing number of cyber threats;
- Train, develop skills and be attractive to keep talented employees;
- Consolidate risk management, audit chosen solutions and their upgrades roadmaps;
- Rethink internal organisational structures by harnessing data and cybersecurity to converge industrial and information systems;
- Encourage proofs of concept with startups and work with solution integrator intermediaries to industrialise them;
- Communicate with all staff to raise their awareness, immerse them in the digital culture, and reassure them about its development;
- Think “customers” and “world market”.

4. Stakeholders interviewed

Institutions	**French embassy**	Discussions with Madame Hélène Le Gal.
	Israeli parliament	Discussions with Eli Elaluf MP.
Public Authorities	**Innovation Authority**	Governmental organisation which develops and funds innovation in Israel (the equivalent of the French Public Investment Bank called BPIFrance).
	Israeli National Cyber Directorate	Agency responsible for the security of the private sector and Israeli civil institutions, reporting to the prime minister (the equivalent of the French National Cyber Security Centre called ANSSI).
	National CERT	Governmental centre providing intelligence, alerts and responses to cyberattacks.
Venture Capital	**Glilot Partners**	Specialist investment fund for B2B cybersecurity startups and the use of data.
Multinationals	**Qualcomm R&D centre**	R&D centre focusing on the development of 5G: technology and use cases.
	Harman	World leader in connected automobile technology, audio innovations, cloud services and IoT solutions.
Israeli companies	**Israel Railways**	Meeting with the deputy CISO.
	Verint	Cybersecurity solutions for researching the open, deep and dark web.
	Cybereason	Cyberattack detection solutions.
University	**Ben-Gurion University of the Negev**	R&D centre focusing on computing and biotech, with applied research projects.
Startups	**CyberX**	Cybersecurity solution for industrial IoT.
	Duality	Secure digital collaboration platform to maintain data privacy.
	Cognigo	Data management solution for GDPR compliance.
	Silverfort	Adaptive multi-factor biometric authentication solution.
	Intezer	Genetic detection and analysis solution for malware.
	SecBi	Full-scope threat detection solution with unsupervised machine learning.
	Nanolock	Device protection solution and secure remote management system for end-points.
	Minerva	Connected objects cybersecurity solution through deception.

ABOUT CIGREF
KEY PLAYER IN THE DIGITAL SOCIETY

Cigref is a network of major French companies and public administrations set up in order to develop its members ability to acquire and master digital technology.

NETWORK OF MAJOR COMPANIES

Created in 1970, Cigref is a nonprofit organization. It counts among its members some 150 major French corporations and public administrations across all business sectors, all users of digital services.

DIGITAL PLAYER

It is a key player and federating body in the digital society, thanks to its high-quality thinking and the extent to which it represents its members.

TO SERVE ITS MEMBERS

15 Board members, elected by the General Assembly, ensure its governance. A team of 10 permanent members leads the activities.