Global Alliance

Innovate UK

Connecting for Positive Change

ktn-uk.org/Global

Global Expert Mission
Cybersecurity in Israel 2018

Contact
Dr Nee-Joo Teh
Head of International and Development
neejoo.teh@ktn-uk.org

Contents

Welcome 4
Introduction 5
Cybersecurity Landscape in Israel 8
1.1 Policy, Regulation and Funding 8
1.1.1 Funding 9
1.1.2 The Cybersecurity Capital 9
1.1.3 Military Intellectual Property 9
1.1.4 The Cybersecurity Professions 9
1.1.5 Cyber and Financial Services 10
1.2 The Cybersecurity Ecosystem 11
1.2.1 Unit 8200 11
1.2.2 Israel Cyber Industry - Main Categories of Focus 11
1.2.3 Israel National Fintech + Cyber Innovation Lab 12
1.2.4 Education 13
1.2.5 Cybershark 13
1.2.6 IL-Cert 14
1.3 Israel Cybersecurity Market and Investment 15
1.3.1 Government Incubators 16
1.3.2 Israel University VC Funds 16
1.4 Research , Innovation and Commercialisation 17
1.4.1 Academic Research 17
1.4.2 Technology Transfer Offices 18
Conclusion 19
1.5 History and Policy 19
1.6 The Israel Cyber Ecosystem 19
1.7 Synergies in the UK 20
Annex 1 - List of UK Participants 21
Annex 1 - List of Israeli Participants 22

Welcome

Innovate UK's global missions programme is one of its most important tools to support the UK's Industrial Strategy's ambition for the UK to be the international partner of choice for science and innovation. Global collaborations are crucial in meeting the Industrial Strategy's Grand Challenges and will be further supported by the launch of a new International Research and Innovation Strategy.

Innovate UK's Global Expert Missions, led by Innovate UK's Knowledge Transfer Network, play an important role in building strategic partnerships, providing deep insight into the opportunities for UK innovation and shaping future programmes.

The Cybersecurity Expert Mission travelled to Tel Aviv and Be'er Sheva in June 2018 and in this publication we share the information and insights gathered during the delegation's time in Israel.

Introduction

Innovation is a major driver of productivity, economic growth and development. Many OECD countries are looking to boost productivity through investments in science, technology and research and development (R&D). Israel's innovation laurels are numerous – highest gross expenditure on R&D (4.3% of GDP), largest number of companies listed on NASDAQ outside of North America, highest level of venture capital as share of GDP, highest number of graduates per capita anywhere in the world, the highest number of engineers per capita and the largest number of start-ups in Europe, second only to the United States globally. In the Deloitte Global Venture Capital Confidence Survey in 2015[1] Israel is second only to the United States (quite an accomplishment given the geopolitical landscape in the region). Around 8.38% of employment in Israel is tech-related, generating 12% of business sector GDP and contributing a massive 43% of exports[2].

There is no doubt that smart policies have played a key role in spurring innovation. The Israeli Government made a crucial strategic decision to jump-start a science-based sector by providing financial support for commercial R&D. This policy was designed to make up for the market failures and the heightened risk in operating in a geographically-isolated market like Israel. The Office of the Chief Scientist (now the Israeli Innovation Authority (IIA) [3]) was created in 1969 within the Ministry of Industry, Trade and Labour, and would eventually become an important player during the high-tech boom.

Israel's export-based high-tech sector has only really begun to emerge since the 1990s. Israel also had the human capital by the early 1990s to fuel the boom. Israel's compulsory military service provides early training in sophisticated technologies (read more about Unit 8200 in see section 1.2.1). Furthermore, the country saw the influx of almost one million ex-Soviet Jewish immigrants in the 1990s. These highly-educated immigrants, whose ranks included 82,000 Russian-trained engineers, assimilated into the local labour market, providing key scientific and IT skills.

Israel's culture of innovation is ingrained in its very foundation. Just as in the US, a few centuries before, the founders came to a "new" land to make a better life for themselves. Also like the US, opportunity and threats are two sides of the same coin, and settlers had a constant awareness of how everything they were fighting to build could crumble away. With this mentality, an urgency to develop new technology - whether the US inventing the revolver to combat bow-wielding Apaches or Israeli's latest missile defence systems – these two superpowers have constantly innovated to protect the nations they are building. If you are fighting to protect a life or culture, then it also must be worth doing. In Israel, there is a sense of individually and nationally, proving your worth to the world.

When it comes to building a technology community such as Silicon Valley or in Tel Aviv, the density of connections is also key. Silicon Valley grew out of communes with technologists and entrepreneurs cohabiting, causing connections and ideas to grow. This mirrors the dense ties Israel benefits from.

The principles of opportunity and threat when talking about the attributes that make Israel the Start-up Nation are clearly apparent:

- **Start-up Nation** – Founded in the twentieth century the country has had to build the infrastructure, economy and state from scratch. It also faced a number of issues such as defence, water supply and food supply which led to innovating to solve its own needs[4].
- **Immigration** – A nation founded and continually growing through aspirational immigrants wanting to make a better life for themselves who come to the nation and start their own businesses to provide for their family.
- **Culture of growing and selling** – The Expert Mission was told that it is desirable for start-ups to aim to exit in Israel. This is partly driven by venture capitalists (VC) but also out of necessity as acquirers with global markets are usually much better placed to sell a technology, and for Israel, this means that there is no brain drain and Israel retains the R&D.
- **Embracing failure** – Israel has a strong culture that embraces failure as a positive reflection on entrepreneurship and track record. Private investors do not view investment in uncommercial ideas as high risk as in the UK. This can be attributed to the chutzpah culture that instils a high degree of audacity to take on new challenges and appetite to succeed.

[1] Deloitte and National Venture Capital Association, Sept 2015
[2] Cybersecurity landscape and investments Israel, 2016 (CyberDB Research Dept, Jan 2017)
[3] www.matimop.org.il
[4] http://oecdobserver.org/news/fullstory.php/aid/3546/Start-up_nation:_An_innovation_story.html

The combination of skills, network and brand from military conscription enables new companies to be formed and raise VC money with ease, with the pipeline of talent and ideas continuous. Its key military benefits include:

- **Military as an education** – Instilling the right temperament in its population and giving a hard-working mentality to the young. Teenagers are given a lot of responsibility at a young age which prepares them well for the working world. The military also gives the technical skills and students are supported in degrees by the military by paying back service over a longer period.
- **Military as a network** – The density of connections in Israel is clear, and the military is the beginning of this where after conscription, peers go into different companies and industries but have built strong links. When they return each year to serve, this also builds new connections.
- **Military as brand** – Unit 8200 is a coveted brand with its members recruited into the tech world where success is expected. The technical training given is world-leading and allows them to create world-leading companies. People in 8200 get real-life experience and can take that invaluable training and experience and put it into practice in civilian life and the commercial world when they leave.

Government policy seems to have been instrumental in unleashing the potential of this abundant human capital. The technological incubator programme was set up in 1991, in part to provide skilled immigrants with funding and know-how to become successful entrepreneurs. It was run by the previous Office of the Chief Scientist, which funded potential entrepreneurs. Since the first companies emerged from the incubator programme in 1993, 61% have secured follow-on funding, and 40% are active to this day. The private sector has since invested over US$2.5 billion in incubator graduates, according to the OECD[4].

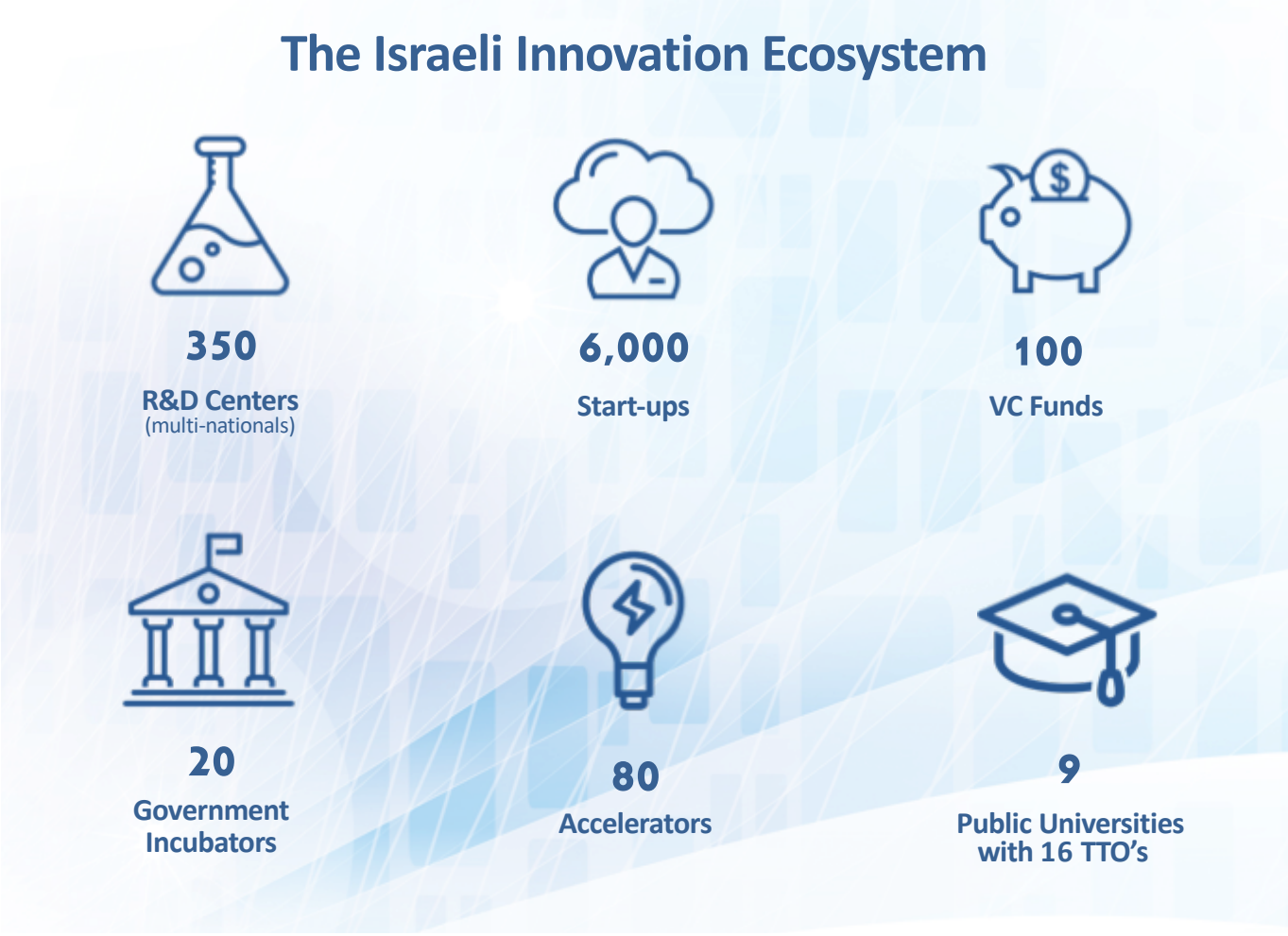

Figure 1 The constituents of the Israeli innovation ecosystem

Facing continual geopolitical conflicts created the confidence to solve problems that others deemed impossible. The fact that many of Israel's founders were scientists and intellectuals certainly laid the groundwork for placing a high cultural value on technology. But, above all, the fact that Israel is such a small country with limited resources confronting multiple simultaneous threats means it must rely on better tools and automation and ingenuity in order to survive. In one sense, Israel is defined and bolstered by the threats against it.

The combination of the country's perpetual concern with defence and its technological prowess has turned cybersecurity into one of its most important exports. In 2013 alone, IBM[5] , Cisco[6] , and GE[7] all made large acquisitions or investments in Israeli cybersecurity companies. And, because of the new security and privacy issues being raised by the spread of cloud computing, this trend has accelerated.

Israel identified cybersecurity as its fourth frontier thirty years ago. Capabilities and human capital have been developed in the Israel Defence Force (IDF)[8] and specifically Unit 8200[9]. They have and continue to see cyber and solutions for threats from a very holistic perspective incorporating:

- Education and professionalism
- Intelligence gathering
- Forensic investigation
- Scenario-based analysis
- State-of-the-art technologies
- Command and control
- Real-time presentation
- Comprehensive and continuous risk assessment.

The date, 3 September 2013 marked a new chapter in the history of the tech industry and cybersecurity in Israel. Prime Minister Benjamin Netanyahu led the inauguration of the Advanced Technology Park on the campus of Ben Gurion University of the Negev[10] in Be'er Sheva. The Be'er Sheva region is now the cyber capital of Israel, and a cyber ecosystem continues to flourish and grow there.

In the UK a thriving cybersecurity sector is a key national security and prosperity aim as set out in the five-year National Cybersecurity Strategy[11]. The accelerated pace of digital transformation brings about a great opportunity to promote the UK's cybersecurity expertise to international markets and to utilise that expertise in international collaborations.

[5] https://www.ibm.com/uk-en/
[6] https://www.cisco.com
[7] https://www.ge.com/uk/
[8] https://www.idf.il/en/
[9] https://en.wikipedia.org/wiki/Unit_8200
[10] http://in.bgu.ac.il/en/Pages/atp.aspx
[11] UK National Cybersecurity Strategy 2016-2021, November 2016

Cybersecurity Landscape in Israel

Israel is a major force in cybersecurity innovation and development internationally, and Israeli cybersecurity companies are at the forefront of technology, rubbing shoulders with global industry giants. In fact, according to CyberDB[12] data-bank, Israel has the second largest amount of cybersecurity companies in the world, second only to the US. In terms of actual sales, Israel cybersecurity exports account for anything between 10-15% of the global cybersecurity market, an amazing figure given Israel's miniscule size and small population[13] .

Israel's leadership in this field stems from a myriad of things, including its geopolitical situation, tech-savvy workforce and start-up culture. Israel has been fighting foreign armies and domestic terror throughout its existence and has for a very long time invested resources in bolstering its intelligence capabilities.

1.1 Policy, Regulation and Funding

1.1.1 Funding

At the core of Israeli innovation policy is the Israel Innovation Authority (IIA)[14] matching grants programme. Through this initiative, firms submit R&D proposals, and grants are awarded on a competitive basis, with between 60% and 90% of the research costs covered. Proposals are reviewed according to their technical and commercial feasibility, risks and the potential for projects to generate expertise. These grants are actually high-risk loans – commercially-successful projects must pay back the IIA funding received by paying up to 3% of its annual turnover. The IIA estimates that its investment returns an economic benefit at a ratio of US$1 to between US$5 and US$10.

Another government programme set up in the early 1990s, Yozma[15] , has been credited with creating Israel's vibrant venture capital industry. Founded with a budget of US$100 million in 1993, Yozma established 10 venture capital funds, contributing up to 40% towards the total capital investment. The rest was provided by foreign investors, who were attracted by risk guarantees. In 1997 the government received its original investment with 50% interest and the funds were privatised[16].

The IIA advises the government and Parliament ("Knesset") committees regarding innovation policy in Israel and furthermore monitors and analyses the dynamic changes taking place throughout the innovation environments in Israel and abroad. The IIA creates cooperation with counterpart agencies, internally and overseas, to promote technological innovation in the Israeli industry and economy.

Innovation is by far the most valuable resource for the State of Israel, serving as a national asset crucial to economic prosperity. Strengthening the innovation ecosystem is the mission of the IIA, which seeks to further develop and support technological innovation in Israel through various support tools.

The objectives and functions of the IIA are:

- Responsibility for developing the innovation infrastructure in Israel: Developing the high-tech industry, while utilising and expanding the existing technological and scientific infrastructure and human resources in Israel.
- Maintaining Israel's international status as the "Start-up Nation": Creating jobs in the industry and incorporating scientific and technological personnel, as well as creating returns for the economy and encouraging growth.
- Distribution of grants and financial support for innovative-technological R&D: Increasing productivity and promoting technological innovation across all of Israel's industrial sectors, as well as improving Israel's economic status through production and export of R&D-intensive high-tech products.
- Connecting the Israeli economy with the global innovation industry: Initiating and establishing international agreements with countries and multinational corporations to advance the goals of the R&D law relating to international cooperation in R&D and innovation.
- Promoting and encouraging programmes, policies, laws and government reforms, as well as major moves with public and private collaboration[17] .

There is a network of 20 incubators across the country, with 85% and 15% of investments from the IIA and private investors, respectively. In return, the incubators tend to receives 50% equity in the start-ups (mainly medical and pharma companies).

Figure 2 Funding structure of the Israel Innovation Authority Incubator Programme

1.1.2 The Cybersecurity Capital

Be'er Sheva was founded in 1969 as part of a plan to make optimal use of the Negev desert area in Israel – and the city has been designated the capital of the Negev. Be'er-Sheva and the Negev cover almost two-thirds of the country's land area, and are considered the most significant source of available land reserves.

The Israeli Government initiative to utilise this land better changed national priorities and saw the IDF's elite units relocated to the Be'er Sheva along with the establishment of the national cyber complex – CyberSpark[18] - in Be'er-Sheva, placing the city in the heart of the Israeli high-tech industry.

The Israeli Defence Force (and Unit 8200) moving to Be'er Sheva is coupled with a law in place which states that Be'er Sheva is the Cyber Capital. It is unheard of for a government putting into law that a certain location will be a technology hub. It is a clear move by the government of Israel that they don't want any question or double-guessing from investors and global corporates that they should open an office in Be'er Sheva. This is legislated – "You must because law says that is the location the tech will be in". This approach reinforces the government policy to maximise the potential of the land reserve in the desert region.

A policy motivator from the Israeli Government to bring cyber companies to Be'er Sheva is that for every employee in the cyber sector, the government will subsidise 20% of that employee's salary. This reflects the government's commitment to maintaining Be'er Sheva as the Cyber Capital[19]. All the key stakeholders are located within walking distance as indicated in the aerial photo below.

1.1.3 Military Intellectual Property

The Israeli Government's policy to not keep its military intellectual property in the IDF and allow it to be commercialised for civilian use has proved to be very fruitful. Israeli policy has been to develop its core capabilities as opposed to importing the capabilities.

1.1.4 The Cybersecurity Professions

On 31 December 2015, the National Cyber Bureau (NCB)[20] under the Israeli Prime Minister's office published a policy document on the regulation of cybersecurity professions in Israel. The NCB advises the Prime Minister and the government on cybersecurity policy and implementation. [21]

Figure 3 The Be'er Sheva Campus

[12] https://www.cyberdb.co
[13] Cybersecurity landscape and investments Israel, 2016 (CyberDB Research Dept, Jan 2017)
[14] http://www.matimop.org.il
[15] www.yozma.com
[16] Israel innovation policy platform, 2016
[17] Israel innovation policy platform, 2016
[18] http://cyberspark.org.il/
[19] Be'er-Sheva, the Opportunity Capital of Israel, 2016
[20] http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx
[21] Policy of Regulating Cybersecurity Professions in the State of Israel (Policy Document) (Dec. 31, 2015)

The policy explains that the regulation of cybersecurity professions is needed to protect Israeli organisations from cyber threats and attacks. Regulated professions include that of a Cybersecurity Practitioner, a profession that requires basic theoretical and hands-on knowledge of the implementation of certain aspects of cybersecurity in an organisation.

Professions that require additional professional knowledge within one's area of responsibility are: Cyber Penetration Testing Specialist, Cyber Forensics Specialist, Cybersecurity Methodology Specialist, and Cybersecurity Technology Specialist. The last two professions generally require an academic degree in specified areas related to computer science and engineering. The policy describes the responsibilities and qualifications needed for each of these professions.

To obtain certification authorising work in one of the above professions, an applicant will have to prove compliance with the professional and educational requirements, has attained the age of majority (18 years of age) and not had a criminal record. In addition, the applicant will need to have successfully passed theoretical as well as practical tests to prove relevant professional knowledge and ability. Professionals will be further required to successfully pass professional eligibility testing once every three years, to ensure their knowledge of "main changes and tendencies" in their respective profession.

A new unit has been established within the NCB that oversees the cyber defence services market. Among other responsibilities, the unit is authorised to approve the list of regulated professions at least once every three years. The unit also evaluates the professional knowledge required under the different professions on an annual basis, to ensure that these requirements are current and relevant. The unit can also authorise grant professional certification.

In the UK, the National Cybersecurity Centre (NCSC) runs the Certified Cyber Professional scheme (CCP)[22]. It has been developed in consultation with government, industry and academia to address the growing need for specialists in the cybersecurity profession. The CCP scheme sets the standard for UK Cybersecurity professionals and is at the heart of our efforts to build a community of recognised professionals.

People can gain certification for any one of the following skills-based roles:

- Information Assurance Accreditor
- Security and Information Risk Advisor (SIRA)
- Information Assurance Architect
- Information Assurance Auditor
- IT Security Officer
- Communications Security Officer.

There are three competency levels against which an applicant can be assessed:

- Practitioner – Entry level to CCP and suitable for individuals who work on routine Information Assurance (IA) tasks under supervision.
- Senior Practitioner – Suitable for individuals who work independently on complex projects and who normally lead a team of IA professionals or lead or oversee the work of other IA professionals.
- Lead Practitioner – Suitable for highly experienced individuals working at senior levels in an organisation, who provide advice and/or leadership on complex strategic IA issues.

The international body ISACA[23] provides internationally-recognised qualifications for cybersecurity professionals and CREST[24] provides widely recognised certifications for penetration testers.

Both Israel and the UK recognise the need to get skilled cybersecurity professionals, and both schemes have synergies in so far as their objectives are closely matched.

1.1.5 Cyber and Financial Services

The Cyber and Finance Continuity Centre (part of the Israeli national CERT[25] - FC3[26]) is a guidance unit for the financial supply chain. Breaches tend to start from the supply chain, and the units work with these suppliers to run surveys to identify cyber priorities and critical risks. The suppliers work on this voluntarily, and the survey results are only shared with the supplier.

The Ministry of Finance and National Cyber Directorate[27] in Israel have recognised the need to collaborate to ensure business continuity. There is a concerted effort to map critical processes to systems, tools and roles – to identify vulnerabilities and then focus on them. The biggest value to the whole supply chain is information sharing.

The CERT is independent with no influence or involvement by the regulator. The main areas of focus for the CERT are: cyber financial resilience, information sharing, situation estimation and incident handling.

[22] https://www.ncsc.gov.uk/scheme/certified-professional
[23] https://www.isaca.org/
[24] http://www.crest-approved.org/
[25] CERT - Computer Emergency Response Team
[26] https://il-cert.org.il/
[27] https://www.gov.il/en/Departments/israel_national_cyber_directorate

1.2 The Cybersecurity Ecosystem

	Ranking		Performance	Funding	Market Reach	Talent	Startup Experience	Growth Index
Silicon Valley	1	0	1	1	1	2	1	4.2
New York City	2	0	3	2	3	7	4	4.5
London	3	▲ 3	4	4	2	10	5	4.8
Beijing	4	NEW	2	5	19	8	2	4.4
Boston	5	▼ -1	6	6	12	4	3	4.0
Tel Aviv	6	▼ -1	9	8	4	11	7	4.5
Berlin	7	▲ 2	7	9	6	5	10	4.6
Shanghai	8	NEW	8	3	10	9	13	5.5
Los Angeles	9	▼ -6	5	7	15	14	11	4.2
Seattle	10	▼ -2	12	13	14	3	6	4.5
Paris	11	0	14	14	9	16	8	4.2
Singapore	12	▼ -2	16	16	11	1	20	4.6
Austin	13	0	15	11	18	6	9	4.3
Stockholm	14	NEW	17	20	8	18	12	5.3
Vancouver	15	▲ 3	19	19	7	15	15	4.3
Toronto	16	▲ 1	18	12	5	20	18	4.7
Sydney	17	▼ -1	20	10	13	12	17	6.3
Chicago	18	▼ -11	13	15	20	13	14	3.9
Amsterdam	19	0	10	17	17	19	16	4.8
Bangalore	20	▼ -5	11	18	16	17	19	4.7

Figure 4 Global ranking of global start-up ecosystems

Tel Aviv has the sixth best start-up ecosystem in the world, as indicated in Figure 4 above, which for a 70-year-old country of Israel's size is quite an achievement and it makes it competitive with the likes of Silicon Valley, New York, London, Boston and Beijing.

1.2.1 Unit 8200

Unit 8200 is the largest unit in the Israel Defense Forces (IDF), comprising several thousand soldiers. It is comparable in its function to the United States' National Security Agency (NSA)[28] and is an Israel Ministry of Defense body just as the NSA is part of the United States Department of Defense.

Subordinate to Unit 8200 is Unit Hatzav, responsible for collecting intelligence. The unit monitors and collects military intelligence-related information from television, radio, newspapers, and the internet. The translation of various items accounts for part of what is termed "basic intelligence", which is collected by the units. According to media reports, the unit provides over half of the overall intelligence information for the Israeli intelligence community.

Unit 8200's remit covers cybersecurity, cyber offence, encryption and intelligence (web intelligence, threat intelligence, communication intelligence and signals intelligence) and is responsible for producing highly-skilled cyber experts from those who have spent three years in the Israeli army. Most of Israel's new cyber start-up businesses have founders and management team members who have served in Unit 8200.

The IDF is unique - in the sense that young recruits spend two-to-three very intense years in training, developing and operating the worlds' most sophisticated systems. Recruits are taught how to hack and defend, develop tools and systems and gain operational experience, equivalent to many years of civilian training and operation.

1.2.2 Israel Cyber Industry – Main Categories of Focus

Israeli cyber start-ups cover almost all cyber categories, but there is a certain bias towards the following major competencies:

- **Threat intelligence systems**, services as well as automatic tools for monitoring the web and dark web. Offering real-time threat feeds and periodic reports for forensics and integration security system.
- **Cloud security**, mainly around the CASB category.
- **Automotive security** and connected car security.
- **EUBA**; Entity and User Behaviour Analysis, heuristic

[28] https://www.nsa.gov

analysis and data mining for detecting APT at networks and endpoints.

- **ICS/SCADA security,** Operations Technology (OT)/ industrial automation security, including OT network monitoring and visibility and alerting based on behaviour analysis.
- **Incident response** and investigation automation based on integrations with other enterprise IT solutions and data mining capabilities.
- **Mobile security**, for highly-secured mobile devices. Including voice and data encryption, protection against hijacking by malicious networks and prevention of APT and malicious agents protection.
- **Deception technologies, honeypots, honeynets**; Israeli cyber vendors are leading this emerging technology.

The last three years has also seen the emergence of companies focused around providing data protection and data privacy in line with the new EU GDPR (General Data Protection Regulation) and the growing threat from the Internet of Things.

An increasing number of Israeli cybersecurity companies with an international presence now cover the solution landscape in the above categories. Examples include:

- Illusive Networks (a Team8 company) based in Tel Aviv, Israel, London, UK and the US[29]
- CyberBit based in Tel Aviv, Israel, London, UK and the US[30]
- Guardicore based in Tel Aviv, Israel and the US[31]
- Reblaze based in Tel Aviv, Israel and the US[32]
- Cy-OT based in Tel Aviv, Israel and the US[33]
- BigID based in Tel Aviv, Israel, and the US[34]
- Intezer based in Tel Aviv, Israel, and the US.[35]

1.2.3 Israel's National Fintech-Cyber Innovation Lab

The future Israel National Fintech-Cyber Innovation Lab[38] is a new initiative led by Israel's Ministry of Finance with involvement from the IIA and the Prime Minister's Office National Cyber Directorate. It is due to be launched in the coming months, once all plans are ratified by the government.

The proposal is to build an open innovation lab led by the private sector: financial institutions and technology companies with expertise in cyber and fintech. This will bring about a stronger financial ecosystem through the collaboration of all the stakeholders: innovators, financial institutions, technology companies, government and regulators.

The Innovation Lab will have cohorts of fintech and cybersecurity start-ups on six-monthly cycles chosen by the consortium leading the running of the lab. If the start-up is to qualify for a grant from the Israel Innovation Authority they must be approved by the Innovation Lab as well.

The consortia leading the lab will get US$1 million and US$130K per year for a three-year franchise. The start-ups each get up to a US$110K over six months. The qualifying criteria for the start-ups include the requirement to have a Minimum Viable Product (MVP) or beta of their technology/ product in Israel.

The unique point of the Innovation Lab, shown in Figure 5, is that it has government support and embracement, it is connected to the CERT, it can leverage government connections to banks, other governments and regulators and they get a fast track to the regulatory sandbox.

The proposed regulatory sandbox is likely to be modelled on the UK FCA (Financial Conduct Authority) Sandbox for fintech established in the UK. The FCA Sandbox[39] provides a space for fintech to test out their products without the worry of any penalties as a result of any regulatory breaches that might occur. UK financial institutions participate and provide data to the sandbox as it mitigates a large degree of risk that they would otherwise carry in the event of a regulatory breach during a technology trial. The Ministry of Finance in Israel has had some direct dialogue with the FCA to learn from them so that they can build a similar facility in Israel that will be directly linked to the lab.

Figure 5 Proposed operating model for the upcoming Israel Fintech-Cyber Innovation Lab

[29] https://www.illusivenetworks.com/
[30] https://www.cyberbit.com/
[31] https://www.guardicore.com/
[32] https://www.reblaze.com/
[33] https://www.cy-ot.com/
[34] https://bigid.com/
[35] https://www.intezer.com/
[36] http://mof.gov.il/en/About/Units/CyberEmergenciesSafetyDraft/Pages/Cyber-Fintech.aspx

1.2.4 Education

Along with degree programmes in cybersecurity, Israel also teaches cybersecurity skills to high school children. The programme is overseen by Israel's defence establishment and co-sponsored by the Rashi Foundation[38], a philanthropic group. It is part of Israel's efforts to invest in its youth as a way to build up the country's cybersecurity prowess. Approximately 50% of high school children will, as a result, end up in Unit 8200 after they graduate. Alongside this, the Magshimim[39] after-school programme — for gifted high schoolers from underprivileged parts of the country — teaches computer programming, coding, encryption and how to defend a computer network against hacking.

Countries around the world are scrambling to teach children cyber skills. The NSA sponsors free summer camps to teach coding and cyber skills to elementary and high school students in the US, while the UK recently announced a new curriculum to teach cyber skills to children aged 11 to 18 through the NCSC Cyber First programme[40].

What is different in Israel is that the majority of high school graduates are called up to the military, offering Israel a large talent pool to join official efforts. The cyber skills the youth gain in the army will help them land a job one day in Israel's powerful cybersecurity industry. Israel is particularly focused on recruiting more girls to join programmes such as Magshimim.

Israel recently announced a new national, cyber education centre to train educators, develop more programmes, and oversee the learning programmes that already exist. Some fourth-grade classrooms in Israel are teaching computer programming, and there are even two new kindergartens focused on computers and robotics. Companies like CyberBit provide some of the technology and infrastructure to support these programmes.

1.2.5 CyberSpark

CyberSpark[41] is the Israeli cybersecurity innovation arena in Be'er-Sheva. It is a joint venture between the Israeli National Cyber Bureau[42] in the Prime Minister's Office, Be'er Sheva Municipality, Ben Gurion University of the Negev and leading companies in the cybersecurity industry.

CyberSpark is part of the Global EPIC (Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity)[43] programme, whose purpose is to co-create and adopt world-changing solutions to high-impact cybersecurity challenges, both current and emergent. It was founded in 2017, with an inaugural meeting in October 2017 and aims to have 50 ecosystem members by 2020. The UK participates in Global EPIC through Queen's University Belfast, one of the three co-founding organisations.

CyberSpark is a non-profit organisation, designed to be the central coordinating body for joint cyber industry activities with all stakeholders. It aims to leverage the region (Be'er Sheva) and maximise its potential as a global cybersecurity centre, to encourage joint academia-industry partnerships and to support the plans to draw other companies, whether international or Israeli, to base their projects or themselves in the region.

CyberSpark incorporates a number of facilities:

- Research Centre – In collaboration with Ben-Gurion University of the Negev researchers.
- R&D Hub – Supported by the government (tax incentives), which allows companies to have access to potential bids and engage in joint research with BGU.
- Training Centre – Cyber training services led by industry and government.
- Innovation Hub – Exposure to Israel's advanced technologies.
- Incubator – Supported by the Israel Innovation Authority.
- Intelligence Centre – SMEs from CERT and the industry provide intelligence information relating to the most imminent cyber threats to businesses.

CyberSpark, as indicated below, is a coming together of all the stakeholders to bring about critical mass with a view to maximising the impact and potential[44]. This shows the global interest and involvement in the overall ecosystem in the area.

Industry and research personnel also teach at the university. That way they can directly influence the curriculum, and therefore graduates leave university better-equipped with real-world practical skills for cyber technology when they enter the world of work.

CyberSpark also provides a model by which overseas corporations can initially set up in the region and minimise

[37] https://www.fca.org.uk/firms/regulatory-sandbox/global-sandbox
[38] https://www.rashi.org.il/
[39] https://www.rashi.org.il/magshimim-cyber-program
[40] https://www.cyberfirst.ncsc.gov.uk
[41] http://cyberspark.org.il
[42] http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Pages/default.aspx
[43] https://www.globalepic.org/ece/index.php
[44] CyberSpark Presentation, November 2015

the risks that come with moving to a new geographical jurisdiction. The scheme called "Landing Pad"[45] enables global companies to smoothly transition into the Israeli cyber innovation area by outlining a gradual, bespoke, zero-risk entry path that best complies with the companies' strategies. CyberSpark provides the service environment, so they get the specifics including infrastructure, personnel and support that they require at zero risk.

1.2.6 IL-CERT

IL-CERT (Israel's Computer Emergency Response Team)[46] is Israel's civilian centre for addressing information security and cyber events. IL-CERT is an unaffiliated and professional organisation that provides an address for people and organisations in Israel and worldwide to report incidents concerning the cyber threats and events in Israel. IL-CERT is responsible for coordinating activities in addressing security events, pro-actively before they occur and information sharing and public awareness on issues of information security and privacy.

The CERT focuses on an important part of the overall cyber-ecosystem and it is located in Be'er Sheva in the heart of the cyber capital. The important sectors that the CERT focuses on are:

- Critical infrastructure
- Financial services
- Government affiliates
- Ministry offices
- SMEs
- The general public.

The CERTs work is focused around efforts on policy, national guidance, research and development, capacity building and national resilience. They track threats and provide incident response teams – "boots on the ground". This capability is unique and isn't found in the UK or elsewhere in Europe. The CERT provides a 24/7 Incident Management Centre, proactive threat intelligence and global cooperation.

International cooperation is generally in the form of threat and information sharing and a small number of international exercises. IL-CERT is also a member of FS-ISAC[47] which is an information sharing forum run by eight of the big US banks, and all of the main global financial institutions are involved.

There are three sector CERTs; FC3 for the financial sector, G-SOC for government and a further unit for the energy sector. They provide:

- Investigation and response to information security events that affect their constituency and provide quality assessments and recommendations to the public.
- Coordination in the handling of security events when they occur while remaining non-affiliated and professional, between various entities in Israel and abroad.
- Public relations and awareness. Publishing threat information and defence tools.

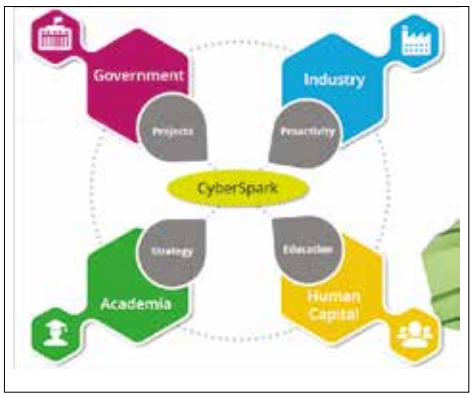

Figure 6 CyberSpark's integrated collaboration model

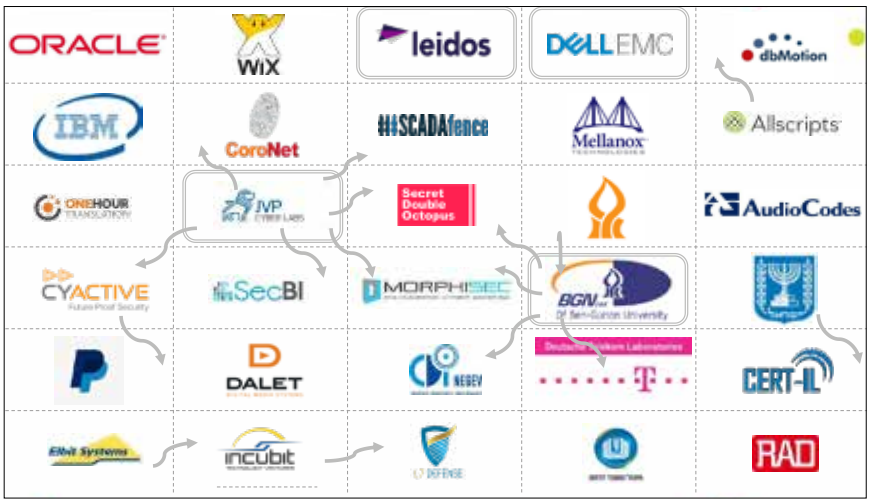

Figure 7 CyberSpark founders and partners (2016)

[45] http://cyberspark.org.il/landing-pad/
[46] https://il-cert.org.il/
[47] https://www.fsisac.com/

1.3 Israel Cybersecurity Market and Investment

Israel's start-up scene is second only to Silicon Valley and is currently estimated to host over 5,000 start-ups. In fact, Israel has more tech start-ups and venture-capital funding per head of population than anywhere in the world – even the United States.

Country	2015 Investment ($B)	2015 Population (mil.)	$pC
Israel	**2.6**	**8.4**	**310**
US	72.3	321.6	231
Canada	1.5	35.8	42
China	49.2	1,374.6	36
Europe	14.4	602	24
India	8.0	1,293	6
Japan	0.8	126	6

Figure 8 Ranking of private investment in Israel (per capita) in 2015.

The venture capital industry is very knowledgeable, and many of its leaders are Unit 8200 veterans, so any young founder can pitch to any VC in town (and many foreign ones which have lately also set up shop in Israel) and get initial funding.

The cybersecurity sector is still growing, and over 100 solutions from Israel now cover the enterprise security stack. Overall investor interest is still growing. In 2017, Israel attracted between 25% and 50% of global private investment in cybersecurity, a level of investment second only to the United States.

Figure 8 and Figure 9 show how Israel attracts per capita more private investment than any other country in the world and more in absolute terms than any country in Europe.

Start-ups are assisted in getting proofs-of-concept through a government innovative finance instrument. There are four main dedicated VC funds in Israel:

- **Glilot Capital**[48]
  Glilot Capital headed by Arik Kleinstein and Kobi Samboursky, is dedicated to investing in cyber start-ups, from the seed stage. Glilot is ranked as one of the best performing funds in the world.
- **JVP (Jerusalem Venture Partners)**[49]
  JVP Cyber Labs Fund[50] is one of the JVP funds specialising in investing in cyber start-ups from the seed stage. It is based in Be'er Sheva and Jerusalem and led by the JVP partners Yoav Tzruya and Dr Nimrod Kozlovsky.
- **Team8**[51]
  Team8 is led by Nadav Zafrir, ex-Commander of the IDF's Technology & Intelligence Unit 8200 and founder of the IDF Cyber Command. Based in Tel- Aviv, this is a unique VC/ start-up creator that managed to raise US$50 million in initial funding. Today they are an incubator that builds and holds companies until they find a suitable "founder". Illusive Networks30 which has reached 85 employees with over US$30 million of investment to date is one example of the fund's success.

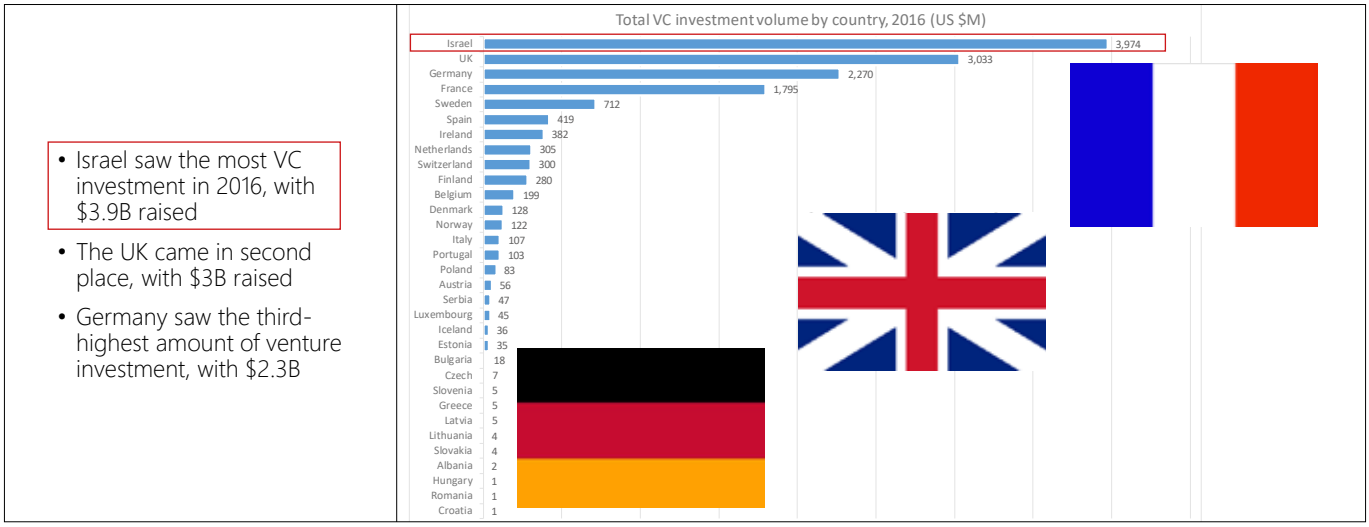

Figure 9 Total venture capital investment by country in 2016

[48] http://glilotcapital.com/
[49] https://www.jvpvc.com/
[50] http://www.jvpvc.com/cyberlabs
[51] https://www.team8.vc/

- **OurCrowd**[52]
  OurCrowd is a crowdsourcing venture capital model. It is one of the largest VC investors in Israel and aims to democratise access to VC fund investment. There is no minimum investment level in the fund, and OurCrowd normally crowdsources funds from over 100 countries from accredited investors. Typical investments range from US$2 million to US$20 million in series A to C.

The graph in Figure 10 below represents the trend of private investments in Israel's cybersecurity companies

1.3.1 Government Incubators

The government incubators that were part of the directed government policies have been privatised. The first group of VC funds was seeded by a government fund – to get things off the ground. The result is that there are a reasonable number of funds worth US$50 million to US$300 million, with increasingly more international funds focusing on the later stage rounds of investment.

1.3.2 Israeli University VC Funds

Tel Aviv University has announced plans to set up an early-stage start-up venture fund, the first of its kind by an Israeli university. The TAU Ventures fund, which will be located in Tel Aviv, has already raised some $20 million in commitments from investors including the Singaporean investment fund Chartered HighTech (CTH)[53] and additional investors from the US and Canada. It will operate for seven years, investing in start-ups set up mainly by homegrown university graduates or students.

The investment fund is modelled on ones established at a number of universities in the US, including the Massachusetts Institute of Technology (MIT)[54], University of California, Berkeley[55] and Stanford[56] University. In addition to investing money in the start-ups, the fund will be able to offer entrepreneurs the use of university resources including its labs, scientific knowledge and the network of contacts.

The new fund is defined as a micro-VC fund (funds that manage capital below US$50 million) and will join the Israeli venture capital funds operating in the local market. These Israeli funds have about US$3 billion in capital available for investments. In total, Israeli VC funds raised US$1.3 billion in 2017.

BG7 Ventures is an early stage VC fund from the technology transfer office of Ben Gurion University (BGN Technologies, see section 1.4.2). The fund will invest in high-tech, biotech and social ventures by students and graduates of the university. It will incorporate training to help interested students to develop skills in identifying and investing in promising technologies. Graduates will then have the opportunity to join the fund's investment committee, together with industry leaders and BGU's management, and become on-campus scouts for innovative technologies.

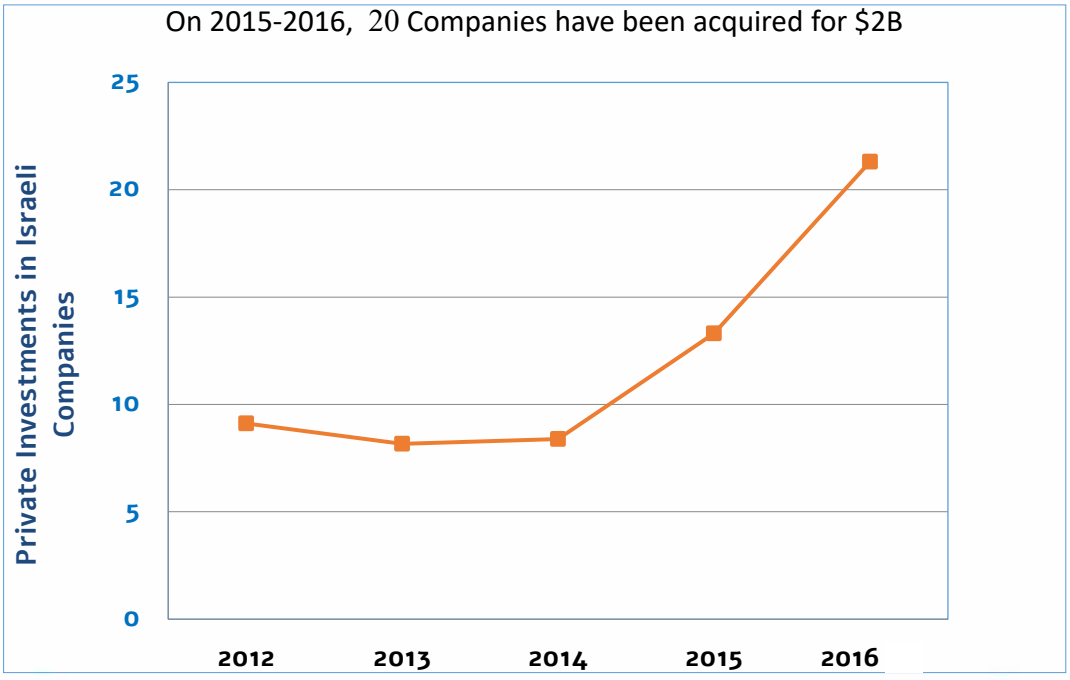

Figure 10 Trend of private investments in cybersecurity companies in Israel (2012-2016)

[52] https://www.ourcrowd.com/
[53] http://www.chartered.sg/chartered-high-tech/
[54] http://web.mit.edu
[55] https://www.berkeley.edu
[56] https://www.stanford.edu

1.4 Research, Innovation and Commercialisation

1.4.1 Academic Research

The National Cyber Strategy of 2011 advocated an increase in research and development. As a result, funds were given to universities to manage programmes as opposed to the government directly running them.

At Tel Aviv University, an Interdisciplinary Cyber Research Centre (ICRC)[57] has been created with funding from the national cyber directorate. The main focus of the centre is to look at problems in the context of a digital society.

In essence, the ICRC is operating a research fund from which 56 full research projects have been funded. Alongside these, ten exploratory projects were funded in 2014 from people not traditionally qualified, with support from a faculty member. One of these projects matured to a full research project in 2016.

The centre is looking to stimulate true interdisciplinary work – with social science and humanities and engineering, philosophy etc all bringing viewpoints to a problem. In Israel, universities still have a focus on fundamental research primarily driven by academic culture – through curiosity and scientific discovery without any specific end application.

The modes of co-operation for the universities seem to follow a very traditional approach i.e. get involved in joint research proposals and through direct formal agreements between universities. Formal agreements allow both universities to fund their own part of the work directly. There is a tendency to make the research objectives quite vague, giving the academics the latitude they desire. The main output from the research has to be publications.

Ben Gurion University (BGU)[58] has a much more direct relationship with industry with labs directly sponsored by big multinational companies.

Following compulsory military service, soldiers often go on to study at Israel's universities and technological institutions, which are amongst the best in the world. Upon graduation (and in many cases, during their studies) they will be recruited by one of Israel's established technology companies or multinationals (Google[59], Facebook[60] and Samsung[61] all have local R&D centres). By the time such a technologist reaches the age of 28, they have a decade of experience in multiple technologies, often with substantial managerial experience and business skills. Coincidently, this is the age many people decide to form their own companies or join their friends, colleagues and ex-service people in new start-ups.

Also, older, skilled immigrants hailing from the former Soviet Union participate in the technological workforce, adding unique skillsets and academic know-how in mathematics, encryption and computer science.

The Advanced Technology Park (ATP)[62] on the campus of Ben Gurion University (BGU) in Be'er Sheva creates a symbiotic relationship between three potent entities:

1. Academia

2. Technology companies

3. The Israeli Defense Forces.

Where the magic is expected to happen is in co-locating these three entities onto adjacent campuses where they can collaborate on projects, share data, and feed each other's needs for talent, resources, and thought leadership.

Some of the occupants include technology industry stalwarts Deutsche Telekom[63], EMC[64], RSA[65], and Oracle[66], as well as three incubators – Jerusalem Venture Partner's Cyber Labs[67], Elbit Systems' Incubit Ventures[68], and BGN Technologies (see section 1.4.2 below).

[57] https://icrc.tau.ac.il/
[58] http://in.bgu.ac.il/en/Pages/default.aspx
[59] https://www.google.com/about/our-company/
[60] https://newsroom.fb.com/company-info/
[61] http://samsung.com
[62] http://in.bgu.ac.il/en/Pages/atp.aspx
[63] https://www.telekom.com/en
[64] https://www.dellemc.com/en-gb/index.htm
[65] https://www.rsa.com
[66] https://www.oracle.com/uk/index.html
[67] www.jvpvc.com/cyberlabs
[68] http://incubitventures.com

1.4.2 Technology Transfer Offices

All the universities in Israel have technology transfer offices (TTOs) and whilst each has a specific remit based on expertise, capabilities and local ecosystem they have common objectives including:

- Bringing technological innovation to the market, which includes commercialising patents and technologies.
- Managing both intellectual property and business partnerships.
- Creating real industry-academia collaboration:
    - delivering collaborative applied research
    - working closely with multinationals
    - promoting rapid growth of the regional technology scene
    - catalysing entrepreneurship and start-ups
    - supporting the creation of a technological eco-system
    - launching technology accelerators, incubators and business hubs.

The best example of how this works in reality, is the technology transfer office of Ben Gurion University, BGN Technologies[69], a for-profit institution, aiming to create an ecosystem which consists predominantly of (again) the ex-military. A key part, is moving technology out of the army to their facility. They are in the middle of a very thriving and vibrant technology ecosystem in Be'er Sheva and are closely aligned with the university and industry in the area. This includes areas outside cybersecurity, such as biotech and cleantech. More than 100 companies have been launched via Ben Gurion University innovation and entrepreneurship.

BGN Technologies has signed agreements with more than 150 companies, including ExxonMobile[70], Johnson & Johnson[71], Siemens[72], and General Motors[73]. BGN Technologies has been so successful at this that universities from the US and Europe are studying their approach.

Figure 11 shows how BGN Technologies sits at the heart of a Ben Gurion University thriving ecosystem. BGN is also an equity holder in multiple innovation hubs and accelerators and as a result is a full partner in the local collaborative ecosystem.

The success has not been exclusive to BGN Technologies, other technology transfer offices across Israel have been equally successful in commercialisation, including T3 at Technion University[74], Yissum at Jerusalem University[75] and Yeda at the Weizmann Institute of Science[76].

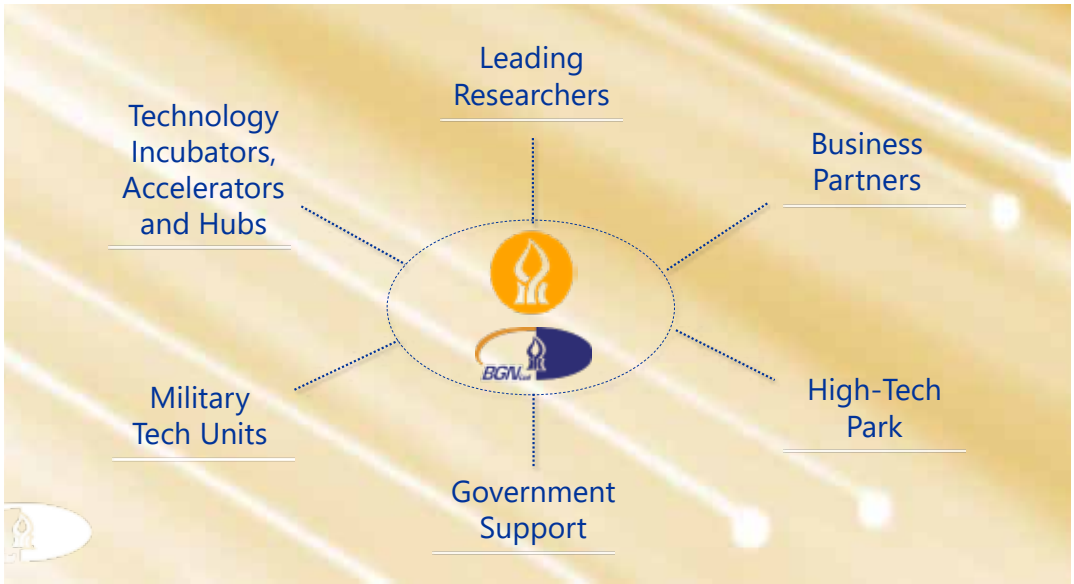

Figure 11 BGN collaborations in the local ecosystem

[69] http://in.bgu.ac.il/en/bgn/Pages/default.aspx
[70] http://corporate.exxonmobil.com/en
[71] https://www.jnj.com
[72] https://www.siemens.com/uk/en/home.html
[73] https://www.gm.com
[74] http://t3.trdf.co.il
[75] http://www.yissum.co.il
[76] http://www.yedarnd.com

Conclusion

1.5 History and Policy

Success in cybersecurity in Israel has originated and continued as a result of a number of long-term policy decisions and strategic investments, both public and private, made a long time ago. Although these policies and innovation programmes have benefited Israel's export-led growth in high-tech and specifically cybersecurity and offered a model for other OECD countries, their legacy is mixed today.

"The returns in terms of longer-term job creation and income growth have not kept up, despite continued investment in high-tech, many Israeli start-ups are sold to the US market and get absorbed into global firms, never really expanding in Israel. This is expected given the small size of the internal market, but it does raise questions about how much of the returns from innovation end up back in the economy in terms of jobs created.", according to the OECD[77].

One of the overriding messages is that the unique political situation of Israel shapes the mindset of its business and innovation eco-system. Specifically:

- Entrepreneurial mindset (conducive to acceptance of failure) with a very high accessibility to investment.
- Strong ongoing personal and professional network connectivity (often formed during military service).
- An open mindset from top to bottom leading to a willingness to share and cooperate openly in the country.
- The relatively small size of the country with strong patriotic closeness, enabling high social, political and commercial connectivity.
- A global-facing economy with strong desire to export, driven by aggressive ambition and lack of local and regional market.
- Specific technology education in the military and in specialised universities.

Due to the role of military service and Israel's geopolitical needs, government ministers clearly understand cybersecurity in a way that UK politicians don't. From the top, there is a total understanding of national and cyber security. The entire population understands what is going on.

The top 1% of children in the UK, go to the best universities such as Oxford and Cambridge and get good academic knowledge. The top 1% in Israel go into Unit 8200 and learn on the job. Children want to join Unit 8200 and are actively encouraged to by their parents. Going to Unit 8200 is seen as a sign of success.

1.6 The Israeli Cyber Ecosystem

Incubators have been set up as partnerships with companies (i.e. tendered out to). What is remarkable about these incubators is that they run for eight years; much longer than usual.

There is a relatively low level of indigenous venture capital investment. Most investment comes from the US and China. There is still a high amount of investment as a proportion of GDP, but almost 70% comes from the private sector, and the majority of that is foreign investment.

There is not a brain drain on a mass scale – the communities for high-tech and R&D are thriving, so the foreign funding that comes in does not seem to attract people, talent and IP overseas.

The innovation approach is not dissimilar to the United States and the challenge-based approach taken by DARPA[78] (US Department of Defense). The notion of public-private partnerships is widely applicable within cybersecurity in Israel. Team8[79] from its founding has successfully taken this approach; the origins of all the start-ups that have come out of Team8 stem from commercial challenges – they get together with stakeholders, find out what everyone is up to, identify the challenges and see what emerges in terms of ideas for solutions.

The new Fintech-Cyber Innovation Lab37 is very impressive because it has made the most of government connections to promote the credibility of the companies engaging with the three programmes of:

1. Cyber and Finance Continuity Centre

2. Guidance Unit for the Financial Supply Chain

3. The Fintech Innovation Lab.

[77] https://www.oecd-ilibrary.org/economics/oecd-observer/volume-2011/issue-2_observer-v2011-2-en
[78] https://www.darpa.mil
[79] https://www.team8.vc

What is remarkable about this programme of work is that the design is holistic across all of the various areas of fintech/cyber domain. Regulators are kept out of the more innovative areas of engagement to create a safe space for assurance and experimentation. In particular, the programme to encourage supply chain best practice and resilience was impressive. This takes the form of company surveys and guidance which is conducted away from regulation. However, the power of the ministry enables suppliers to become accredited for taking part in the scheme, which provides a powerful incentive to participating companies.

In some cases, there appears to be a lack of engagement in these programmes by universities with Ben Gurion University seeming to be the exception. They appear to target (international) business engagement, with very generous investment incentives (50% of equity in the national accelerator programmes). This creates challenges around the retention of IP.

The cybersecurity business and sales landscape in Israel focuses on exports and the global market – this is a natural direction for a country the size of Israel and its geopolitical environment. The investment landscape, in both private and public, for cybersecurity in Israel is currently very strong. However, the usual dynamic shifts in technology trends mean that investors' interest in cybersecurity could shift causing the bubble to burst.

The connectivity of the ecosystem in Israel is impressive. The fact that it is a small place where everyone knows everyone else means that people can get to whoever it is they need to with a degree of ease which makes progress rapid and easier. There is a hierarchy across government, customers, academia and start-ups. Formality and protocol do not appear to be important – if people want something they ask without fear of rejection.

The Israeli cybersecurity companies and ecosystems appear to target major organisations and multinationals customers with enterprise solutions. Very little focus is on the SME market, which still makes up the most significant number of organisations around the world. SMEs face increasing threats and regulatory burdens and therefore are becoming an increasingly large untapped market.

1.7 Synergies with the UK

The UK and Israel share a set of core principles in the sense that Israel tends to align itself to western values. This may be because it is a cosmopolitan country with a heavy western influence.

The Israel Innovation Authority is in many ways similar to Innovate UK, with a focus on funding businesses with innovative ideas through a number of funding programmes. The majority are matched funded as well, in the same way as the programmes are in the UK.

The UK also has a number of incubators and accelerators with a focus on cybersecurity. This is supported by a host of high-tech incubators across a range of technologies from artificial intelligence, the Internet of Things, through to digital health.

Cylon[80] was the first UK accelerator in 2014 and promotes itself as Europe's first dedicated cybersecurity accelerator founded as a not-for-profit entity by Epsilon Partners[81], Amadeus Capital[82] and Winton Capital[83]. It is on its eighth cohort and has a number of global sponsors. Since the advent of Cylon, the UK government, supported by the private sector, has invested in a number of incubators/accelerators including GCHQ's NCSC Accelerator, HutZero[84], the academic cyber start-up programme and the recently launched London Office for Rapid Cybersecurity Advancement (LORCA)[85].

The UK also has a number of cybersecurity centres of excellence, and they have close relationships with industry and participate in international collaborative research and development activities.

There is a start-up culture and a world-leading capability in high-tech in the UK – maybe not on quite the same scale in relative terms compared with Israel, nevertheless it does exist and has been very successful attracting significant private investment in 2017[86].

The UK cyber ecosystem whilst not as integrated as in Israel is still active and vibrant with involvement and engagement from all the stakeholders across government, industry and academia.

[80] https://cylonlab.com
[81] http://www.epsilonpartners.com/index.php/en/
[82] https://www.amadeuscapital.com
[83] https://www.winton.com
[84] https://www.hutzero.co.uk
[85] https://www.lorca.co.uk
[86] IPGlobal, 2018

Annex 1
List of UK Participants

Amaryllis Ventures
Assentian Partners
BT
Crossword Cyber security
Innovate UK
Inogensis
Knowledge Transfer Network (KTN)
MyDocSafe
National Cybersecurity Centre (NCSC)
Queen's University Belfast Centre for Secure Information Technologies (CSIT)
Science and Innovation Network, British Embassy Tel Aviv
UK-Israel Tech Hub, British Embassy Tel Aviv

Annex 1
List of Israel Participants

6D Cyber
Ben Guiron University
BGN Technologies
BigID
CDiNegev
Check Marx
Cyberbit
Cyberspark
Duality Technologies
Giolt Capital Partners
Guardicore
Israeli Innovation Authority (IIA)
IL-CERT
Illusive Networks
Intezer
Intsights
Ministry of Finance
OurCrowd
SAM (Seamless Network)
SINET
Taglit Birthright Innovation Centre
Team8
TechSee
Tel Aviv University
Unbound Technology
Vdoo


ktn