Civil Cybersecurity in Israel

Policy and Research Environment Review From one of the World's Leading Cyber Hubs

ICDK Outlook No. 05, October 2020

Ministry of Higher Education and Science Denmark

Published by Danish Agency for Higher Education and Science
Haraldsgade 53
2100 Copenhagen Ø
Telephone: 7231 7800
E-mail: ufs@ufm.dk
www.ufm.dk

Photo Photo from https://www.colourbox.com/image/cyber-background-image-20676833

Edited by **Ann-Christina Lange**
Innovation Attaché ICDK TLV
Emilie la Cour
Research Analyst ICDK TLV

Reviewed by **Charlotte Slente**
Ambassador of Denmark in Israel
Sune Kaur-Pedersen
Senior Adviser, Danish Ministry of Higher Education and Science
Nikolaj Herning Gitz-Johansen
Desk Officer, Danish Ministry of Higher Education and Science

Publication can be downloaded at icdk.um.dk and ufm.dk/publikationer.

ISBN (electronic publication): 978-87-93706-89-7

INNOVATION CENTRE DENMARK

Contents

Abstract

English abstract

Israel was faster than many other countries to understand the need to protect civilian infrastructure and cyber vulnerabilities. In Israel, cybersecurity is viewed as a foundational part of society's digital transformation and a key driver of economic growth and social development. This report highlights the framework conditions for the Israeli success, which can inspire other nations when developing national strategies, turning cyber into an innovation driver and securing the right talent. The first part of the report will outline the components and evolution of Israel's National Cyber Strategy and its organisation. The second part maps the various research and innovation initiatives currently underway in Israel, as well as their evolution. The third part highlights the mechanisms that has created Israel access to large numbers of high-quality talent, much of which is developed through elite military training units. Such training units feed the civil cyber sector with expert knowledge and high-tech talents. The final section analyses the methods used to identify generate and develop young talent within cybersecurity, which provides a solid foundation for the entire ecosystem. These three unique elements, the national strategy, the research and innovation ecosystem, and well-trained tech talents, have positioned Israel as a global leader in cybersecurity. As our world grows ever more digitalised, and thus, ever more vulnerable, Israel offers valuable lessons in how to build a more cyber-secure civilian world.

Dansk Resumé

Israel er et af de lande der har været på forkant med udviklingen inden for cybersikkerhed. Landet udviklede allerede i 2010 en national strategi for cybersikkerhed i den civile sfære. Israels styrkeposition hviler på tre ben: etablering af en national cyber strategy, et stærkt innovation- og forskningsøkosystem og adgang til kvalificeret og veltrænet talent. Denne rapport har følgende formål: 1) at opridse udviklingen og organiseringen af Israels nationale cybersikkerhedsstrategi, 2) bidrage med indsigt i de innovations- og forskningsprogrammer der har været afgørende for at etablere et økosystem inden for cybersikkerhed, og 3) opridse de typer af træningsprogrammer, der bidrager til landets talentmasse. Hensigten er at drage nytte af den israelske erfaring og synliggøre mulige samarbejdsrelationer til gavn for det danske innovations økosystem inden for cybersikkerhed.

1. Introduction

Israel is a small and young state geographically located on the Arabian Peninsula with a population of just under 9 million people. Israel was faster than many other countries to understand the need to protect civilian infrastructure and cyber vulnerabilities. In Israel, cybersecurity is viewed as a foundational part of society's digital transformation and a key driver of economic growth and social development.

In 2010 Prime Minister Netanyahu announced that Israel aimed to become one of the top five world-leading cyber nations. A National Cyber Directorate was established directly under the Prime Minister's Office as part of Israel's newly formulated national cyber strategy. The Israeli government has since invested massively in cyber, and now account for 7% of the global cybersecurity market (2nd largest after the US). 20% of global cybersecurity investments go to Israel. 47 MNCs have established their cyber-related R&D facilities in Israel (such as general Electric, IBM, Paypal) and more than 420 cyber startups exist in Israel. In less than a decade, Israel has indeed managed to become a world leading cyber nation.

The Israeli case - the implementation of a national cyber strategy and the efforts to accelerate the establishment of a civil cyber-security innovation ecosystem - gives insight into the challenges and potential benefits of turning cyber security into a driver for economic growth. One key issue of particular relevance for Danish-Israeli collaboration is the future of quantum technology. Although Denmark has a lead in quantum science, the invention of a new quantum supercomputer is certain to compromise all existing cybersecurity systems. This poses a threat to civilian infrastructure such as transportation systems, hospitals and water supply chains. The Israeli government has been quick to comprehend the nature and scale of such future threats and has accordingly established a special task force to deal with quantum security. In light of Denmark's existing expertise in quantum, the relatively quick development of a civilian cyber ecosystem in Israel is an interesting case of inspiration for Danish researchers, institutions and private companies interested in cybersecurity.

What we might learn from the Israeli case is that cybersecurity not only represents a new global challenge but also bears huge innovation potential, which points towards potential future Danish-Israeli collaboration.

The focus of this report is on the civilian cybersecurity sector in Israel. However, how does one define cybersecurity as opposed to cyber? According to Merriam-Webster, cybersecurity is 'measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack'[1]. Cyber, on the other hand, is anything 'relating to, or involving computers or computer

[1] https://www.merriam-webster.com/dictionary/cybersecurity

networks'[2]. While the focus of our analysis is cybersecurity, cybersecurity is a component of the broader cyber ecosystem, and therefore both terms will be used throughout.

This report analyses Israeli efforts to establish a strong civil cyber ecosystem, the methods employed by public and private sectors alike, and how talent is actively generated and supported. It is important to emphasise that this report focuses only on the case of Israel's civil cyber ecosystem and not the areas developed by the defence establishment. The report is structured in three parts explaining the key characteristics of the Israeli civil cyber eco-system:

First, government has been a vital driving force in establishing and developing a national civil cybersecurity strategy. Through varied tools such as regulation, coordination, and subsidies, the Israeli government has been central in developing the civilian cyber infrastructure at all levels and across all sectors. Therefore, the first part of the report will outline the components and evolution of Israel's National Cyber Strategy. Importantly, science, technology development and innovation have been an integrated part of the national cybersecurity strategy from the outset.

The second section will map the various research and innovation initiatives currently underway in Israel, as well as their evolution.

Third, Israel has access to a large amount of high-quality talent, which is developed through early educational programs and elite training units for defence. Such training units feed the civil cyber sector with expert knowledge and high-tech talents. This section analyses the methods used to identify, generate and develop young talent within cybersecurity, which provides a solid foundation for the entire ecosystem.

The fourth section sums up the various parts of the Israeli ecosystem and concludes with several recommendations for how to make use of the Israeli case in securing the future of the Danish innovation and research landscape.

This report is based on research conducted by Innovation Centre Denmark (ICDK) in Tel Aviv. This includes more than 40 interviews with key leaders in the Israeli cyber ecosystem, several site-visits to companies, research institutions and government agencies, an advisory report written by the Blavatnik Interdisciplinary Cyber Centre at Tel Aviv University and desk research reviewing relevant written material including government resolutions. The report is part of the ongoing activities in the field of civil cybersecurity conducted by ICDK Tel Aviv. One such project is funded by the Danish Industrial Foundation. A few conclusions from this work also appears in this report.

[2] https://www.merriam-webster.com/dictionary/cyber

2. National Cyber Strategy

Cybersecurity is an unpredictable and ever-evolving field and Israel's government has been adept at constructing a flexible yet robust civilian ecosystem, which can adapt to changing realities and threats. This adaptability is because the Israeli approach was to include academia and industry from the outset, in order to build a multifaceted and robust cyber infrastructure. To understand the organisational set-up, which supports the implementation of a national cyber strategy, this first section reviews the history behind its development.

The public discovery of Stuxnet in 2010 propelled cybersecurity to the top of policy agendas worldwide, and prompted Israel to acknowledge that their contemporaneous regulations (primarily focusing on security issues/attacks within or against the defence establishment) were insufficient to meet the scale and breadth of cyber threats. Thus, a new and broader approach was required that focused on protecting the country's civil cyber infrastructure. This realisation resulted in the National Cyber Initiative launched in 2010 with the following vision:

> *To preserve Israel's standing in the world as a centre for information technology development, to provide it with superpower capabilities in cyberspace, to ensure its financial and national resilience as a democratic, knowledge-based and open society.*

The strategy was formulated by academic experts, defence representatives, R&D directors and ministry representatives. The Blavatnik Interdisciplinary Cyber Research Centre at Tel Aviv University played a key role in performing a systematic review of the challenges and opportunities and recommending new policy.

The National Cyber Initiative set three key focus areas:

1. How to incentivise and develop cyber technology in Israel to ensure its position as a (top five) world leader by 2015?

2. Which infrastructures are required to develop cyber technology in Israel?

3. What arrangements are required to best deal with the risks and threats in cyberspace?

The National Cyber Initiative thus clearly dealt with more than narrowly defined national security. In fact, it articulated a broader goal of world-leading cyber

capabilities, realising that the most robust solution would be to create a civilian ecosystem capable of handling future cyber attacks, the characteristics of which are unpredictable. The initiative was cemented as the National Cybersecurity Strategy with Government Resolution No. 3611 'Advancing National Cyberspace Capabilities'[3] in 2011. To lead cyber efforts amongst public and private Israeli stakeholders and to coordinate policy instruments, the main recommendation was to establish a dedicated government agency, which would, after several different iterations, come to be known as the Israel National Cyber Directorate.

A total of 2.5 billion NIS (4,84 mia DKK) was invested by the Israel government in implementing the entire cyber security strategy.

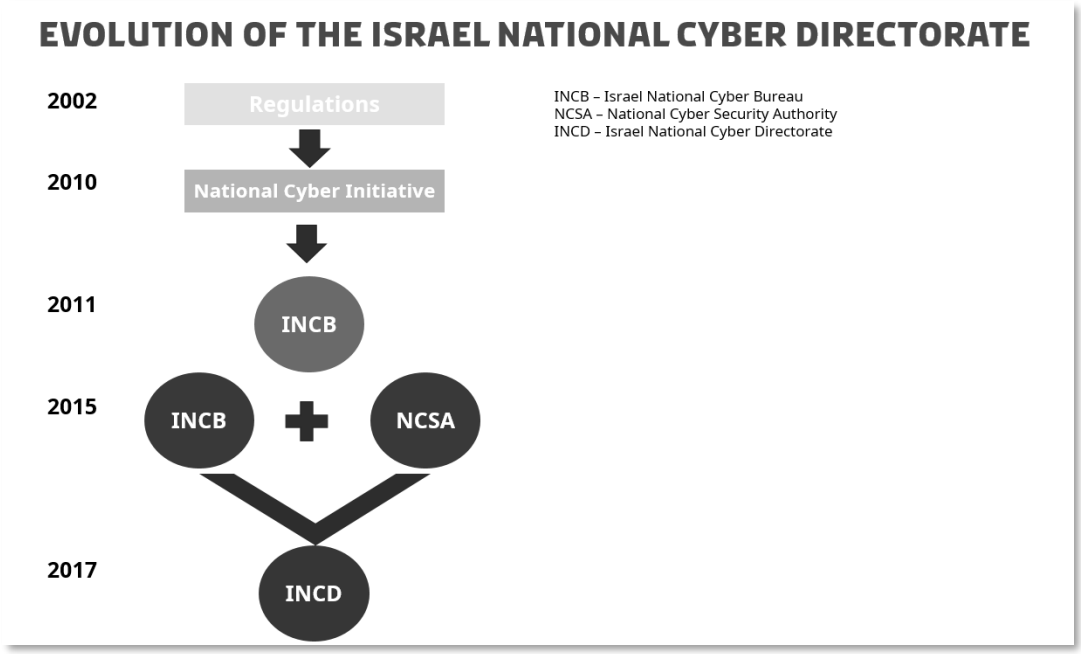
2.1 The Israel National Cyber Directorate (INCD)

To develop and implement the national cyber security strategy, the first action was to establish a National Cyber Bureau and a National Cyber Security Authority directly under the Prime Minister. The Bureau was set up to secure capability development, which means promoting research and development and boosting the export-oriented cyber industry. The Authority was defined as an advisory body to the Prime Minister which recommended national policy in the cyber field and promoted its implementation. In 2017 the two organisations were merged and now operate as the National Cyber Directorate (INCD), still under the Prime Ministers Office. The goals of the Directorate are to promote R&D in cyberspace and supercomputing; to facilitate the cyber industry in Israel; to formulate national education plans; to advance regulation and legislation; to develop tools for cyber emergencies; and to establish general infrastructure for cyber technology, amongst many other responsibilities.

Most countries continue to grapple with the desired role of the government in cybersecurity and placing the INCD in the office of the Prime Minister may not be an obvious choice. The decision stems from an assessment of bureaucratic limitations. The INCD encompasses a holistic strategy that includes public outreach, education, research, ICT technology development, economic, legal and ethical aspects as well as national security. Considering this multifaceted strategy, the INCD simply did not fit in any one department or ministry, and placing it within an existing entity would have risked paralysing the flexibility it needed to address its plethora of responsbilities and to balance overlapping and conflicting interests of numerous stakeholders. Therefore, the best choice was to place the INCD under the Prime Minister's Office, which in Israel is practically the sole office that can effectively resolve conflicts between different government stakeholders.

Figure 1: Evolution of the Israel National Cyber Directorate

[3] Government decision 3611: *Promoting national capacity in cyber space.* Jerusalem, Israel, PMO Secretariat.



Thus, within 8 years, two influential organisations were established, significantly developed independently, and then merged. Despite these many iterations of the cyber strategy, the underlying goal and method has been consistent: to protect Israel's civilian cyber spheres, with significant influence, or even intervention, from the government. Moreover, this dynamism suggests that the government is surprisingly willing to innovate and experiment with bureaucracy and new institutional constellations. Arguably, the national cybersecurity organisation will be re-arranged yet again in the future to meet new demands, realities and stakeholders.

It is this national organisation of cyber affairs which uniquely frames innovation, R&D and entrepreneurship in Israeli society. The way this has been done, and the characteristics of the Israeli cyber ecosystem will be explained in the following section.

3. The role of research and innovation in Israels cyber strategy

Israel's national cyber strategy focuses heavily on civilian research and innovation, which contributes to social development and economic growth. The Ministry of Defence carries out some research, but the majority is conducted by universities. Likewise, some innovation is housed in the defence establishment, but the government and private actors also fund large innovation programs focused on promoting civilian cyber technologies. Israel is truly unique in how it has supported the establishment of an independent civilian cyber ecosystem and the INCD has been a key player in building this Israeli 'innovation machine'. The next paragraphs will describe the innovation model in general terms and some of the projects and programs currently underway with the support of INCD.

3.1 A holistic innovation model

As a part of the national effort to develop cybersecurity, the Israeli government promotes research and innovation through various joint funding programs, which have contributed to positioning Israel as a leading country within cyber innovation. Such programs are built around the general Israeli innovation model, which focuses on open innovation, and where new startups are considered the ultimate way of adapting new technology to commercial use. Commercial partnerships with large companies, typically multinational companies (MNCs), are the end goal for Israeli startups and thus has significant influence on how the ecosystem is structured. In 2018, a total of more than $1 billion was invested in Israeli cyber startups. The natural outcome of this model is a high number of exits, where cyber startups are sold to large companies, and its technology and systems are integrated into the MNC. Israel also has a well-developed venture capital market. Once venture capital is added to startups or incubators, a disproportionately high number of cyber startups are bought by MNCs, or 'sold' through an IPO on NASDAQ, or similar technology stock exchange.

The case of Adallom is a good illustration of how the Israeli ecosystem functions: a small start-up, founded by former intelligence officers, was bought by a big multinational company.

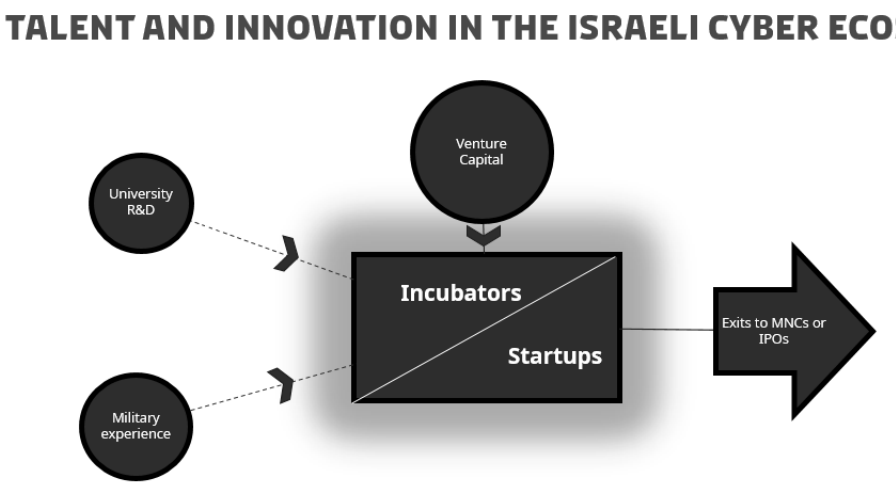
CASE 1: ADALLOM

Acquired by Microsoft for $320 million
Founders: 3 former IDF members

Adallom is a startup offering cloud security services. Adallom has developed security technology for remote servers, including those running Salesforce's, Microsoft's and Google's cloud services. Its software can monitor the use of cloud application by individual employees, and this includes looking for patterns and anomalies that could be security breaches.

The figure below illustrates how the various components in the Israeli cyber ecosystem interact.

Figure 2: The Israeli cyber eco-system



3.2 The INCD as promoter of innovative university research

Arguably, the INCD functions as an innovation agency because they exist to promote and develop the civilian cyber industry. According to the OECD[4] *'the success of the Israeli system is primarily attributable to vibrant business sector innovation and a strong entrepreneurial culture, the government has also played an instrumental role in financing innovation, especially in SMEs, and in providing well-functioning framework conditions for innovation, including venture capital (VC), incubators, strong science industry links, and quality university education.'* To have innovation, of course, research must come first. In Israel, more than half of basic research within cybersecurity is carried out on the civilian side. Therefore, universities play a very substantial role in civilian cyber R&D and the INCD works closely with universities to promote this. The establishment of an industry-focused cyber park in the south of Israel (Beer Sheva) is one example of how the INCD works with universities to support the innovation agenda. The cyberspark was established with public funds for a comprehensive incentive scheme for business to locate themselves in Beer Sheva, the National CERT is

[4] http://www.oecd.org/israel/41559762.pdf

strategically placed there and the government has supported the establishment of a cyber research center and education programmes at Ben Gurion University.

3.3 The CyberSpark Project

CyberSpark is the name of the Israeli Cyber Innovation Arena in Beer Sheva. It is a joint venture between 4 partners: the INCD, Beer Sheva Municipality, Ben Gurion University and leading cybersecurity companies. The INCD decided to move the core operational element of the CyberSpark project, the Israeli Cyber Innovation Arena, to the "remote" city of Beer Sheva, primarily to support the geographical clustering effort. The CyberSpark project aims to design a cluster of cybersecurity competence through an engineered ecosystem, consisting of a newly built office compound (*Gav-Yam*) that houses civilian (CERT-IL) and defence cybersecurity centres, Israeli startups, MNCs and co-working space. The Israel Defence Forces (IDF) is also planning to establish a presence there in the coming years. This compound is within walking distance of academia (BGU) and the railway station. The benefit of gathering industry and research at the same physical location is, theoretically at least, that innovation is easier and more likely[5]. The geographical proximity of these various stakeholders enables watercooler discussions to grow into actual solutions through partnerships across all sectors.

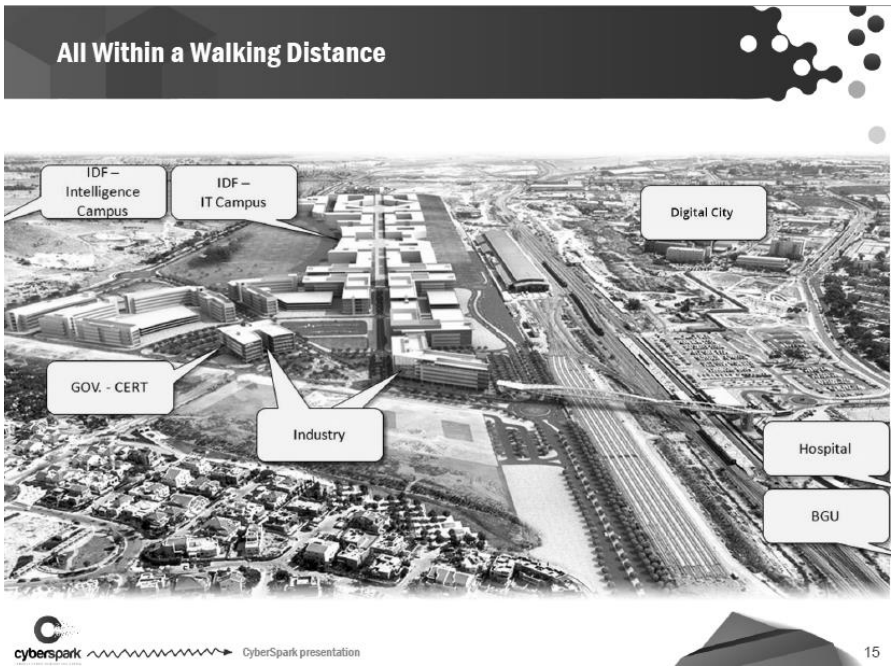


Figure 3: Aerial view of CyberSpark

The Gav-Yam Negev Advanced Technologies Park (ATP) now has three occupied buildings, planned to grow to eleven. The list of ATP tenants includes companies like Dell, Oracle, and many more. Ben Gurion University invited Deutsche Telekom to establish their cyber lab at campus. Deutsche Telekom (DT) began collaborating with BGU Software and Information Systems Engineering in 2004

[5] http://destinationinnovation.economist.com/wp-content/uploads/sites/3/2016/07/Destination-Innovation-Spatial_alchemy_why_proximity_matters_for_innovation.pdf

and expanded it with the launch of the Telekom Innovation Laboratories in 2006. The mission of Telekom Innovation Laboratories BGU is to investigate breakthrough technologies and technological advancements that provide a competitive advantage for DT, and to create business opportunities that enhance DT's current strategies. The collaboration centres on applied network engineering serve as an example of how public-private partnerhips can promote a regional cyber ecosystem.

3.4 INCD and University Cyber Research Centres

Another program supported by the INCD is offered to all research universities in Israel. Thus far six of Israel's seven research universities have established Cyber Research Centres supported by the INCD[6]. The INCD developed a model whereby it funds part of the research budget on the condition that the university matches it with additional funds. Still, the government refrains from commanding innovation processes: grant allocation is guided by the standard academic criteria of research excellence. In the first 5 years of the program, the INCD invested some $60 million in research funding. The INCD will continue this funding scheme for the next several years. As the universities enjoy a large degree of autonomy, the resulting Centres have developed in different ways, detailed below:

Ben Gurion University of the Negev (BGU)	In 2014 the **Cyber Security Research Centre (CSRC)** was inaugurated. Their mission is to foster groundbreaking and impactful cyber security research, whilst increasing user and organisational security and privacy; developing cyber defence tools; and identifying emerging threats, devising countermeasures and extending public awareness. The CSRC and Telekom Innovation Laboratories BGU[7] overlap to a large extent. Therefore, the thematic focus of the CSRC is on applied software and network engineering.
Hebrew University of Jerusalem (HUJI)	**The Federmann Cyber Security Centre** at the Hebrew University combines law and cybersecurity, working predominantly on legal aspects of cyber, especially internatinal human rights law.[8] Cybersecurity-related work is the minority in this organization.
Bar-Ilan University (BIU)	The **BIU Centre for Research in Applied Cryptography and Cyber Security** aims to promote and carry out academic research in the fields of applied cryptography and cybersecurity,

[6] The last research university, the Weizmann Institute, does not have an INCD-funded cyber research center, but it is home to several high-profile cyber experts nonetheless.

[7] https://cyber.bgu.ac.il/telekom/

[8] https://csrcl.huji.ac.il/current-research

	and to train graduate students to become the next generation of leaders in these fields. The centre also promotes collaboration with both industry and government.[9]
University of Haifa	The University of Haifa established the **Centre for Cyber, Law and Policy (CCLP)**. The CCLP predominantly addresses legal research and civil rights in the digital ecosystem, but aims to provide policymakers with an interdisciplinary 'toolkit' that addresses all aspects of cyberspace.[10]
Technion – Israel Institute of Technology	Technion University established the **Hiroshi Fujiwara Cyber Security Research Center** and focus on the technological side of cybersecurity. With over 65 faculty members, they aim to contribute to securing the digital world. Research areas include hardware, software, OS, network- and cloud-security, IoT, cryptology and more.[11]

3.5 INCD in Joint Funding Programs

The Israel Innovation Authority (IIA) is an independent publicly funded agency that supports the growth and development of Israel's innovation ecosystem by providing various tools to support industry R&D. In August 2018, they teamed up with The Israeli Ministry of Economy and Industry and the INCD to launch a new dedicated program to strengthen Israel's cyber industry at a scope of ILS 90 million over three years. The program consists of three parts:

1. investment in technologies with "gamechanger" potential on a global level;
2. funding support for companies moving from the development stage to the testing and demonstration stage;
3. and the allocation of resources to CyberSpark, which has already been discussed.

In addition, the INCD and the IIA will jointly promote the creation of innovation arenas in sectors undergoing significant digital transformations that expose them to cyber threats (e.g. health, transportation, finance, etc.). The innovation arenas will convene international industrial players, regulators, academics, and Israel's cyber industry to create solutions for tomorrow's cyber challenges and preserve Israel's global cyber leadership. The first two pillars of this joint funding program are elaborated on below:

[9] https://cyber.biu.ac.il

[10] http://cyber.haifa.ac.il/index.php/community/affiliated-faculty

[11] http://cyber.technion.ac.il/

3.5.1 Support for Game-changing R&D Programs in the Field of Cyber

This incentive program supports breakthrough research and development programs in cybersecurity. The goal is to promote significant growth of core technological capabilities that will enable innovative technological solutions and the development of groundbreaking products in the field of cybersecurity. Through their support of technological innovation, the program thus also encourages the creation and cultivation of sustainable civil cybersecurity companies. The program, called KIDMA, is intended for Israeli cyber technology companies that have developed products/services that are yet to be launched in Israel and still undergoing development. KIDMA offers companies a grant of 20%-50% of the approved R&D budget. An exceptional support rate of 66% of approved R&D expenditures is awarded to companies with significant potential to influence the global cyber market, or that constitute an outstanding technological breakthrough in its field.[12]

The first flagship program was KIDMA 1 that ran from 2013-2015 with a budget of 136 mill NIS. 91 out of 125 submitted requests for funding were approved. Due to the success of the program a second round, KIDMA 2.0, has been designed with a budget of over 100 mill NIS. The KIDMA 2.0 program offers three primary branches of support:

1) Groundbreaking & disruptive technologies to motivate the growth of larger companies in Israel. Supporting the development of groundbreaking solutions based on advanced technology and with significant potential to influence the cyber market on a global scale (disruptive technology).
2) Product creation and proof of concept. Helping companies bridge the gap between proving technological ability while supporting POC processes and creating a product beyond technological R&D.
3) Promoting industrial partnerships. To help create wide-scale cyber solutions for specific market problems while applying Israeli technologies to gain a competitive edge for Israeli industry on a global level.

12 http://www.pmo.gov.il/English/PrimeMinistersOffice/DivisionsAndAuthorities/cyber/Documents/Kidma%20Program.pdf

4. Where does the talent come from?

The previous section highlighted how Israel established a well-funded and well-integrated civilian cyber innovation ecosystem. However, the success of such a strong ecosystem depends on access to well-trained talents who can enter the civilian sector as innovators. The Israeli government has, through the INCD, spearheaded many civil cyber educational training efforts to build on this method of cultivating talent. Currently, the INCD is drafting a national strategy for cyber training and education in Israel, which is due to be published next year. Thus far, the INCD has supported a range of educational training programs with third parties (mainly universities and private cyber training companies). Subsidised funding for cyber courses has significantly contributed to the maturation and progression of the cyber ecosystem in Israel. As mentioned, 6 out of 7 universities have cyber research centres (partly funded by the INCD) and offer advanced training for academics and executives. This section outlines the mechanisms that created Israel's pool of cyber talent. In large part, the answer lies in the compulsory military service that all youths are subject to. But more important is the fact that the IDF has several elite training programs catered to cybersecurity recruits, and also funds civilian afterschool programs aimed at younger civilian students.

4.1 Which actors are involved in cyber education in Israel?

There are several noteworthy actors in the cyber education field in Israel. The military, the government and the Cyber Education Centre are the three most prominent institutions with a role in cyber educating the Israeli population. The unique combination of these three institutions and how they have learned to complement each other is of interest to anyone looking to understand how Israel produces the level and quantity of talent within cyber that it does.

4.1.1 Compulsory military service as an incubator for cyber talent

Although civilian cyber is detached from the military establishment in Israel, the IDF has historically had a unique role in talent generation that necessitates further explanation. The IDF has compulsory conscription of two years for females and three years for males. The IDF conducts educational and professional vocational training for recruits and soldiers not only to fill their own ranks, but also to supplement the role of schools. As mentioned, the IDF excels at training recruits in cybersecurity skills, which are later transferred to the civilian sector when the recruits enter the private sector. This is one way that positive spill-over effects of IDF service have developed a substantial ecosystem of human capital and knowledge transfer.

By way of example, the Israeli military intelligence Unit 8200 is the central collection unit of the intelligence corps. The unit admits young recruits with rapid

adaptation skills and who are quick learners. Moreover, the unit has well-established elite career tracks for advanced cyber training. Former Unit 8200 soldiers have, after completing their military service, gone on to found and occupy top positions in many private international IT companies, primarily in Israel and the US. In addition to the actual skills gained through training, a unique culture socialises the soldiers and officers to innovate within a general mission-oriented spirit. Soldiers are expected to accomplish their missions and to rise to the occasion despite limited resources, high risks and expectations – not unlike innovation in the civilian sector.

A specific case exemplifying the way the Israeli ecosystem functions is CyberArk, which is an Israeli company recently listed on Nasdaq and established by two former IDF members.

CASE 2: CYBERARK

Listed on NASDAQ

Founders: 2 former IDF members

CYBERARK

Founded in 1999, CyberArk introduced digital vault technology, which surrounds data with eight layers of security. They are the global leader in privileged access technologies, and more than 50% of Fortune 500 companies have used their services including PWC, Hershey's and Fannie Mae.

4.1.2 The Cyber Education Centre as a national coordinator

Many programs are now part of the Cyber Education Center (CEC), a non-governmental organisation responsible for coordinating and managing all aspects of cyber education at the national level. It was founded by the Rashi Foundation – one of Israel's largest and most influential philanthropies – and the Ministry of Defence. The Centre operates in conjunction with the security forces and high-tech sectors to stay current in this quickly evolving field, translating advancements and needs of both the industry, academia and the army's elite cyber units into educational curricula. The different training programs are developed in cooperation with the IDF, Ministry of Education, Ministry of Defence and the Rashi Foundation. CEC supports existing programs described below and works to advance new initiatives such as StarTech, a program for teenage boys and girls (7th-9th grade) without any prior knowledge of computer science. In developing such elite programs, the Centre draws on existing knowledge within Israeli universities through an advisory committee whose members include leading researchers in computer and cyber fields. They also involve science education professionals in evaluating the teaching methods and content.[13]

4.2 Examples of military elite training: Atuda & Talpiot

The best example of elite training programs is the long-standing Academic Reserve (*Atuda*) track: each year 1000 select high school graduates defer their military service to first pursue a university degree (mostly in science and engineering) financed by the IDF; they then serve two to three years as officers. After completing their compulsory service, they typically serve in the IDF for three to five additional years, with full salary and benefits. As a result, they join the Israeli workforce as engineers following six to ten years of IDF service. Technology-intensive IDF units such as Unit 8200 are the typical destination for

[13] https://www.rashi.org.il/cyber-education-centre

these graduates, who later join the private sector.

A second program exists for the very best of the Atuda-qualified youth. These top students are invited to participate in the exclusive *Talpiot* program, an elite 40-month IDF training program established in 1979. Students in this program pursue higher education while serving in the army, and then commit to six years of IDF service during which they hone their skills and develop expertise in various IDF and Ministry of Defence R&D projects. During their military service, these young people develop considerable entrepreneurship skills and gain substantial work experience in a highly competitive and high-pressure environment. After the completion of their military service, Talpiot graduates easily assimilate into the Israeli labour market to occupy senior positions in the Israeli high-tech industry. Talpiot graduates have launched many of the start-ups established in Israel since the 1990s. The Talpiot program is a particularly good example of how supply-side government human capital investment has a significant spill-over effect on demand-driven civilian innovation in the long-run.

A case in point is the establishment of the Israeli company Check Point. Please see the figure to the right.

CASE 3: CHECK POINT

Listed on NASDAQ
Founder: Former IDF intelligence member

Check Point
SOFTWARE TECHNOLOGIES LTD

Check Point was founded in 1993 and made its name by introducing the first firewall technology. It has since become an industry leading provider of cybersecurity solutions, particularly within securing Internet data and communications. They work with over 100.000 organisations.

4.3 Examples of Civilian Training Programs

Apart from defence-focused programs, the IDF has also pursued and supported educational initiatives in the civilian school system. For example, the *Magshimim* extracurricular program is a partnership between the IDF, Ministry of Education, and the CEC that focuses on the training and development of cyber skills in pupils with basic computer knowledge from the lower geo-social strata. Initially launched for 400 people, the Israeli government decided in 2013 to make it a national program open to over 4800 youths. The government, IDF and CEC cover the costs while parents pay a symbolic fee. The smaller *Gvahim* extracurricular program teaches 16-to 18-year olds more practical cybersecurity skills, and prepares pupils for a newly launched matriculation exam in cybersecurity.

As such, it is clear that the Israeli civilian cybersecurity ecosystem benefits from heavy investment in educational training programs for children and young adults. Years of expertise coupled with government funding and institutional frameworks have created a massive and unrivalled pool of tech-intuitive talents, who are tomorrow's innovators. Without this foundational component, the Israeli cybersecurity ecosystem would not be what it is today.

5. Recommendations

This section describe a few key areas and points where Denmark can find inspiration in the Israeli innovation model.

The first point is that by making a national cyber strategy and establishing a central unit (the INCD) operating directly under the Prime Minister, the Government of Israel made Cybersecurity conspicuous and a high priority issue among both public and private actors in the ecosystem

The second point is that academic research was an integral part of fomulating the strategy from the beginning. Moreover, academic research ensures continuously that the government stays up to date with the evolving cybersecurity landscape and new technologies.

The third point is that a dynamic and flexible approach is necessitated by the ever-changing nature of the cyber field. The central organisation INCD went through multiple organisational changes as described above. Recently, INCD established a taskforce to handle the emerging threats posed by the invention of quantum technology, which underlines the organisational adaptability.

The fourth point is that setting up cyber centres at almost all Israeli universities has been beneficial in terms of integrating cyber into existing areas of expertise (i.e. cyber for counterterrorism, cyber in health, cryptography etc.). These centres are fertile ground for further Danish collaboration in science and higher education. Moreover, it provides inspiration for how to ensure that cyber becomes an integral part of training talent in Denmark.

The fifth point is Israel is highly alert to the cyber landscape and has a well-educated population in this field. Israel can be an important example on how to create greater cybersecurity awareness and training among Danish stakeholders – not least among companies.

Finally, two points can be drawn from the observations made about Israeli training programs. Firstly, national-level training programs at early stages (high school) are crucial to enhancing the pool of cyber talents that can later fill positions in the industry. Secondly, the fact that Israel via the IDF elite programs has managed to present cybersecurity as an attractive career path for the best students.

6. Conclusions

The close examination of the civilian Israeli cyber ecosystem provided here has argued and provided evidence for it being a robust, well-funded and talented ecosystem. Israel is world-leading in terms of civilian cyber, and understands that cyber should not be an afterthought in business strategies. Instead, it is vital for cybersecurity to be integral and omnipresent in public and private strategies alike. The reasons for Israel's current position are many. This report focused on the unique role of government; on the vibrant and well-funded research and innovation community; and on the proactive development of young cyber talents across the country.

The role of the government in the civilian cyber sector is currently advisory and supportive. The national cyber strategy has undergone major transformations since 2002, and this flexibility to meet changing realities has proven worthwhile. However, common to all the iterations of the cyber strategy, is the centrality of academia and research. Through the INCD, the government funds large civilian cyber initiatives, in an effort to stimulate the ecosystem and continue their already good track record of innovation. It is a model of government involvement, which has not been seen elsewhere in the world.

The role of research and innovation has been presented in this report as central to civilian cyber in Israel. Universities carry out the majority of research with plentiful funding opportunities from the government, amongst others, and it is not a stretch to label Israeli researchers the foremost experts within civilian cyber. Israel is truly a knowledge hub in this sector, which naturally spurs high-quality innovation given the correct infrastructure.

The active interest taken in investing in and fostering young talents to become cybersecurity experts underlies the entire success of civilian cyber. After years in specialised educational and training programs, followed by military service to further hone their cyber skills, many youths enter the private sector and try their luck at becoming entrepreneurs. This expertise translates into high-quality civilian startups and in-depth knowledge of how to tackle cyber challenges in sectors such as transportation, finance and healthcare. It is thus expertise, developed early on, which proves beneficial to the entire civilian society years down the road.

Thus, with its distinctive combination of strategy, research and innovation, and talent generation, Israel has found at least one version of a silver bullet to meet the enormously complex challenge that is cyber. Israel offers many lessons that other digitalised and cyber-vulnerable societies could benefit from and should not be overlooked in any exploration of cyber strategies and solutions.

About ICDK Outlook

ICDK Outlook is written by the Danish Ministry of Higher Education and Science's Innovation Attachés.

The Innovation Attachés are a part of Innovation Centre Denmark which is a partnership between Denmark's Ministry of Foreign Affairs and the Ministry of Higher Education and Science. Together the two ministries manage seven centres in Brazil, China, India, Israel, Korea, Germany and the USA. ICDK Outlook is a concept where the attachés provide new knowledge and inspiration about opportunities or trends within a given topic with relevance for stakeholders within higher education, research and innovation. Find out more about Innovation Centre Denmark on www.icdk.um.dk, where you also can find all ICDK Outlooks.

Ministry of Higher Education and Science Denmark

MINISTRY OF FOREIGN AFFAIRS OF DENMARK