BRITAIN-ISRAEL
AFTER BREXIT

bicom
Britain Israel Communications and Research Centre

UK-Israel relations after Brexit: cyber security

April 2018

bicom

Key Points

- While cyber security is an issue of growing concern to governments and the private sector, the future of EU-UK cooperation in cyber security post-Brexit is uncertain.

- However, Britain's deepest intelligence partnerships already lie beyond the EU. The UK has exceptional long-standing relationships with the US, as well as with Commonwealth allies Canada, Australia and New Zealand through the formal Five Eyes intelligence sharing alliance.

- Government-to-government cooperation between the UK and Israel in cyber security is also strong and has been described by a senior UK official as a "first-order partnership". Israel is widely recognised for having a unique innovation ecosystem with close interaction between government/military, academia and industry – a model which the UK has sought to emulate – and there are close working relationships between the countries' national cyber security agencies and acknowledged cross fertilisation in the development of their national security strategies.

- UK-Israel commercial cooperation in cyber is growing stronger. Israeli cyber security experts are playing an important role maintaining London's status as a safe and secure global financial centre in the build up to Brexit by helping to secure the financial sector – which is a prime target for cyber attacks due to its leading role in global finance. An increasing number of UK banks and finance companies are working with Israeli cyber security companies to protect their operations and demonstrate that London and the UK lead the world in secure financial services.

- With many Israeli cyber companies involved in the British market, several UK firms have joined the growing list of multinational corporations establishing cyber security centres in Israel that focus on research and development (R&D), scouting, innovation, acceleration platforms.

- Academic cooperation between Israel and the UK is receiving encouragement from the government but remains under-developed compared to UK cooperation with other countries.

Introduction

This paper, part of a BICOM series on Britain-Israel relations after Brexit, focuses on cooperation in cyber security. First it sets the context regarding the UK's challenges in this issue of fast-growing importance and the potential impact of Brexit on Britain's international cyber cooperation. Then, the paper explores Israel's strengths in this field, and the impact Israel's successful innovation ecosystem has had on the development of Britain's cyber security strategy. The paper goes on to explore current and potential UK-Israel cooperation in government, commercial and academic cyber sectors.

Britain and the global cyber security challenge

- *Cyber security is a global challenge* requiring international government, commercial and academic cooperation to defend against threats from criminals, terrorists and hostile states. It is also an opportunity for those states that are well-adapted to position themselves as secure places to do business and to supply the fast-growing market for cyber technology. Technology sector analysts Gartner forecast that worldwide enterprise security spending will reach $96.3bn (£68.9bn) in 2018, an increase of 8 per cent from 2017.

- *The threat is growing* as more vehicles, household appliances, industrial equipment and infrastructure become internet connected (a development known as the Internet of Things or IoT) and therefore vulnerable to cyber attacks. The tools to carry out attacks are simultaneously becoming more widely available. As a result, the need for government-to-government cooperation has risen as has the commercial demand for cyber security products and solutions. As the chief executive of a British technological incubator told us: "The appetite in financial services for cyber security is rocketing upwards".

- *Britain is one of the world's most digitised societies,* from which it derives benefits but also finds itself particularly exposed to cyber threats. Some 3.5m new jobs have been created by tech companies in the UK, and four out of five people in the UK bought something online in the past year. This is a higher figure than in any other country, according to UK Government figures. The UK is also a founding member of the D7 (formerly D5) network of digitally advanced nations alongside Israel, South Korea, Estonia, New Zealand, Canada and Uruguay. This group aims to promote improved digital public services; openness in government systems and procurement; and digital access and skills, including coding skills for schoolchildren.

- *Addressing cyber threats that are by nature transnational requires international cooperation,* both in terms of technological development and information sharing. A senior UK official involved in UK cyber security told BICOM: "The good guys need to stick together and make use of each other's technology. That powers key security relations." The National Cyber Security Center includes within its remit "working hand in hand with industry, academia and international partners".

Why cyber security matters

- Cyber security is a fast rising priority for all industrialised states. Our day to day lives and the government and commercial infrastructure we rely on depends on digital networked systems which are vulnerable to external disruption. Individuals, groups or states with hostile intentions can access or delete data, steal sensitive information or money, damage or disrupt systems, or disseminate false information. The threats come from criminal gangs, terrorists and hostile governments, or from individual trouble makers. They threaten infrastructure, financial services, businesses, and even trust in media and the political system.

- Cyber security is a fast growing industry. The need to have effective defences is now being recognised by medium and small sized businesses, not only big corporations, and the range of vulnerabilities will grow as 'the internet of things' means an increasing number of devices are vulnerable to cyber threats.

- States that are cyber secure will be more attractive for investors and businesses to locate themselves.

- *The biggest cyber incidents of 2017 included:*

    1. Equifax, the US credit-reporting service, was subject to a major data leak, with the theft of 143m identity records, including names, addresses and social security numbers.

    2. A secret group called The Shadow Brokers published cyber warfare information and tools stolen from the NSA in 2013 – such as details on how to exploit security weaknesses in popular operating systems – making them available to non-state hackers.

    3. In May 2017 the Wannacry malware infected 200,000 computers in 150 countries by encrypting their data and demanding a ransom for decryption, using tools leaked by The Shadow Brokers. The attack disrupted NHS services.

    4. In June 2017, an even more harmful ransomware called NotPetya caused billions of dollars in damage to major companies including FedEx TNT, Danish shippers Maersk and US pharmaceuticals company Merck.

The evolution of UK's cyber security strategy, and Israel's influence

- *The UK has placed a high priority on cyber security.* In 2016 the UK Government launched its second five-year cyber security strategy with a £1.9bn budget that defined three key objectives: defend against cyber threats; deter by being a hard target and having the capability to take offensive action; and develop innovation, skills and expertise. The key shift since the original strategy was published in 2011 is the decision that government needs to take a more direct role, including developing a skills base, investing in innovative technologies, and protecting key infrastructure and services.

- *Key infrastructure, business and individuals need greater protection.* Should essential infrastructure such as energy, finance or transport be affected by a cyber attack, it could significantly harm the economy, society or government services. The government is committed to working with businesses to ensure they are protected.

- *In 2016 the UK's National Cyber Security Centre (NCSC) was established* as part of the UK Government's GCHQ signals intelligence centre. It is tasked with being the external face of UK Government action on cyber security. It defines its mission as making Britain "the safest pace in the world to live and do business online".

- *The UK and Israeli national strategies for addressing cyber challenges have developed in parallel* with acknowledged cross fertilisation between them. It is perhaps no coincidence that former UK Ambassador to Israel Matthew Gould returned from his posting in Tel Aviv in 2015 to become Director of Cyber Security at the UK Cabinet Office, and is now Director General for Digital and Media Policy in the Department for Digital, Culture, Media and Sport.

- *The UK has taken inspiration from Israel to fill a skills gap,* which is identified by the National Cyber Security Strategy as "a national vulnerability that must be resolved". The NCSC is working to promote

CYBER SECURITY: BY THE NUMBERS

Analysts Gartner forecast worldwide enterprise security spending in 2018 will reach

£68.9bn

which is an increase on 2017 of

8%

250 multinational companies

have invested in Israel mostly in R&D

£1.2 M

of joint funding UK and Israeli government's bilateral research programme focusing on the growing global cyber threat, including:

Identity management

Cryptography

Cloud security

In Israel, gross annual domestic spending on R&D consistently exceeds

4%

which is

2x

the OECD average

337

Israeli high-tech companies are currently operating in the UK

> "We have taken inspiration on Israeli ability to get a flow of people and ideas between government agencies, the military and universities."
>
> *Senior UK official familiar with the development of UK policy*

cooperation between government, academia and industry. According to a senior UK official familiar with the development of UK policy, "We have taken inspiration on the Israeli ability to get a flow of people and ideas between government agencies, the military and universities." In a speech in September 2017 NCSC Chief Executive Officer, Ciaran Martin, acknowledged this, saying: "As the UK developed a radically different, and more interventionist approach to cyber security we borrowed from some brilliant ideas … on boosting the skills base from Israel."

- *The UK has copied Israeli projects to attract talented young people into the industry.* The UK's cyber after schools programme, Cyber Discovery, is explicitly modelled on the "Magshimim" programme in Israel, and aims to draw talented 14-18 year olds into the industry.

- *The UK Government funds 14 academic centres of excellence in cyber security,* a model which is in the process of being adopted in Israel. It currently has cyber research centres in Ben Gurion University, Tel Aviv University, Hebrew University, Bar Ilan University and the Technion, with a cyber law center at Haifa University.

> "The Israeli brand is very strong and the legendary status of 8200 is pretty well known among expert consumers, which creates a strong appetite for Israeli cyber expertise."
>
> *Ben Brabyn, Level 39 Chief Executive*

Britain's international cyber cooperation post-Brexit

- *It is unclear what relationship the UK will have with EU cyber security institutions post-Brexit.* The UK is currently implementing the EU's Networks and Information Security Directive, which aims to improve security across the 28 current member states and create a Cooperation Group for strategic collaboration and information sharing between them. In a speech discussing future EU-UK security cooperation in February 2018, UK Prime Minister Theresa May stressed a mutual interest "to continue working together on developing the capabilities – in defence, cyber and space – to meet future threats". The UK's Brexit position paper on foreign and defence policy states on cyber security that "the UK's partnership with EU agencies and bodies should be as flexible and innovative as the nature of the threats we face". It adds that "the UK is ready to maintain and deepen our shared ability to support our collective security," including participation in EU emergency response team networks and the Cooperation Group for "sharing relevant threat information," and "joint analysis".

- The UK will also have to *implement the requirements of the General Data Protection Regulation (GDPR).* This requires that personal data must be processed in a manner ensuring an appropriate level of security and which will become binding and directly applicable in all EU Member States on 25 May 2018. Following Brexit, the UK will aim to be subject to Article 45 of the GDPR, which stipulates that data transfers will only be permissible if the UK – considered a third country – ensures an adequate level of protection.

- *How these principles and legislation will translate into an actual post-Brexit relationship* – including cooperation frameworks in R&D and intelligence and information sharing – *will depend on the outcome of withdrawal negotiations.*

- *As it stands, Britain's deepest intelligence sharing partnerships already lie beyond the*

EU. The UK has exceptional long standing and deep intelligence cooperation with the US, as well as commonwealth allies Canada, Australia and New Zealand through the formal Five Eyes intelligence sharing alliance.

- *Britain and Israel are generally recognised as two of the world's five cyber superpowers,* alongside the US, Russia and China. Israel is known as the "start-up nation," boasting a world leading concentration of high-tech and software companies, that build on Israel's outstanding innovation ecosystem and entrepreneurial culture. Israel generates the second largest revenue in the cyber security market behind the US.

- *UK-Israel government-to-government and commercial cooperation in tech issues, including cyber, is strong and growing.* The potential for UK-Israel commercial cooperation in the high-tech fields was recognised by the British government several years ago with the establishment in 2011 of the UK Israel Tech Hub in the British Embassy in Israel. The hub's role has been to partner UK businesses with Israeli start-up companies, building on synergies between British strengths in global commerce and Israeli strengths in innovation, and creating a culture of bilateral private sector partnership. The UK announced in 2017 it was copying the model in five emerging markets.

- *UK-Israel cyber cooperation is unlikely to be adversely affected by Brexit.* Israeli organisations are participating in aspects of EU cyber security policy, such as the Horizon 2020 R&D programme, and the new European Cyber Security Organisation, intended to foster cooperation between public and private sectors. Britain and Israel, however, have separate bilateral institutions promoting cooperation between cyber security industries (see below), and cooperation between government agencies is already strong.

Reasons behind UK-Israel cooperation: The Israeli model and capabilities

- *Israel (population 9m) is the world's second largest cyber security technology exporter* after the US. Israeli cyber security exports were worth $3.7bn in 2016, according to the Israel Cyber Alliance, and in 2017 Israel attracted 16 per cent of all global cyber security investments.

- *Israel is renowned for its "innovation ecosystem"* – the interaction between government, academia and industry which is considered crucial to developing a successful cyber security industry. In the cyber security field, Unit 8200, the signals intelligence unit of the IDF's military intelligence division, is renowned for attracting among the best and brightest Israeli recruits. After three years of military service these individuals go to university or into industry with a wealth of hands on experience and strong personal network, and often retain their links with 8200 through reserve duty. This expertise is recognised internationally. Ben Brabyn, Chief Executive of the Level 39 technology hub told BICOM that "the Israeli brand is very strong and the legendary status of 8200 is pretty well known among expert consumers, which creates a strong appetite for Israeli cyber expertise".

- *Due to its hostile neighbourhood, defence has always been central to Israeli society and culture* and a focus for national investment. Israel faces a wide range of external cyber threats, including from terrorists, criminals, "hacktivists" and hostile states. An Israeli official working in a government cyber security role with a background in commercial cyber R&D told BICOM: "Living in Israel, we are used to the fact that we are being attacked and used to being in protective mode. Because our mind-set is automatically thinking that way it is easier for us to put ourselves in the position of companies addressing security challenges." Chen Dembo of CyberInt, an Israeli cyber security company that works in the UK, reiterated this point. She told BICOM that the one thing the British market finds attractive about Israeli cyber companies is their understanding of cyber threats from the perspective of the attacker and emphasises that these firms are generally filled with former 8200 graduates. "By understanding

the methodology of attackers, even nation-state actors, Israeli companies are capable of creating cyber security solutions that are truly fit for today's cyber challenges," she said.

- *Israel had a very strong innovation culture for which it has been dubbed the start-up nation.* According to Dan Senor and Saul Singer, the authors of the best selling book that goes by the same name, this is due to a unique combination of traits in Israeli culture, including a readiness to question authority, determined informality, a constructive attitude towards learning from failure, and strong features of IDF institutional culture including teamwork, commitment to mission, acceptance of risk, and cross-disciplinary creativity.

- *The Israeli Government is working to enhance the strengths of its innovation ecosystem* – especially the cyber security industry – to ensure that Israel is well defended. In addition it aims to promote foreign investment in its cyber industry and Israeli exports of cyber tech. Israel's National Cyber Directorate (Israel's equivalent to the UK National Cyber Security Centre), based in the Prime Minister's Office, includes a Cyber Technology Unit to foster research, the development of human capital, and international cooperation.

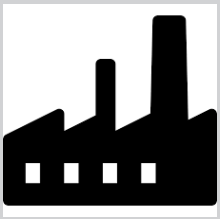
- *The Israeli market and ecosystem is small, so it needs global commercial investment and partnerships* alongside global export markets to sustain and develop the industry and to market its products internationally. Foreign investment is one of the main sources of R&D investment in Israel and accounts for Israel's annual gross domestic spending on R&D consistently exceeding 4 per cent of GDP. This is nearly twice the OECD average

Israel's cyber security ecosystem

- *Israel's cyber security innovation ecosystem is based on interaction between three pillars* of cyber knowhow in Israeli society: military, academia and industry. These interactions, combined with Israel's small geographic size and relatively small population, mean that the tech and cyber security community is densely networked. There is also a strong sense of social cohesion that comes from factors such as persistent external threats and shared experiences that many have of military service.

- *Military: Israel has universal conscription and service in Israel's elite 8200 signals intelligence unity is highly prestigious,* attracting some of Israel's brightest and most tech savvy high school graduates. These young recruits get immediate training and experience in handling cyber crises and challenges, in a military culture where innovation and initiative are encouraged. Having graduated from the army they then study for degrees at Israeli universities before entering industry enriched with technical knowhow and high level professional and military experience. Many graduates will continue to serve in the reserves.

- *Academia: Israel has nine universities, with seven ranked in the world's top 500.* Each of these has, or is establishing, a cyber security research centre, focussing on the strengths of that particular university.



- *Industry: Israel has the largest concentration of cyber security companies anywhere in the world.* By the end of 2017 there were 420 active cyber security companies in Israel (up from 148 in 2011). Half are start-ups established in the last five years. Around 10 per cent have raised $20m, and five are traded on Nasdaq, including CYREN, Checkpoint, Forescout, Varonis (according to Israel Cyber Alliance). Around 30 multinational companies from various industries have cyber security-related R&D centres in Israel.

Israel's cyber security ecosystem: case study – Advanced Technology Park, Beersheva, aka "CyberSpark"

The Advanced Technology Park in Beersheva brings all the elements of Israel's innovation ecosystem into close proximity. The Park is located across from the Beersheva campus of Ben Gurion University and houses the university's Centres of Excellence in various technological fields, including the Deutsche Telekom Laboratories which are the result of a long standing collaboration between the German commercial telecoms giant and Ben Gurion University, and the university's Cyber Security Research Center. Next to the site the IDF is developing a 2m-square-foot high-tech telecommunications R&D center. This is the home of Israel's Cyber Emergency Response Team (CERT) and its elite Cyber technology teams are also relocating to this campus. By 2017 the Technology Park was also home to 70 start-ups with 1,500 engineers, with a goal of 10,000 engineers by 2026. The ATP also hosts JVP Cyber Labs, a government backed commercial incubator which identifies and nurtures new cyber security and big data companies.

and matched only by South Korea. By comparison, UK gross domestic spending on R&D in 2016 was 1.7 per cent.

- *250 multinationals have invested in Israel, mostly in R&D.* Around 30 multinational companies from various industries have cyber security-related R&D centres in Israel, including automotive companies, financial institutions, professional service providers, and internet companies. These include: Paypal, Cisco, CitiBank, Microsoft, EMC, Accenture, Intel, Amazon, McAfee and IBM. Companies that opened R&D centres in Israel in 2017 include Symantec, TD Bank, Renault, Daimler AG, and Harman. These investments typically mean either acquiring a start-up or opening an office and hiring local employees.

- *The density of tech research and development in Israel draws in ever more companies and investors, creating an "investment ecosystem"* alongside the "innovation ecosystem". An Israeli who works with multinational corporates, startups and investors referred to the importance of this additional ecosystem. He describes it as the combination of "both the big and smaller start-ups, the VCs, the accelerators, the mentors, the tech-companies … [creating] a certain critical mass". He added that "because companies rarely know in advance where they will end up finding solutions for their challenges, the diverse ecosystem in Israel provides a useful platform for them".

- *Multinational investors see the advantage of employing Israeli engineers in Israel.* A senior industry expert told BICOM that many companies have come to realise that it is more fruitful to employ Israelis working within the Israeli ecosystem, rather than bringing them to work overseas.

- *British banks are "early adopters" of technology, which often leads them to utilise Israeli expertise.* An Israeli cyber expert in the field for almost 20 years told BICOM that fighting cyber crime, (financially motivated cyber rather than cyber espionage) often involves significant collaboration between the UK and Israel. He added that major British banks are clients of many Israeli cyber companies and explained that there are two main drivers to this collaboration. The first is that the UK's financial sector, which is the most advanced in the world and thus a larger target for cyber attacks, is characterised by being an "early adopter of technology", which makes them more attracted to Israeli start-ups. The second is that because the recent European Revised Payment Service Directive (PSD2) legislation requires authentication for all digital transactions, UK companies look to Israeli experts in the authentication field. He concluded that Israeli cyber technology is already prevalent in Britain: "Today, the vast majority of digital transactions and credit card ecommerce in the UK is essentially protected by Israeli technologies, first developed by Cyota (and later bought by RSA Security, the number one e-commerce technology used by UK credit card companies and banks)."

ISRAELI CYBER SECURITY FIRMS BY SECTOR

Israeli cyber security exports were worth $3.7bn in 2016 and in 2017 Israel attracted 16 per cent of all global cyber security investments.

- Connected Devices, IoT: 72 companies. Solutions for security challenges when using connected devices, from IoT network and mobile device management, to connected cars, industrial control systems, and medical devices.
- Network Security: 65 companies. Prevention of APT, visibility solutions, isolation and deception (for the enterprise network.
- Security Operations and Orchestration: 57 companies. All operational measures required to protect an enterprise network, including incident response, forensics, SIEM, alert management, threat intelligence, and penetration tests.
- Data Protection, Encryption and Privacy: 50 companies.
- Anti-fraud, Authentication and IAM (Identity and Access Management): 44 companies.
- Applications and Website Security: 39 companies. Security measures for software and web applications, including code review, bot detection, web application firewall (WAF) and DDoS prevention.
- GRC and Vulnerability Management: 26 companies. Vulnerability management, solutions for cyber insurance, supply-chain monitoring, and compliance audit.
- Endpoint Security: 21 companies. All anti-malware and anti-ransomware solutions, and Endpoint Detection and Response (EDR).
- Cloud and Infrastructure Security: 20 companies Solutions for securing Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (Paas), container-based virtualization and serverless computing.
- Mobile Security: 17 companies

Source: Start-Up Nation Central

Components of UK-Israel cyber cooperation: present and future

Government to government: "Israel a first order partner"

- *Cooperation between British and Israeli Governments on cyber security is strong.* A senior British official familiar with the situation told BICOM that Israel is a "first order partner" in cyber security. An official basis for this relationship was outlined with a Memorandum of Understanding on bilateral digital cooperation in 2014. During a February 2016 visit to Israel, then-UK Cabinet Office minister Matt Hancock announced extended cooperation in cyber defence of national infrastructure. This included a programme promoting academic cooperation in cyber-physical security and information sharing between cyber emergency response teams (CERTs). Hancock is now the Secretary of State for Digital, Culture, Media and Sport, giving him a key role in future relationships.

- *There is close cooperation between government agencies.* Though activities involving secret intelligence are necessarily kept private, public statements by UK officials hint at the depth of cooperation with Israel. In a speech to Tel Aviv University's international Cyber Week conference in June 2017, the CEO of the UK's NCSC Ciaran Martin spoke of relations with Israel as "one of our newest but fastest developing cyber security partnerships". He described his bilateral meetings with his former Israeli counterpart Eviatar Matania on "technological collaboration, operational detection, on policy and communications, on how we manage responses to incidents that effect all of us". Martin also expressed gratitude for Israeli cooperation and information sharing in responding to the WannaCry ransomware attack in 2017 (see box). In January 2017, the outgoing Director-General of the GCHQ Robert Hannigan, said: "As we establish the new National Cyber Security Centre as part of GCHQ, we are building on an excellent cyber relationship with a range of Israeli bodies and the remarkable cyber industry in Be'er Sheva." Similarly, Treasury Minister Robert Jenrick told a fintech conference in London in March 2018: "We put strong emphasis on cyber security, including strong collaborations with leading countries such as Israel."

> "Today, the vast majority of digital transactions and credit card ecommerce in the UK is essentially protected by Israeli technologies, first developed by Cyota."
>
> *Israeli cyber expert*

- *Cooperation is enhanced by the similarity of UK and Israeli cyber security strategies.* A senior analyst on national cyber security policies at Tel Aviv University told BICOM: "Both countries see cyber security not only as threat but an opportunity. Since cyber is becoming an essential tool of the global economy, companies will locate to places with strong cyber security, whilst the market for cyber products and services is growing."

> "If I were a UK company with big cyber exposure, I would be troubled if I was not making use of Israeli tech and expertise."
>
> *Senior UK official in the cyber security field*

Commercial cooperation: fast developing

- *Brexit creates an impetus for Britain to deepen bilateral economic relationships beyond the EU* and Israel's growing economy and significance as a strategic power has led to it being identified as a particular target for trade expansion. A UK Government White Paper identified Israel as a trade priority for post-Brexit Britain because of the potential synergies between Israel's high levels of innovation and British strengths in design, business growth and finance, as well as the UK's own high-tech and scientific strengths.

- As the threats to companies and their vulnerabilities grow, *global companies*

are expanding their investments in cyber technology and security. The UK's 2016 Cyber Strategy stresses the need for "businesses and organisations to take all reasonable steps to protect their personal data and build resilience … into the systems and structures on which they depend".

- *UK investments in Israel are developing* with several major British companies establishing R&D operations in the country. Financial services are leading the way due to the centrality of IT in their businesses and the need for innovation in the fintech sector. In September 2017, HSBC opened a Cyber Hub in Tel Aviv, joining Barclays and Royal Bank of Scotland (RBS), who also have a presence in Israel, as well as UK chip designer ARM, which in 2017 announced an expansion of its Israel operation from 200 to 350 engineers (see box). An Israeli who works with British companies at a Jerusalem-based investment incubator for early-stage tech firms told BICOM: "What's attractive for British companies is often the interface between Israeli expertise, the country's geographical proximity to Europe, and the professional care that international companies receive in Israel because the market here is still relatively small."

- *A notable example of a British company investing in Israel is UK chip designer ARM.* It began its Israel operations with the acquisition of Israeli chip security company Sansa Security Inc. in 2015 for $90m, with a focus on security software relating to the Internet of Things. By 2017 ARM had expanded the operation from Sansa's initial 90 engineers to 200. In late 2017 it announced it was hiring 150 more, making it one of ARM's leading research centres.

- *The opportunity cost of not having a presence in the Israeli ecosystem is recognised by UK officials.* A senior UK official in the cyber security field told us: "If I were a UK company with big cyber exposure, I would be troubled if I was not making use of Israeli tech and expertise."

- *Director of Innovations for RBS Kevin Hanley, spoke highly of his company's investment in Israel* in a recent film, saying: "Our experience over the last couple of years of working in Israel is that there are some great technology capabilities. It's a great centre for cyber security and biometric authentication, it's a great centre for data and analytics, it's a great centre for payments technology as well."

Case study: ARM

- The UK Chip designer ARM began its Israel operations with the acquisition of Israeli chip security company Sansa Security Inc. which it bought in 2015 for $90m, with a focus on security software relating to the Internet of Things. By 2017 ARM had expanded the operation from Sansa's initial 90 engineers to 200. In late 2017 it announced it was hiring 150 more, making it one of ARM's leading research centre.

- However, some industry experts point out that the UK investment in Israel's cyber sector is still relatively small. Out of 87 companies from 18 countries – including Booking.com, Hyundai and Dropbox – which have opened offices in Israel since 2014 to pursue R & D or innovation, only five of these were British: chip designer ARM Holdings, Atmosphere Control Technology business Johnson Matthey, Fin-Tech venture ShareGain, multinational telecommunications testing company Spirent and Yoobic Retail Experience.

- The UK is considered a primary export target for Israeli companies, according to the Israeli export institute. The UK offers several advantages as a stepping stone to global markets, including English language, which is widely spoken in Israel, a similar time zone (two hours difference), coupled with UK expertise in global commerce. In September 2017, British companies Aviva Insurance, BT, Goldman Sachs, RBS, Visa and others hosted Israeli cyber security startups for a series of targeted events in London.

- *However, industry experts point out that the Israel-based R&D operations of UK companies are relatively small* compared to other major multinationals, and that the number of UK companies utilising Israeli tech expertise still lags behind Canada, China, and the US.

Israeli companies in the UK post-Brexit

- The Israeli Export Institute confirmed to BICOM that *the UK is considered a primary export target for Israeli companies,* with the CEO of one cyber security company telling us that "being able to break into the UK market is of strategic importance for Israeli vendors". The UK offers several advantages as a stepping stone to global markets, including English language, which is widely spoken in Israel, a similar time zone (two hours difference), coupled with UK expertise in global commerce.

- *Israeli companies have proven themselves in finding solutions to cyber challenges.* There has also been a sea change in the way in which Israeli cyber companies are perceived in the UK. Jonathan Gad CEO of Elite Cyber Solutions, which works with the best-of-breed Israeli cyber technology vendors in order to help enable their go-to-market strategy and sales told BICOM that there has been a "tremendous positive shift in the UK over the last few years" in which Israeli cyber technology companies "have proven to be extremely successful in defending against the modern day cyber threats".

- According to the Israeli high-tech and venture capital database IVC-Online, *337 Israeli high-tech companies are currently operating in the UK.* Of those, 125 were set up over the last five years. In July 2017, the British Embassy in Tel Aviv reported that the number of companies has actually risen since the Brexit referendum, with 25

Case study: responding to WannaCry

- The WannaCry attack in 2017 affected computers all over the world. Computers infected by the virus had their data encrypted and users were presented with a ransom demand. In Britain it led to the cancellation of at least 6,900 NHS appointments after many NHS computers were affected. This attack was subsequently attributed by UK and other intelligence agencies to North Korea.

- In a speech at Tel Aviv University in June 2017, CEO of the UK National Cyber Security Center Ciaran Martin, spoke about the deep cooperation between Britain and Israel in responding to global cyber-attacks like WannaCry:

> "Phoning people in California, in Israel, all over the world in the middle of the night saying: 'What have you got, give us this, is this working?' and getting a specific piece of guidance, that gets British hospitals back up and running as quickly as possible - that is partnership. I will never forget and I will always be grateful for Eviatar Matania (Head of the National Cyber Bureau in the Prime Minister office of Israel), phoning me on a Sunday morning, to tell me how the first day of the working week in Israel was working with the mitigation that had been put in place in this country. And that again is partnership in action."

Israeli companies entering Britain between June 2015-May 2016 – investing £114m and creating 787 jobs and 32 Israeli companies set up in the 12 months following the referendum (an increase of 28 per cent) with an investment of £152 m pounds (an increase of 33.5 per cent) and the creation of 888 jobs (an increase of 12.8 per cent.) These companies focus on a variety of issues such as software, financial services, media, life sciences, infrastructure and energy.

- *One example of an Israeli cyber security technology company protecting key UK infrastructure is Waterfall Security.* This company's product is installed routinely in offshore platforms, liquid natural gas terminals, pipeline control systems, refineries and petrochemical manufacturing plants all over the world, protecting their control systems from dangerous traffic coming from the internet. While its specific customers and projects are not public, the company confirmed to BICOM that its biggest UK market is the oil & gas industry. Another leading Israeli cyber company, CheckPoint, told us that it has many long standing customers in the UK banking and healthcare sector that have invested heavily in their technology.

- *The extent to which tech companies in general will be deterred from setting up in Britain by Brexit remains an open question.* An Ipsos MORI survey in October 2017 involving 17 Israeli tech firms highlighted some potential concerns, such as the need for "a solution that allows for companies to have smooth access to the EU market for goods and services" and "a solution that allows for continued regulatory alignment with the EU".

- *Israeli and British cyber experts are divided over the potential influence of Brexit.* One British tech expert who runs an accelerator programme for international companies told BICOM that while for Israeli fin-tech companies London was seen as the "next place to go," many Israeli cyber companies are prioritising breaking into the American market. Others in the industry played down the significance of Brexit. Uri Rivner, Chief Cyber Officer at BioCatch, which uses behavioural biometrics for fraud prevention and detection, told BICOM that it was "too early to understand the implications of Brexit. Yet it's unlikely to change the game in terms of UK-Israeli collaboration. As long as London remains a very strong financial sector which is characterised by adopting new technologies, Brexit won't put a dampener on the relationship". The CEO of an Israeli company who helps start-ups break into the British market told us that "Brexit is still seen as far away, and it's unclear what it will mean…most smaller Israeli start-ups – whose mentality is often more short term focused – are not overly bothered by it". Another interviewee reported that Brexit was not on their company's radar at all in terms of their hopes to expand their business in the UK.

Academic cooperation: untapped potential

- *In 2015, UK and Israeli Governments jointly funded a £1.2m joint academic project,* promoting collaborative research partnerships into cyber security threats. Grants were awarded to collaborations between teams at Bristol University and Bar Ilan University, University College London and Bar Ilan University, and the University of Kent and University of Haifa.

- *In 2016, Matt Hancock announced "a new academic engagement* between the UK and Israel in the emerging area of cyber-physical security" with the proposal that "Israeli experts will engage in joint research with UK academics in cyber security". He announced "a competition to find the best ideas and people to work together to develop research focussed on what is another new frontier: protecting our cyber physical systems: like protecting industrial control systems, the internet of things and driverless cars".

> "Brexit is unlikely to change the game in terms of UK-Israeli collaboration. As long as London remains a very strong financial sector which is characterised by adopting new technologies, Brexit won't put a dampener on the relationship."
>
> *Uri Rivner, BioCatch Chief Cyber Officer*

- *In 2017 the British Council and UK Science and Innovation Network invited applications* for grants to fund joint UK-Israel academic symposia and workshops in various scientific fields including cyber.

- *UK-Israel bilateral research cooperation in cyber remains limited, however.* An Israeli academic at one of Israel's top university cyber research centres, told us: "I am afraid the reasons are political because when I tried to work with a couple of colleagues of mine, that's the understanding that I got. To sell it [UK-Israeli cooperation] internally through the university governance creates unnecessary political problems for them … we have cooperation with other countries, many in the United States and some also in continental Europe, but almost none in the UK."

- *The potential for joint research could also be affected if the UK does not participate in future EU R&D funding projects,* such as the successor to the €80bn Horizon 2020 programme (which runs until 2020). Horizon 2020 funds research projects undertaken by academia and industry that frequently bring together several partner organisations from various member states or associated countries. The UK currently ranks first in the EU for numbers of participants receiving Horizon 2020 grants. Israel became the first non-EU member to join its R&D framework as an associate in 1996. Israel pays a contribution into the grant fund in return for eligibility for Israeli institutions to compete for grants on an equal basis to those from EU states, and Israeli researchers have been very successful at winning grants. The UK Government has sought to reassure researchers whose EU funding is put in doubt by Brexit by committing to underwrite bids for Horizon 2020 projects submitted while the UK is still an EU member. British researchers hope the UK will also become an associate member of the successor to Horizon 2020, something the government is yet to commit to. This positon was criticised in a March 2018 report by the House of Common Science and Technology Select Committee. Also in question is Britain's future participation in the Erasmus+ academic and student exchange programme, in which Israel is a partner country.

Conclusion

- *Cyber security is a fast-growing threat and opportunity for all developed nations.* While the UK will continue its strong cooperation with international partners, the future of the UK's participation in EU-wide cyber cooperation is uncertain pending the outcome of Brexit negotiations.

- *The existing strong UK-Israel cooperation looks set to develop further* on the basis of bilateral agreements and fast-developing working relationships between government agencies. The UK is keen to learn from and cooperate with the extraordinarily successful Israeli innovation ecosystem.

- *Israeli tech firms have continued to set up in the UK,* even whilst uncertainty about investing in the UK will remain an inevitable feature of the economic environment for the time being. The UK continues to be seen as an export target for Israeli industry and a good place for Israelis to do business.

- *UK officials recognise the particular opportunities for British companies participating in Israel's unique innovation ecosystem,* as the UK Government encourages British industry to invest more in cyber security. Several major British companies are establishing R&D operations in Israel, though there is considerable scope for growth in this area.

- *UK and Israeli Governments continue to promote academic cooperation* in the cyber field, though some Israeli academics report resistance from UK colleagues – thereby representing a potential missed opportunity for the UK cyber innovation ecosystem.

Ten of Israel's leading cyber companies operating in the UK

CyberArk develops technologies to secure businesses against cyber attacks carried out by insiders, and boasts more than half of Fortune 100 companies among its clients. Founded in 1999 it employs more than 1,000 people. With its main offices in Petah Tikva, Israel, and in the US, it also has an office in London.

Check Point Software Technologies Ltd is the largest network cybersecurity vendor worldwide, protecting more than 100,000 businesses of all sizes. Founded in 1994, it employs more than 4,000 people in its main offices in Tel Aviv and the US, along with its international subsidiaries, including in London.

ForeScout offers enterprises and government organizations the ability to view and control traditional and IoT devices connected to their networks. Founded in 2000, it employs more than 800 people, with main offices in San Jose and Tel Aviv, as well as an office in London.

Varonis Systems Ltd offers software to protect file and email servers from cyberattacks, data breaches, and insider threats. Founded by two Israelis in 2005, its main office is in New York with its research centre in Herzliya. It employs more than 500 people, with an office in London.

Radware provides solutions to protect virtual, cloud, and software-defined data centres from cyber-attacks. With its international HQ in Tel Aviv, it employs more than 800 people, with offices across Europe, including in London.

Allot Communications is a global provider of security and analytics tools used by over 500 mobile, fixed and cloud communication service providers including five of the top ten global mobile operators. Based in Hod Hasharon, Israel, it employs more than 700 people, with an office in the UK.

Team 8 develops disruptive companies that challenge the biggest problems in cybersecurity to provide organisations the advantage over cyber attackers. One of its portfolio companies, *Illusive Networks*, is a pioneering deception-based cybersecurity that creates a deceptive layer across the entire network in order to neutralise targeted attacks and Advanced Persistent Threats and recently set up in the UK.

BioCatch was founded in 2011 by experts in neural science research, machine learning and cybersecurity, to develop behavioural biometrics profiles of online users in order to recognise a wide range of human and non-human cyber-security threats to prevent fraud. It works with three of the top four banks in UK and recently opened an office in the UK.

Imperva is a leading provider of cyber security software and services to protect enterprise data and application software, ensure regulatory compliance, and improve performance and delivery. Founded in 2002, the company went public and was listed on the New York Stock Exchange in 2011. In February 2017, Imperva purchased Camouflage, a data masking company. Its has several offices around the world including in Tel Aviv, New York, California, Melbourne, Hong Kong and Singapore. Its UK office is located in Berkshire.

Cyberbit, founded in 2015, secures enterprises and critical infrastructure against advanced cyberthreats by providing a first unified, product suite for threat detection, incident response and simulated training. Employing over 500 people and acquired by Elbit, its headquarters are in Raanana, with additional offices in Singapore, Austin, Munich and London.

This report has been produced by BICOM's research team in consultation with British and Israeli cyber security experts. We are grateful for their help.

For more information please contact:
Charlotte Henry, Senior Press Officer
020 3745 3348
07879 644099
charlotteh@bicom.org.uk

BRITAIN-ISRAEL
AFTER BREXIT

bicom
Britain Israel Communications and Research Centre