*Oficina Económica y Comercial de España en Tel Aviv**

INVERSIÓN ESTRATÉGICA EN EL SECTOR DE LA CIBERSEGURIDAD: EL CASO ISRAELÍ

El objetivo principal de este texto es, de forma divulgativa, describir el sector de la ciberseguridad en Israel, prestando especial atención a la forma en la que el mismo se financia. La aproximación al sector se ha realizado desde lo general hasta lo particular, comenzando por el estado actual de la ciberseguridad en el mundo, para a continuación describir el sistema de innovación israelí y por último analizar el sector en el país, comentando sus casos de éxito. El estudio concluye con ideas sobre cómo la empresa española puede aprovecharse de este dinámico ecosistema en el campo de la ciberseguridad para mejorar sus procesos y ganar competitividad.

Palabras clave: capital riesgo, ciberataques, *start-ups*, Israel.
Clasificación JEL: O31, O32, O33, O38.

1. Introducción

«La ciberseguridad es un gran negocio». Estas palabras fueron repetidas en varias ocasiones por el primer ministro de Israel, Benjamin Netanyahu, durante la última edición de la feria Cyberweek, celebrada en la Universidad de Tel Aviv. Razón no le falta. En 2017 el gasto mundial en ciberseguridad habría alcanzado los 86.400 millones de dólares de acuerdo con la consultora tecnológica Gartner.

Israel abarca una parte importante de este mercado. Este pequeño país de unos 8,8 millones de habitantes recibe entre un 15 y un 20 por 100 de la inversión mundial en ciberseguridad, lo cual lo sitúa en el liderato del sector junto con EEUU. Nombres como Check Point, CyberArk, Imperva o Argus destacan entre las más de 450 *start-ups* y empresas del sector.

Para comprender mejor los porqués de la gran relevancia de la ciberseguridad en Israel primero estudiaremos el estado del sector en el mundo y sus principales tendencias, para más adelante analizar el caso particular de Israel.

2. Contexto internacional

Hay pocas palabras que hayan ganado más notoriedad en los últimos años que las de ciberataque o ciberseguridad. ¿Quién no ha oído hablar de WannaCry o NotPetya, de los robos de información en Yahoo o Equifax, de los intentos de sabotear campañas electorales en países como EEUU o Francia? ▷

* Este artículo ha sido elaborado por Víctor Vegas Serrano.
Versión de enero de 2018.

Individuos, empresas y Gobiernos han sufrido de una u otra forma ataques contra sus intereses mediante el uso de la tecnología y el ciberespacio. Los ataques son cada vez de tipologías más variadas, más sofisticados y de mayor alcance. La razón principal de su incremento es que la tecnología está presente en más y más aspectos de nuestra vida. El tratamiento y análisis masivo de datos (*Big Data*), la interconexión entre usuarios y cambios en los sistemas de acceso y almacenamiento de información (*Cloud Computing*), la conectividad de numerosos dispositivos a internet (*Internet of Things*) o la digitalización de servicios, como puede ser la banca a distancia, han sembrado un campo de cultivo perfecto para ser blanco de ciberataques malintencionados.

Los ciberataques pueden ir más allá del robo de información o la suplantación de identidad. Pueden ir tan lejos como al ataque de infraestructuras críticas (centrales energéticas, hospitales, etcétera) o directamente ser actos de ciberguerra. Recordemos, por ejemplo, el ataque de Stuxnet supuestamente destinado a ralentizar el programa nuclear iraní.

En fechas tan recientes como enero de 2018 ya están surgiendo nuevas vulnerabilidades que sin duda muchos voluntarios están dispuestos a explotar. Dos nuevas tipologías de ataques, denominadas Meltdown y Espectre, pueden aprovechar un fallo en los procesadores modernos para obtener información sin autorización. Además, el actual auge de las criptomonedas y su elevado valor incentivan los posibles robos de las mismas, que se han multiplicado en los últimos meses.

Cada vez se va a requerir un mayor esfuerzo para proteger adecuadamente todo el espectro de tecnologías que nos rodean. Esto no se consigue solamente mediante mejores sistemas de ciberseguridad; también es necesaria una mayor educación en TIC para que individuos y empresas sepan mantenerse protegidos. Asimismo, la coordinación y colaboración entre Gobiernos para combatir eficazmente futuras amenazas es esencial. En el siguiente apartado se va a analizar el desempeño de Israel en este campo y se va a tratar de modelizar los factores que han llevado al país a ser una potencia en ciberseguridad.

3. La ciberseguridad en Israel

Israel es, en segundo lugar tras Estados Unidos, el país con más inversión privada recibida en ciberseguridad, con un mayor número de empresas incluidas en el *ranking* Cybersecurity 500 y con unas mayores exportaciones en el sector.

Ahora bien, ¿cuál es la razón por la que Israel, un país de apenas 8,8 millones de habitantes, haya alcanzado semejante notoriedad en el campo de la ciberseguridad? Esta pregunta no tiene una respuesta sencilla, y para comenzar a responderla es necesario comprender en primer lugar el ecosistema de innovación israelí.

3.1. El ecosistema innovador

Muchos son los factores que han llevado al Estado de Israel a convertirse en la denominada *Start-up Nation.* En primer lugar, su complicada situación geopolítica y sus escasos recursos naturales[1] han forzado a Israel a especializarse en la tecnología y el conocimiento, convirtiéndolos en la base de su economía. ▷

[1] En los últimos años se han descubierto importantes reservas de gas natural en la costa de Israel, mejorando por tanto su situación respecto a posesión de recursos naturales.

Por otra parte, la juventud de Israel como país, el origen multicultural de sus habitantes y la obligatoriedad de un servicio militar muy exigente en la toma de responsabilidades causan que los israelíes tengan por lo general una fuerte capacidad de liderazgo, escasa aversión al riesgo y una mentalidad altamente emprendedora, que les lleva a la creación de *start-ups* y a la innovación.

Es precisamente esta gran apuesta por la innovación el factor más relevante en la formación de la *Start-up Nation*. De acuerdo con datos de la OCDE y la UNESCO, Israel destina a I+D civil alrededor de un 4,3 por 100 de su PIB, líder mundial junto con Corea del Sur en este aspecto. Este porcentaje destaca en comparación con la mayoría de países desarrollados, que se sitúan en un porcentaje de gasto de entre 1 y 3.

En cualquier caso, en Israel la innovación es mucho más que un porcentaje. La innovación es una filosofía que se aplica en todos los aspectos y procesos del día a día y que no afecta tan solo a sectores tecnológicos, sino que también remodela sectores tradicionales como el turismo (*traveltech*), la moda (*fashtech*) o la construcción (*constructiontech*).

Las universidades son, de igual forma, una pieza sustancial del ecosistema. De las nueve universidades de Israel, cinco son altamente competitivas internacionalmente en investigación y están muy vinculadas al sector privado.

Otro incentivo es que los proyectos innovadores en el país están ampliamente respaldados por el Gobierno. Israel dispone de programas de apoyo público de hasta el 85 por 100 de la inversión para *start-ups* innovadoras. Esta ayuda tan solo es devuelta al Estado, si el proyecto es exitoso, en forma de *royalties*.

En este atractivo contexto, un gran número de multinacionales se está instalando en el país mediante centros de I+D con el objetivo de beneficiarse de esta cultura innovadora. En el periodo 2014-2017 hasta 87 corporaciones han abierto nuevos centros de innovación en Israel, que se suman a los ya existentes de empresas como Intel, Google o Apple.

Otro factor importante para completar la imagen de la *Start-up Nation* es el relativamente fácil acceso a capital. De acuerdo con IATI (Israel Advance Technology Industries), casi 150 fondos de capital riesgo están registrados en Israel, a los que se deben sumar otra veintena de fondos pertenecientes a grandes corporaciones. Además, según el World Economic Forum, en su estudio de competitividad global 2017-2018, Israel es el segundo país del mundo (tras EEUU) en disponibilidad de capital riesgo. El gran vínculo existente entre EEUU e Israel se hace aquí patente: gran parte de los fondos de capital riesgo presentes en Israel tienen como origen el país norteamericano y, en muchos casos, además de aportar capital, también proporciona a la *start-up* una vía de acceso al mercado estadounidense. Adicionalmente, la existencia de un gran número de incubadoras de empresas, aceleradoras y de plataformas especializadas que unen las necesidades de las grandes empresas con las soluciones tecnológicas israelíes facilitan la actividad de los emprendedores.

3.2. La apuesta por la ciberseguridad

En este contexto tan favorable al emprendimiento y la innovación han prosperado un gran número de empresas tecnológicas en distintas verticales. Sin embargo, la ciberseguridad es la que ha alcanzado una mayor notoriedad. Este sector es uno de los líderes en las exportaciones de Israel y cada año surgen nuevas ▷

start-ups que revolucionan la manera en la que nos protegemos en el ciberespacio. Esta industria se apoya en tres vértices de un triángulo que veremos a continuación: un fuerte apoyo institucional, un formado capital humano y un ecosistema de negocio favorable.

3.2.1. Ciberseguridad, industria nacional

Israel realizó su apuesta por la ciberseguridad mucho antes que otros países de su entorno. Ya en 1997 se lanzó la iniciativa *Tehila,* destinada a la protección de edificios gubernamentales, y cinco años más tarde se estableció la Autoridad Nacional de Seguridad de la Información (NISA) con el objetivo de proteger infraestructuras críticas frente a ciberataques. La actuación más importante del país, no obstante, fue la creación en agosto de 2011 del National Cyber Bureau, dependiente directamente de la Oficina del Primer Ministro.

Los objetivos principales del *bureau* son la construcción de una estructura defensiva sólida en el ámbito cibernético y posicionar a Israel como líder mundial en el sector de la ciberseguridad. Varios programas del National Cyber Bureau han tenido una repercusión importante, como, por ejemplo, *Kidma,* en colaboración con el Ministerio de Industria, y *Masad,* con el Ministerio de Defensa, que tienen como objetivo promover la industria cibernética israelí.

A comienzos de 2018 se han producido ciertos cambios en la estructura de esta organización. El National Cyber Bureau está en proceso de fusionarse con la National Cyber Defense Authority*,* de reciente creación, y que ofrece servicios complementarios. La organización resultante de la fusión tendrá el nombre de National Cyber Directorate*.*

Igualmente dependiente de la Oficina del Primer Ministro, la ICT Authority (Autoridad Nacional de las TIC) tiene ciertas competencias relativas a la ciberseguridad, especialmente vinculadas a las relaciones entre ministerios y al e-Gov.

Los distintos ministerios del país también disponen de departamentos o especialistas en ciberseguridad aplicada a su campo. Destacan los Ministerios de Asuntos Exteriores, Defensa, Economía, Seguridad Pública, y Ciencia, Tecnología y Espacio.

Mención especial merece la ciudad de Beerseba. Esta ciudad de poco más de 200.000 habitantes situada en el inhóspito desierto del Neguev se ha convertido en un *hub* mundial en ciberseguridad con la presencia de las empresas más importantes del sector. El gran acierto en la creación de este *hub* fue combinar tres visiones distintas en un solo lugar: la académica, la militar y la empresarial. Inaugurado en 2013, el parque tecnológico ATP (Advanced Technologies Park) está cumpliendo todas las expectativas. El estatus especial de Región de Prioridad Nacional (NRP) permite a las empresas instaladas en dicho parque acogerse a exenciones de impuestos e incentivos a la contratación. Grandes corporaciones internacionales de la talla de IBM, Oracle, Paypal o Deutsche Telekom ya se encuentran presentes en el centro. El segundo pilar es la universidad. El ATP está situado dentro del campus de la Universidad Ben Gurion del Neguev, que tiene el honor de ser la primera universidad israelí en incluir estudios relacionados con ciberseguridad. Esta universidad también alberga un competitivo centro de I+D, el BGU Cyber Security Research Center, y la iniciativa Cyberspark, cuyo objetivo es reunir a todos los actores del sector para alcanzar el potencial de la industria. El tercer pilar que consolidará a Beerseba como la capital del *cyber* de Israel es la construcción, en las inmediaciones del campus, ▷

de un centro de I+D en telecomunicaciones por parte del ejército israelí. La construcción de este centro, no obstante, está sufriendo ciertos retrasos.

Por último, el Gobierno de Israel dispone de varios acuerdos con terceros países, como Estados Unidos, Reino Unido o Singapur, para la colaboración en ciberseguridad. Destaca la creación, en julio de 2017, de un grupo de trabajo bilateral en ciberseguridad entre las distintas agencias de inteligencia de EEUU e Israel.

3.2.2. Capital humano

Como se ha comentado anteriormente, una de las claves del éxito de la alta tecnología en Israel es su preparado capital humano. En Israel se encuentran varias universidades con gran prestigio en el campo de la investigación y en el sector de la ciberseguridad; este hecho es especialmente notorio. A la ya mencionada Universidad Ben Gurion se debe añadir la Universidad de Tel Aviv, que cuenta con el Blavatnik Interdisciplinary Cyber Research Center (IDRC), un centro de investigación que además organiza Cyberweek, una de las ferias de ciberseguridad con las que cuenta Israel. Otras universidades relevantes en el campo son la Universidad Hebrea de Jerusalén o el Technion de Haifa.

No obstante, la educación en ciberseguridad no solamente se encuentra en las universidades. El National Cyber Bureau dispone de varias iniciativas destinadas a formar a la población general. El plan con mayor renombre es probablemente el Magshimim Leumit, consistente en ofrecer formación en TIC y ciberseguridad a estudiantes de entre dieciséis y dieciocho años residentes en zonas periféricas de Israel.

Muchos de estos estudiantes, al cumplir los dieciocho años, solicitan servir en la prestigiosa unidad 8.200 del ejército israelí. La «ocho doscientos» es la principal unidad de inteligencia del ejército y la encargada de la ciberseguridad del país en un ámbito militar. Durante el periodo de servicio en esta unidad (el mínimo obligatorio en Israel es dos años para mujeres y tres para hombres) sus integrantes reciben una formación sin par en programación, seguridad informática o criptografía. Gran parte de los emprendedores que han fundado las principales *start-ups* de ciberseguridad de Israel tienen algo en común: su paso por la 8.200. En muchas ocasiones estos jóvenes prescinden incluso de la universidad tras el ejército y directamente ponen en práctica los conocimientos adquiridos en *start-ups* relacionadas con la ciberseguridad. Check Point Software, Imperva o Argus Cyber Security son buenos ejemplos de empresas originadas de este modo.

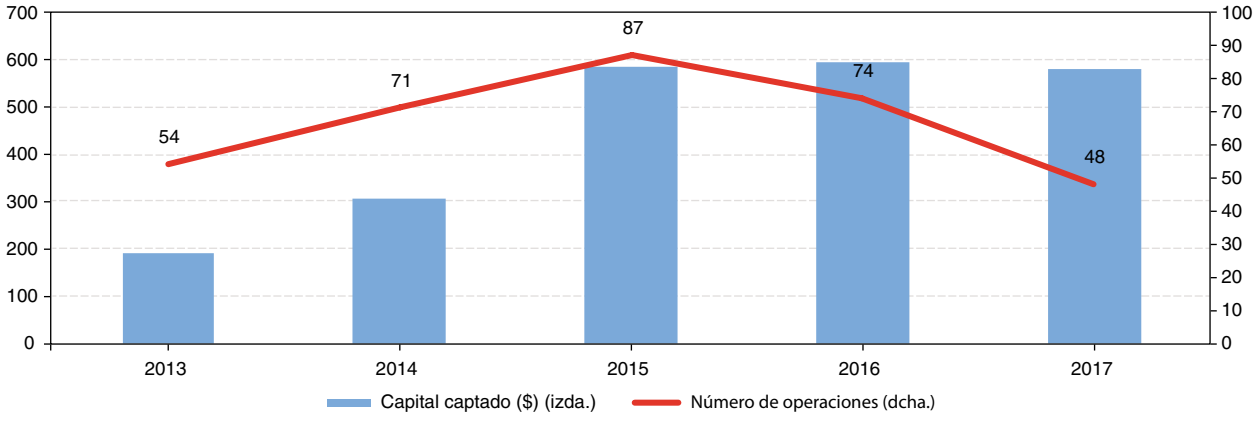
3.2.3. Enfoque empresarial

A diferencia de otros países, donde la ciberseguridad se ha abordado desde las grandes empresas, en Israel la iniciativa se ha originado en las *start-ups*. Existen actualmente entre 400 y 500 empresas dedicadas a la ciberseguridad en el país y en los últimos cuatro años emergen entre sesenta y ochenta compañías nuevas anuales. Condición necesaria para que estas empresas triunfen es el acceso a capital, e Israel tiene uno de los ecosistemas inversores más dinámicos del mundo.

En el año 2016 los fondos de capital riesgo invirtieron 4.800 millones de dólares en las *start-ups* de Israel (la cifra en España en el mismo periodo fue de 579 millones de euros[2]) y esta cantidad habría crecido hasta ▷

[2] Solo se incluyen los fondos captados mediante capital riesgo, otros instrumentos como el *private equity* están aquí excluidos.

GRÁFICO 1
RONDAS DE FINANCIACIÓN EN CIBERSEGURIDAD



Fuente: IVC-Meitar Exit Report 2017.

los 5.240 millones de dólares en 2017, un incremento del 9 por 100. Las inversiones en el sector de ciberseguridad abarcan un porcentaje importante del total: como se puede ver en el Gráfico 1, en los tres últimos años la inversión roza los 600 millones de dólares. En el año 2017 la inversión media por empresa fue de unos 24 millones de dólares.

Observando pormenorizadamente las cifras de inversión se puede comprobar que, a pesar de que la inversión total en ciberseguridad se encuentra estable, se producen menos rondas de inversión. Esto implica que la inversión media por ronda está creciendo. Estudiando en qué fase de la vida de las *start-ups* se produce la inversión, se observa que está disminuyendo en las fases semilla y Serie A (primera inversión significativa), mientras que la inversión en Serie B o en fases de crecimiento está aumentando en gran medida. De esta tendencia se puede obtener la conclusión de que el sector de la ciberseguridad en Israel está entrando en una fase de madurez, en la que se producen menos inversiones pero de mayor tamaño y en empresas más consolidadas. Otro factor que nos da muestras de la madurez en el sector es el valor de sus *exits* (venta de la *start-up* por parte de sus fundadores). En 2017 se ha alcanzado la cifra récord de 1.478 millones de dólares y ha aumentado el precio medio de sus ventas, siendo la más notoria la de Argus Cyber Security, una empresa que protege vehículos frente a *hackeos* por 450 millones de dólares.

El acceso a capital, por tanto, ha incentivado en gran medida la creación de empresas de ciberseguridad. Los fondos de capital riesgo tienen elevados estímulos para la inversión en estas *start-ups,* ya que al tratarse de un sector en fuerte crecimiento (e Israel es un especialista en el campo) las posibilidades de que la empresa triunfe y atraiga la atención de posibles compradores es elevada. En muchos casos, estos compradores son empresas de ciberseguridad extrajeras que adquieren *start-ups* israelíes con el objetivo de introducirse en el país. Un ejemplo reciente es el de Palo Alto Networks, la tercera mayor empresa de ciberseguridad por capitalización bursátil. Esta compañía estadounidense ha comprado en los últimos años dos *start-ups* israelíes: Cybera, por 220 millones de dólares, y Lightcyber, por unos 105 millones. Palo Alto ha anunciado, en ▷

enero de 2018, que usará estas dos adquisiciones como base para ampliar sus actividades de I+D en Israel, centralizándolas en cuatro pisos de un renombrado rascacielos de Tel Aviv.

En Israel hay establecidos alrededor de un centenar y medio de fondos de capital riesgo, a los que se deben sumar veintitrés fondos de grandes empresas que buscan invertir en tecnologías innovadoras para su actividad. Gran parte de estos fondos son nacionales, pero destacan también los fondos de capital riesgo provenientes de EEUU que se instalan en Israel con el objetivo de monitorizar a las *start-ups* del país e invertir en ellas de forma más eficiente.

Gran parte de los fondos de relevancia en el país tiene alguna inversión en empresas de ciberseguridad. Como se ha mencionado anteriormente, esta es la apuesta más «segura», debido a la gran cantidad de casos de éxito que se han dado en los últimos años en el sector. Por otra parte, el alto número de fondos que operan en ciberseguridad provoca que la inversión sea dispersa, es decir, que no haya ninguna firma invirtiendo en un gran número de empresas. El único agrupador es la OCS (Office of the Chief Scientist), que representa a la Autoridad de Innovación Israelí. Este organismo proporciona, bajo varios programas, financiación a las *start-ups.*

Existen, no obstante, varias firmas de capital riesgo que destacan por su volumen de inversiones o número de *exits*. Uno de los fondos más activos en ciberseguridad es Jerusalem Venture Partners. Actualmente tiene inversiones en once empresas del sector y fue inversor en la empresa CyberArk, una de las más exitosas del país y que hoy por hoy cotiza en el NASDAQ. Otro fondo que destaca es YL Ventures, con oficinas en Silicon Valley y Tel Aviv, cuya principal actividad es invertir en empresas de ciberseguridad. OurCrowd, una plataforma de capital riesgo israelí basada en el *crowdfunding* (que recientemente ha desembarcado en España), también posee en su cartera inversiones en seis *start-ups* de ciberseguridad.

Existen, además, dos casos particulares de especial interés, los fondos Team8 y Libertad. Team8 es un fondo de capital riesgo creado en 2015 por varios miembros de alto rango de la unidad 8.200 que invierte solamente en empresas de ciberseguridad israelíes. Financiado por empresas como Microsoft, AT&T, Cisco o Accenture, este fondo es uno de los más prometedores del sector. Libertad Ventures es el nombre del fondo de inversión recientemente creado por el Mossad, la agencia de inteligencia israelí. Aunque todavía se encuentra en una fase inicial, este fondo se dispone a invertir en *start-ups* que innoven en áreas relacionadas con sus actividades, ciberseguridad entre ellas.

3.3. Casos de éxito

El sistema anteriormente descrito ha dado impresionantes resultados, con un gran número de casos de éxito en Israel. A continuación se van a estudiar tres de especial relevancia: Check Point, CyberArk y Argus.

3.3.1. Check Point Software Technologies

La empresa fue fundada en 1993 por Gil Shwed, quien continúa ejerciendo el cargo de CEO hasta la actualidad. Check Point fue pionera en el campo de la ciberseguridad y la primera empresa en comercializar los *firewall* y redes *VPN* como los conocemos hoy en día. Desde entonces la empresa ha batido todos los récords. En agosto de 2017 se convirtió en la mayor empresa de Israel tras el declive de ▷

la farmacéutica Teva. En el campo de la ciberseguridad global también es líder. Check Point es la mayor empresa pura del sector por capitalización bursátil, por delante de Symantec, cuyo valor en enero de 2018 era de casi 17.000 millones de dólares. Actualmente cuenta con unos 4.300 empleados y proporciona un amplio abanico de servicios basados en la seguridad en Internet. Su influencia en el sector, sin embargo, va más allá de estas cifras. Otras dos empresas líderes en sus segmentos guardan una fuerte relación con la compañía: Palo Alto Networks, tercera empresa de ciberseguridad del mundo por capitalización bursátil, fue creada por un antiguo trabajador de Check Point; e Imperva, decimotercera, fue el segundo proyecto de uno de sus cofundadores.

3.3.2. CyberArk Software

Fundada en 1999, CyberArk es una de las empresas de ciberseguridad que más está creciendo actualmente. La empresa ha patentado una tecnología denominada *digital vault,* que ofrece seguridad integral a grandes compañías. El objetivo de CyberArk, por lo tanto, es repeler ataques tanto externos como internos (infiltración) dirigidos contra grandes empresas. Al igual que Check Point, CyberArk nunca aceptó ser comprada (algo poco habitual en las *start-ups* del sector en Israel) y en el año 2014 salió a bolsa. Actualmente es la decimosegunda empresa de ciberseguridad del mundo, con una capitalización bursátil de casi 1.500 millones de dólares.

3.3.3. Argus Cyber Security

Argus es, en muchos sentidos, el arquetipo de la perfecta *start-up* israelí de ciberseguridad. Fundada en 2013 por tres antiguos capitanes de la unidad 8.200, la empresa rápidamente creció y ganó notoriedad hasta llegar a aparecer en el listado «Top 25 Tech Companies to Watch» del *Wall Street Journal.* A principios de noviembre de 2017, Argus fue adquirida por la empresa alemana Continental por unos supuestos 450 millones de dólares. Argus Cyber Security tiene una misión clara: proteger los vehículos conectados frente a ciberataques. Sabiendo que las estimaciones apuntan a que para el año 2020 cientos de millones de coches conectados estarán en circulación, el elevado precio de compra cobra sentido.

4. Oportunidades económicas y comerciales para la empresa española

La ciberseguridad en España se encuentra en un claro crecimiento. Según previsiones de la Unión Europea, el sector puede estar generando más de mil millones de euros al año en España[3] y presenta una tasa de crecimiento de entre el 11 y el 13 por 100 anual. El modo de aproximarse al sector, no obstante, diverge en gran medida del estilo israelí. Los principales pilares de la ciberseguridad en España son los organismos públicos y las grandes empresas, pero ni existe una conciencia colectiva clara relativa a la importancia de la ciberseguridad ni un «campeón nacional». Los organismos públicos de ciberseguridad como INCIBE (Centro Nacional de Ciberseguridad), CNPIC (Centro Nacional de Protección de Infraestructuras y Ciberseguridad) o el CCN (Centro Criptológico Nacional) se encuentran bastante desarrollados, siendo España, por ejemplo, un ▷

[3] No existe una medida exacta de la actividad económica en ciberseguridad.

referente en la protección de infraestructuras críticas. Las grandes empresas también están invirtiendo en el sector, aunque en muchas ocasiones el objetivo es la defensa propia frente a ciberataques, más que el desarrollo de oportunidades de negocio.

En Israel, en cambio, podemos observar un sector ya maduro, cuya base es una amplia red de empresas y *start-ups* sostenidas por un fuerte apoyo institucional, un ecosistema emprendedor favorable y un robusto capital humano. Es esta visión de negocio la que España necesita para no solamente ganar protección frente a ciberataques, sino también para aprovechar el crecimiento de uno de los sectores con mayor potencial hoy en día.

En Israel se celebran tres grandes eventos empresariales vinculados a ciberseguridad: Cybertech y Cyberweek, de carácter anual, y HLS&CYBER, bienal. Además de las mencionadas, es habitual encontrar en el país verticales de ciberseguridad en ferias o eventos de otros sectores, como, por ejemplo, en dispositivos médicos, Smart Cities, Fintech, o movilidad inteligente.

La forma más habitual de beneficiarse de la tecnología israelí, para las grandes empresas, suele ser la apertura de centros de innovación en el país. Intel, IBM, Google, Philips o General Motors son ejemplos de algunas de las empresas que forman los más de 300 centros de I+D que multinacionales extranjeras tienen en Israel. Las ventajas son muchas: el acceso a un preparado capital humano, una buena posición para invertir e incluso adquirir *start-ups* complementarias con la actividad empresarial o unos importantes incentivos gubernamentales que cubren buena parte de los gastos de la empresa en I+D.

En el caso de las *start-ups,* son comunes las estancias en incubadoras o aceleradoras por un periodo de tiempo determinado, que suele oscilar desde un mes hasta programas de uno o dos años. Son también accesibles programas de inmersión profunda en el ecosistema israelí que permitan adquirir la globalidad con la que trabajan las entidades en Israel. Los programas de mayor duración suelen exigir, no obstante, algún vínculo de la empresa con Israel como, por ejemplo, la colaboración con otra *start-up* local para el acceso al mercado de origen.

Israel es un gran modelo de innovación que ve a España como una puerta hacia Europa y Latinoamérica. La colaboración desde la base, mediante los propios intercambios de corte científico o la cooperación tecnológica de aplicación industrial, son otras vías para construir una relación económica y comercial futura entre empresas de España e Israel.

5. Conclusiones

Israel ha construido uno de los ecosistemas más innovadores y dinámicos en alta tecnología, y la ciberseguridad es su punta de lanza. Ciberseguridad entendida como una estrategia que da solidez a la actividad económica y no solamente como una inversión sin retorno. Un fortísimo apoyo institucional, capital humano muy preparado y un ecosistema empresarial e inversor muy dinámico siembran las bases del éxito del sector. La ciberseguridad es uno de los campos en los que se espera un mayor crecimiento en el futuro y las empresas israelíes están aprovechando esta tendencia, exportando más de 3.000 millones de dólares cada año en bienes y servicios vinculados.

Los casos de éxito son numerosos: Check Point, CyberArk, Imperva, Argus…; todas estas empresas se originaron en Israel como *start-ups* y actualmente se encuentran entre los líderes ▷

del sector, con miles de trabajadores repartidos por sus oficinas en todo el mundo. En España, merece la pena plantearse a Israel como socio natural para generar conocimiento y transferencia de tecnología, más aún ahora, cuando la tendencia estratégica en Israel es de renovación, trasladando su eje de desarrollo económico desde el concepto *Start-up Nation* al de crecimiento económico plenamente basado en la innovación.

Bibliografía

[1] ASCRI (2017). *Inversión en Start Up´s en España en 2016. La visión del Venture Capital.* Disponible en: *https://www.ascri.org/wp-content/uploads/2017/06/Estudio-inversion-Start-ups-2016-Ascri-CaixaBank.pdf* [Recuperado: 2018, 12 de enero].

[2] GALINDO RODRÍGUEZ, C. (2015). *Ciberseguridad en Israel.* CDTI, julio de 2015.

[3] CYBERSECURITY VENTURES (2017). *Cybersecurity 500*. Disponible en: *https://cybersecurityventures.com/cybersecurity-500/* [Recuperado: 2018, 10 de enero].

[4] GARTNER (2017). *Business Impact of Security Incidents and Evolving Regulations Driving Market Growth*. Disponible en: *https://www.gartner.com/newsroom/id/3784965* [Recuperado: 2018, 7 de enero].

[5] ICT AUTHORITY (2016). *Strategic Plan 2016-2018.* Disponible en: *https://www.gov.il/blobFolder/generalpage/stratigy_eng/he/STRATIGY- por 10020ICT por 10020ATHORITY por 10020- por 10020ENGLISH.pdf* [Recuperado: 2018, 15 de enero].

[6] INVEST IN ISRAEL (2016). *R&D Centers, Investment Models in Israel*. Disponible en: *http://www.investinisrael.gov.il/resources/2017/R_D.pdf* [Recuperado: 2018, 18 de enero].

[7] ISRAEL EXPORT INSTITUTE (2018). *Israel´s Cyber Security Sector Overview*. Disponible en: *http://www.export.gov.il/files/cyber/CyberPresentation.pdf?redirect=no* [Recuperado: 2018, 7 de enero].

[8] OECD (2016). *Gross domestic spending on R&D*. Disponible en: *https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm* [Recuperado: 2018, 8 de enero].

[9] OFICINA ECONÓMICA Y COMERCIAL DE LA EMBAJADA DE ESPAÑA EN TEL AVIV (2017). *El mercado del capital riesgo en Israel*. Disponible en: *www.icex.es* [Recuperado: 2018, 10 de enero].

[10] START-UP NATION CENTRAL (2017). *Finder Insights Series, Israel´s Cybersecurity Industry in 2016*. Disponible en: *https:///lp.startupnationcentral.org/cybersecurity-industry-report/* [Recuperado: 2018, 18 de enero].

[11] THE TIMES OF ISRAEL (2017). *Prime minister appoints new cybersecurity chief*. Disponible en: *https://www.timesofisrael.com/prime-minister-appoints-new-cybersecurity-chief/* [Recuperado: 2018, 15 de enero].

[12] THE WHITE HOUSE (2017). *Remarks by Homeland Security Advisor Thomas P. Bossert at Cyber Week 2017*. Disponible en: *https://www.whitehouse.gov/briefings-statements/remarks-homeland-security-advisor-thomas-p-bossert-cyber-week-2017/* [Recuperado: 2018, 15 de enero].

[13] UNESCO INSTITUTE FOR STATISTICS (2017). *How much does your country spend in R&D?* Disponible en: *http://uis.unesco.org/apps/visualisations/research-and-development-spending/* [Recuperado: 2018, 8 de enero].

[14] YL VENTURES (2018). *The 2017 State of the Cyber Nation*. Disponible en: *https://techcrunch.com/2018/01/14/the-state-of-israels-cybersecurity-market/* [Recuperado: 2018, 18 de enero].