La industria de la Ciber-seguridad en Israel

Noviembre del 2016

Observatori de Drets Humans i Empresa
Nord d'Àfrica i Orient Mitjà

Abstract

Entre el 14 y 17 de noviembre se ha organizado **en Tel Aviv la 4ª Conferencia Internacional sobre Seguridad Nacional y Ciber-seguridad**[1] **,** cita a la que han asistido agencias de seguridad gubernamentales y empresas de todo el mundo atraídas por la industria militar y securitaria israelí . Cataluña no es una excepción. **La Agencia para la competitividad de la empresa de la Generalitat de Cataluña, ACCIÓ, ha preparado durante los últimos meses una misión comercial[2] que promomueve la participación catalana en esta conferencia** con el objetivo de crear lazos de cooperación empresarial e institucional en este campo. Esta misión empresarial encaja -según ACCIÓ[3] - con la línea estratégica del Gobierno para hacer crecer y potenciar el sector catalán de la ciber-seguridad 'como un sector económico dinámico con una proyección de futuro altamente positiva'. Cada una de las 8 empresas o entes tecnológicos catalanes participantes en esta misión empresarial recibirán o han recibido una ayuda financiera de € 760.28 como bolsa de viaje.

El Gobierno de Israel es el principal promotor de esta conferencia ya que este sector es clave para la economía del país. Hay aproximadamente 250 empresas de ciber-seguridad que operan en Israel[4], que han captado 500 millones de dólares durante el 2015 y que ya suman más de 200 millones de dólares captados durante los primeros dos meses de 2016[5]. **En 2014 las ventas mundiales de las empresas ciber israelíes ascendieron a 6 mil millones de dólares**. Esta cifra representó aproximadamente el **10% de todas las ventas mundiales del sector**. Se calcula que hay 16.000 profesionales cibernéticos en Israel (empresarios y personal contratado), tanto en el sector de la defensa como en el sector privado. Una de las claves principales de este éxito internacional es su capacidad de innovación, una ventaja comparativa basada en la estrecha relación que existe entre la industria militar y de seguridad tecnológica y las Fuerzas Armadas de Israel.

Este sistema se alimenta y justifica por el mantenimiento de la ocupación en Palestina y las tensiones con el Líbano, Siria y otros países árabes, así como por la proliferación de actores armados no estatales en la región. Los territorios ocupados palestinos son un verdadero laboratorio donde corporaciones privadas, centros de investigación, incluyendo universidades y el ejército prueban nuevas armas y sistemas tecnológicos de seguridad para luego incorporarlos al mercado global. La marca "Made in Israel" anuncia frecuentemente esta experiencia probada en "combate", pero obvia el grave impacto en la sociedad civil y las violaciones sistemáticas de derechos humanos de la población palestina que cometen.

Este documento tiene por objetivo identificar los riesgos y potenciales violaciones del derecho internacional y los derechos humanos que implica invertir en Israel a través del análisis de: 1) las nuevas políticas de seguridad globales; 2) la investigación europea en Homeland Security y la participación israelí; 3) las relaciones entre la industria militar y de seguridad tecnológica con las Fuerzas Armadas de Israel; 4) Complicidades con la ocupación en Palestina; 5) Recomendaciones a las instituciones y empresas catalanas.

1 https://www.israelhlscyber.com/
2 http://accio.gencat.cat/cat/empresa-ACC1O/premsa/noticies-notes-premsa/2016/israel_ciber-seguretat.jsp
3 http://accio.gencat.cat/cat/empresa-ACC1O/premsa/noticies-notes-premsa/2016/israel_ciber-seguretat.jsp
4 Embassy of India, Tel Aviv | The Cybersecurity Sector in Israel 2015 | http://www.indembassy.co.il/pages.php?id=6666700#.WB-QjiR-iVA
5 http://accio.gencat.cat/cat/empresa-ACC1O/premsa/noticies-notes-premsa/2016/israel_ciber-seguretat.jsp

Nuevas políticas de seguridad: Homeland Security, ciber-seguridad y privatización de la Seguridad

Los ataques del 11 de septiembre de 2001 en Estados Unidos no sólo sirvieron como justificación para bombardear y ocupar Afganistán en 2001 e Irak en 2003, sino que también permitieron imponer una nueva política de Homeland Security que reforzaba los poderes del Gobierno para **neutralizar las amenazas internas del país** y contribuyó a la explosión, en términos económicos, de las empresas militares y de seguridad privada, y la industria de la seguridad tecnológica. El desarrollo del complejo industrial de la Homeland Security evolucionó paralelamente al incremento de la demanda en seguridad, una demanda basada en la creación de un sentido de peligro en la sociedad especialmente presente durante la Administración de Bush[6]. Desde entonces, el gasto en seguridad nacional no ha parado de crecer en todo el mundo; se estima que **solo en 2009 los gobiernos gastaron alrededor de 141.600 millones de dólares en servicios de "Homeland Security"**[7].

El concepto de "Homeland Security" trabaja sobre la evaluación, mitigación y gestión de las amenazas en el interior de las sociedades, incluyendo las fronteras. Los actuales modelos de Homeland Security se parecen a los esquemas "Full Spectrum Dominance" típico de las lógicas de combate, es decir, el control de todos los elementos de la batalla: mar, aire, tierra y ciber-mundo. En la práctica las políticas de Homeland Security englobarían la protección de fronteras, infraestructuras críticas (plantas nucleares, aeropuertos, edificios gubernamentales, puertos, etc.), macro-eventos (incluyendo manifestaciones), ciber-seguridad, ciber-crimen, gestión de emergencias, tecnologías de la vigilancia, etc.

> El concepto de 'Homeland Security implica la securitización de las sociedades para neutralizar las amenazas internas. Cooperan en ello agentes policiales con el ejército y agentes de seguridad privada.

Ante el nuevos retos para asegurar la seguridad, actores políticos afirmaron que los Estados no tenían suficientes capacidades para dar respuesta a estos retos y que necesitaban de la participación de corporaciones privadas en este sentido. Franco Frattini, ex-vicepresidente de la Comisión Europea afirmó en la conferencia europea sobre investigación en el sector de la seguridad de 2007 que **la seguridad, como bien público, ya no es sólo responsabilidad del Estado, sino que debe ser compartida por actores privados**[8].

Estas palabras atestiguaban una realidad que ya había comenzado años atrás, concretamente en 2003 en Irak, pero que ahora se extendía también a los ámbitos de la seguridad nacional: la privatización de la seguridad y la guerra.

En efecto**, la ocupación de Irak fue el gran escenario de la privatización de la guerra donde muchas empresas militares y de seguridad privada proliferaron**. El director general de la Asociación Británica de Empresas de Seguridad Privada, Andy Bearpark, hacía estas declaraciones durante una entrevista en 2010: "en Irak en 2003 y 2004 el dinero era básicamente gratis, esto significaba que los contratos se adjudicaban por ridículas cantidades de dinero -millones y millones de dólares en contratos fueron bombeados en la industria"[9].

En la práctica, **la privatización de la guerra y la seguridad implica la transferencia de funciones inherentes a los Estados a manos privadas**. Actividades propias del principio del monopolio legítimo del uso de la fuerza y que tradicionalmente ejecutaban los Cuerpos y Fuerzas de Seguridad del Estado bajo la lógica del escrutinio democrático y público. Ahora, empresas militares y de seguridad privada, incluyendo empresas tecnológicas, realizan funciones de orden público, formación de policías, gestión de prisiones, control de fronteras, servicios de inteligencia, entre otras. Concretamente, la participación de corporaciones privadas que se guían por lógicas lucrativas en funciones de inteligencia para la seguridad nacional son doblemente preocupantes: por un lado, supone el acceso, captura y tratamiento de millones de datos de carácter personal con los potenciales abusos de derechos humanos que puede suponer; y por otra parte, la definición de las amenazas y el nivel de riesgo de las mismas. La autora Lou Pingeot en su análisis sobre la política de contratación de Naciones Unidas del servicios de empresas militares y de seguridad, concluye que las empresas privadas terminan definirndo la propia política de seguridad del cliente. Según Pingeot,

---

[6] KLEIN, N., The Shock Doctrine. London: Penguin, 2007, p.306

7 TRANSNATIONAL INSTITUTE, NeoConOpticon. The EU Security-Industrial Complex, p.4

[8] Speech of Franco Franttini 'Security by desing' in the EU Security Research conference in Berlin, 26/03/2007. Disponible: http://europa.eu/rapid/press-release_SPEECH-07-188_en.htm Fecha consulta 20/10/2016

[9] "The rise of the UK's private security companies" BBC News, 02/11/2010. Disponible en http://www.bbc.com/news/business-11521579 Fecha de la consulta 20/10/2016

las empresas militares y de seguridad privada realizan análisis y gestión de riesgos que marginalizan las dinámicas sociales y políticas de contextos, priorizan las respuestas "hard security" por encima de acciones de mediación o construcción de paz, ya que son áreas que escapan de su experiencia y por tanto, no podrían continuar renovando sus contratos[10].

Por lo tanto**, existe un alto riesgo de que las corporaciones del ámbito de seguridad distorsionen el nivel de los riesgos de amenazas a su favor**. Un ejemplo claro, sería el último informe sobre riesgos globales de la empresa militar y de seguridad privada Control Risks. En este informe Control Risks afirma que el Cuerno de África es una las regiones más peligrosas para el transporte marítimo[11]. A pesar de que a principios de año la principal Asociación de Seguridad Marítima del mundo (SAMI), anunciaba su fin afirmando que las amenazas de piratería habían desaparecido en aquellas regiones y como consecuencia muchas empresas de seguridad marítima habían cerrado produciéndose la caída en picado de los miembros de la Asociación.[12].

La investigación europea en Homeland Security

En 2003, la Unión Europea encomendó al Grupo de Personalidades (GoP en su acrónimo en inglés) definir las líneas estratégicas del "Programa Europeo de Investigación en Seguridad" (ERSP). Este grupo estaba formado por los Comisarios Europeos de Investigación y Sociedad de la Información, Relaciones Exteriores y Comercio, el Alto Representante de la UE de la Política de Asuntos Exteriores y Seguridad; representantes de la OTAN, la Asociación deArmamento del Oeste de Europa, el Comité Militar de la UE, 8 empresas multinacionales del sector armamentístico (EADS, BAE Systems, Thales, Leonardo Finmeccanica) y las más grandes empresas del sector tecnológico (Ericsson, Siemens, Diehl e Indra), así como centros de investigación como Rand Corporation. Destaca la total ausencia de la Organización Internacional para las Migraciones, la Agencia de Naciones Unidas para los Refugiados u organizaciones de la sociedad civil especializadas en los conflictos y las dinámicas político-sociales de las regiones vecinas de la UE. Como consecuencia, 3 de las compañías participantes en este Grupo son los mayores beneficiarios del ERSP. Es por tanto, obvio **como las corporaciones privadas están definiendo la política de seguridad de la Unión Europea y dando respuestas que están contribuyendo a la militarización de las fronteras** y por lo tanto, requieren de su propia contratación por parte las instituciones europeas y sus Estados miembros.

> Las corporaciones privadas están definiendo la política de seguridad de la Unió Europea y ofreciendo respuestas que contribuyen a la militarización de las fronteras.

Israel es el único país no europeo que participa en los programas de financiación de la UE para la investigación. Durante el anterior programa de investigación europeo (FP7) de 2007-13, actores públicos y privados de Israel participaron en 1.500 proyectos [13]. En el ámbito de investigación en seguridad, la UE ha canalizado 26 millones de euros a través de 49 proyectos de investigación directamente al sectores de defensa y seguridad del Estado de Israel. 23 empresas israelíes se han beneficiado de este programa incluyendo a Elbit Systems, Israel Aerospace Industries (IAI), Aeronautics. Defence Systems y Opgal Optronics Industries[14]. Sólo Elbit Sytems y IAI recibieron 393.900.149,00 euros, una gran mayoría de ellos destinados a la desarrollar drones[15]. En el actual programa europeo Horizon 2020, Israel participa en un total de 576 proyectos[16] de los cuales 18 son en el ámbito de la Seguridad[17].

El interés de Israel en estos programas es clave ya que gana acceso a proyectos y conocimiento; le permite trabajar en red con universidades y empresas europeas; y avanzar económicamente la investigación académica en el país. Pero ¿qué interés tiene la UE en colaborar con un aliado como Israel?

Israel es un referente en seguridad, no sólo por el alto desarrollo de su industria, sino porque cristaliza el modelo de economía de la vigilancia de 'Homeland Security' que han ido adquiriendo los países occidentales. Pero hay que tener en cuenta de qué manera Israel ha adquirido este estatus internacional: todo este 'know how' procede de la política de ocupación y el intento de vigilar y controlar la población palestina. 'Made in Israel' se ha convertido en

[10] PINGEOT, L., Dangeous Partnership, 2012
[11] Ver RiskMap 2016 de ControlRisks, disponible a: https://riskmap.controlrisks.com/ (visitat el 9/10/2016)
[12] Disponible en https://maritimecyprus.com/2016/04/19/the-security-association-for-the-maritime-industry-sami-announces-voluntary-liquidation/
13 http:/ /europa.eu/ rapid/press_release IP_14_633 en.htm
[14]http://www.vrede.be/english/69_news/1314_european_commission_confirms_millions_of_eu_research_money_flows_to_israeli_arms_industry
15 http:/ /cordis.europa.eu/projects/ home en.html
16 http://www.iserd.org.il/?CategoryID=443
[17] http://www.iserd.org.il/?CategoryID=443

garantía de servicios o productos 'probados en combate', hasta el punto que es común encontrar CEO de empresas que así lo exponen en entrevistas y conferencias, como marca de calidad. Un ejemplo es Saar Koursh, CEO de la empresa israelí Magal Security Systems Ltd. que en una entrevista afirmó recientemente: "Cualquiera puede mostrarle un buen powerpoint, pero pocos podran enseñarle un proyecto tan complejo como Gaza que está constantemente probado en batalla" [18].

Como explica el informe NeoConOpticon del Transnational Institute "a pesar de su existencia hiper-militarista 'y sus' gastos desmesurados en acuerdos ilegales, carreteras ilegales, el muro ilegal y por supuesto, la ocupación ilegal, Israel, mediante el mantenimiento de los símbolos de la democracia liberal moderna, ha conseguido posicionarse como el Estado de la Seguridad nacional por excel·lència"[19] (p.12)

Algunos de los proyectos más relevantes en el marco de la seguridad nacional con participación israelí y española son:

- GLOBE (2008, FP7): para la lucha contra todo tipo de inmigración ilegal desde cualquier ámbito, liderado por Telvent y la participación de Indra [20]. Telvent aporta el sistema de vigilancia marítima AMASS con participación de IAI [21].
- TALOS (2008-12): Desarrollo de un nuevo sistema de protección de las fronteras europeas mediante el uso de vehículos no tripulados, con la participación de IAI, la empresa española TTI y la colaboración con agentes españoles de seguridad pública[22]
- CAPER (2011-14, FP7): creación de una plataforma virtual para la prevención y detención del crimen organizado mediante el uso de las tecnologías de la información, con la participación del Ministerio de Seguridad Pública de Israel, Technion - Israel Institute of Technology, Consejería de Interior de la Generalidad de Cataluña, Guardia Civil Española, Universidad Autonoma de Barcelona, S21sec Information Security Labs SL, entre otros.
- DESURBS (2011-14, FP7): análisis y diseño de herramientas para la detección de amenazas a la seguridad en espacios urbanos. Las ciudad de Jerusalén, Nottingham y Barcelona servirán como casos de estudio de referencia. Participantes: The Hebrew University of Jerusalem, Bezalel Academy of Arts and Design y el Centro Internacional de Métodos Numéricos en Ingeniería.
- EUROSUR - SeaBILLA (2010-14, FP7): Diseño de un nuevo sistema de vigilancia de fronteras marítimas Europeas que integre el control espacial, aéreo, terrestre y marítimo. El proyecto pretende crear una cooperación efectiva entre los diversos Estados miembros en la lucha contra el tráfico de drogas en el Canal de la Mancha, la inmigración ilegal el sur del Mediterráneo y las actividades consideradas ilícitas en aguas del Atlántico desde de las Islas Canarias hasta las Azores. Participantes: Indra, Universidad de Murcia, TTI Norte SL., Eurocopter España S.A., y la empresa israelí Correlation Systems.
- FOCUS (2011-13, FP7): Diseño de una estrategia de investigación en el ámbito de la seguridad europea. El objetivo central es poder analizar el rol de la UE dentro de los nuevos retos derivados de los riesgos y de las amenazas en un mundo globalizado (tales como ataques a ciudadanos europeos o en infraestructuras consideradas críticas). Participantes: University of Haifa, Atos Apsin SA, INTA, Inge de Sistemas para la Defensa de España.
- FORENSOR (2015-18, H2020): orientado a la creación de sensores inteligentes, miniaturizados, de bajo costo, inalámbrico, autónomo para la recopilación de pruebas. El sensor incluirá una cámara ultra-sensible y intelinteligencia integrada que permitirá operar en ubicaciones remotas, identificar automáticamente eventos criminales predefinidos, alertar en tiempo real, y almacenar la evidencia relevante en vídeo, ubicación y tiempo. Participantes: Emza Visual Sense (Israel), Policía Local de Valencia y otras entidades públicas y privadas de la UE.
- LAW TRAIN (2015-18, H2020): Diseño de una plataforma tecnológica para unificar las metodologías para interrogatorios. Unidades de policía practicarán la interrogación con sospechosos en entornos de realidad virtual. Participantes. Israeli Bar Ilan Univeristy, Ministerio de Seguridad Pública de Israel, compedio Software & Hardware Development Ltd., Ministerio de Justicia de Portugal, Ministerio de Justicia de Bélgica, Ministerio de Interior de España, Optimización orientada a la Sostenibilidad, Inesco-ID, USECON, University of Leuven.

Es importante destacar que la investigación europea permite el desarrollo de tecnología que posteriormente es ofrecida a los Estados y otras agencias de seguridad. Esto es especialmente visible en los proyectos donde participan entidades israelíes donde se incluyen demostraciones de proyectos, donde los prototipos de sistemas de seguridad son manufacturados y probados; e infraestructura de proyectos, por ejemplo sistemas de comunicación,

18 http://www.bloomberg.com/news/articles/2016-08-01/israel-s-magal-eyes-trump-wall-boasting-gaza-tested-smart-fence
19 Transnational Institute, NeoConOpticon, 2009, pp19
20 Per més informació veure: http://cordis.europa.eu/project/rcn/88217_es.html
21 Per más información veure: http://www.2020-horizon.com/GLOBE-European-Global-Border-Environment(GLOBE)-s13095.html
22 Per més informació veure: http://talos-border.eu/index.php?option=com_content&view=article&id=53&Itemid=61

infraestructuras críticas y capacidad de gestión de crisis. Estos proyectos están claramente destinados a la compra pública[23].

Esto entra en contradicción con el compromiso de la Unión Europea[24] de no financiar a través de estos programas proyectos que tengan aplicaciones de doble uso militar, dado que muchas de las empresas que participan en estos programas forman parte del complejo industrial israelí de seguridad militar y de seguridad interna. El Programa Horizon2020 lo deja bien claro[25] "Sólo las actividades de investigación e innovación que se centran en aplicaciones civiles son elegibles para la financiación en Horizon 2020. La investigación destinada a ser utilizada en aplicaciones militares, no se puede financiar por el programa marco". También lo define el documento de la Comisión Europea de ética para investigadores del programa FP7[26]. Sin embargo, la investigación y desarrollo propuesto para muchas de estas empresas implica inevitablemente el doble uso militar de la tecnología y el conocimiento, dado que están profundamente implicadas en las violaciones israelíes del derecho internacional.

Por poner un ejemplo vinculado con el doble uso de la industria de la vigilancia, en 2014 salió a la luz un caso de escuchas por parte de reservistas de la unidad 8200 que recibieron órdenes de vigilar a población civil palestina[27] Según declaraciones de un grupo de reservistas, algunos de ellos veteranos, que denunciaron esta pràctica, el personal recibió instrucciones de registrar cualquier detalle nocivo de la vida de los palestinos que vigilaban, incluyendo información sobre preferencias sexuales, infidelidades, problemas financieros o enfermedades familiares que podrían ser "utilizadas para extorsionar a la persona y convertirla en colaboradora".

Relaciones entre la industria militar y de seguridad tecnològica con las Fuerzas Armadas de Israel

Israel se encuentra entre los 10 países mayores exportadores de armas del mundo. Su industria armamentística tiene una fuerte dependencia del mercado global. Al menos ¾ de su producción se exporta, lo que permite reducir los gastos de su producción interna. **El sector de la tecnología securitaria representa una cuarta parte del total de exportaciones de Israel, alrededor de 25 millones de dólares durante el 2014**. Sólo en 2014 se crearon 20 centros de Investigación y Desarrollo establecidos por empresas multinacionales en Israel para desarrollar soluciones de seguridad para el mercado global. **Israel destina más del 4% de su PIB a la investigación y desarrollo** [28], investigación que se desarrolla en partenariado con el mundo académico y la empresa, una fórmula que les permite tener una tasa de patentes anual muy elevada, una ratio de 250 aproximadamente por millón de habitantes al año[29]

El Gobierno Israelí juega, por tanto, un rol clave en la promoción del entramado de la economía de la seguridad. En el 1993 el programa Yozma[30] permitió la atracción de algunos de los mayores fondos de capital riesgo de Estados Unidos y otros países para invertir en empresas israelís. Este programa ha permitido financiar proyectos y empresas del sector de la tecnología e innovación en general y la securitaria en particular.

Se calcula que hay 16.000 profesionales cibernéticos en Israel (empresarios y personal contratado, tanto en el sector de defensa como en el sector privado que se distribuyen en arquitectos y consultores, sistemas SCADA, malware e ingeniería inversa[31]. Los empresarios cibernéticos en Israel provienen de una variedad de backgrounds profesionales: Fuerzas Armadas Israelíes y agencias de seguridad (25%); profesionales de alta tecnología y hackers (22%); profesionales de empresas líderes de telecomunicaciones (18%), otros empresarios (12%) ; académicos y profesores universitarios (6%).

23 Transnational Institute, NeoConOpticon, 2009, pp19
24 http://horizon2020projects.com/global-collaboration/israel-boycott-petition-receives-irish-support/
25 http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-civil-apps_en.pdf
26 http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf
27 https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories
28 https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm
29 http://reports.weforum.org/global-competitiveness-index/competitiveness-rankings/#series=PCTPATENTAPPLPC
30 http://www.yozma.com/home/
31 Embassy of India, Tel Aviv | 2015 | The Cybersecurity Sector in Israel http://www.indembassy.co.il/pages.php?id=6666700#.WB-QjiR-iVA

Fuente: Informe del sector de la ciber-seguridad de la Embajada de la India, Tel Aviv[32]

El ejército israelí ha sido una pieza fundamental en el proceso de desarrollo de la industria Homeland Security y tecnología de la seguridad. Concretamente, la Unidad 8200 de los Cuerpos de Inteligencia de las Fuerzas de Defensa de Israel. La misión de la Unidad es la captación de señales de inteligencia y descifrado de códigos. **La unidad 8200 funciona como una incubadora tecnológica donde se forman los futuros directivos de las start-ups de seguridad de Israel**. Primero, se realiza una búsqueda de talentos en las escuelas secundarias del país para luego incorporarlos a la unidad donde se aprovecha la más avanzada tecnología SIGINT (Inteligencia de señales), utilizan técnicas sofisticadas de minería de datos, y conciben tecnologías altamente avanzadas. Compañías clave del sector de la seguridad como Checkpoint, Imperva, Nice, Gilat, Waze, Trusteer, Wix o Fortscale tienen sus orígenes en la Unidad 8200.

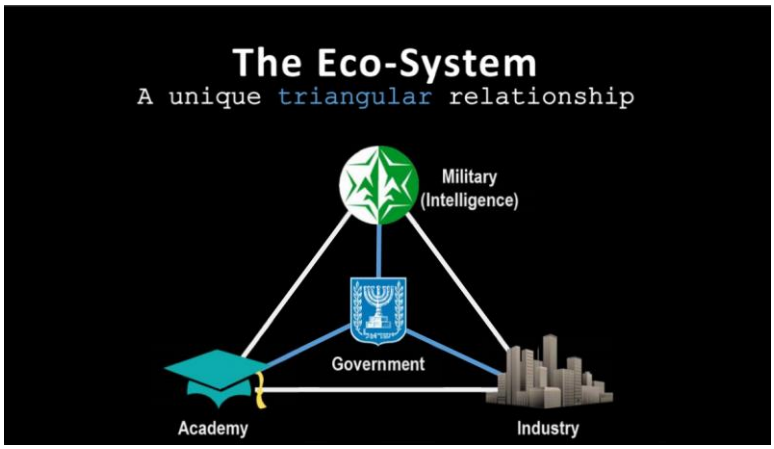
También cabe destacar la **División Tecnológica Lotem-C4I** de las Fuerzas Armadas Israelíes que se encarga de la gestión de los campos de batalla virtuales y ciber-espionaje. Desde 2012, la División se enfoca en la lucha contra el terrorismo a través de la formación de ciber-comandos contra países hostiles a Israel como Irán y sus aliados. Uno de sus logros fue el lanzamiento del virus Flame[33] que afectó en 2012 los sistemas informáticos que controlan la industria petrolera de Irán.

Complicidades con la ocupación de Palestina

El complejo industrial israelí de seguridad militar y de seguridad interna, la inteligencia militar, el Gobierno y las universidades conforman un ecosistema colaborativo que tiene como inevitable consecuencia el doble uso de la tecnología de la ciber-seguridad y de defensa. Por un lado, gran parte de estas empresas proporcionan su tecnología y saber al ejército israelí y el Ministerio de Defensa.

Por otra parte, **hay todo un sistema de "puertas giratorias" entre las unidades israelíes de élite militar como la unidad 8200 y el sector privado**, beneficiándolo directamente de la tecnología y los conocimientos adquiridos en los abusos sistemáticos contra los derechos humanos y los crímenes de guerra cometidos por estas unidades. Por poner un par de ejemplos ilustrativos de estas puertas giratorias: El fundador de Verint es Jacob "Kobi" Alexander[34], el ex oficial de la inteligencia israelí; uno de los directores de Natural Speech Communication (NSC) es el ex jefe del Mossad, Shabtai Shavit[35].

32 The Cybersecurity Sector in Israel http://www.indembassy.co.il/pages.php?id=666700#.WB-QjiR-iVA
33 https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html
34 http://www.forbes.com/sites/jwebb/2016/08/24/fugitive-ceo-kobi-alexander-indicted-to-us-after-decade-on-the-run/#1386of7a1e09
35 http://www.iaesi.org.il/Eng/?CategoryID=329&ArticleID=918



Fuente: Israel Export Institute[36]

Algunos ejemplos de empresas que participan de la complicidad con la ocupación:

Israel Aerospace Industries (IAI) es una de las empresas pioneras en la tecnología de drones y la primera en lanzar un dron de vigilancia[37]. Pero también ha sido una de las empresas que más se ha beneficiado de la ocupación. El modelo Heron 1 y Heron TP de IAI son frecuentemente utilizados sobre Territorios ocupados Palestinos y especialmente sobre la Franja de Gaza. Son drones con capacidad de lanzamiento de proyectiles, concretamente hasta 4 misiles Spike. Según Human Rights Watch, Israel habría utilizado drones Heron de IAI y Hermes de Elbit Systems, equipados con misiles Spike y otros sobre Gaza[38]. Pero también con funciones de vigilancia e identificación de objetivos. Existen evidencias de que aseguran que los drones Heron 1 fueron utilizados durante la Operación Lluvia de Verano de 2006 sobre Gaza donde murieron más de 400 palestinos/as[39]. En 2008 durante la Operación Plomo Fundido sobre Gaza, con más de 1330 palestinos/as muertos se volvieron a utilizar drones de IAI, modelo Heron TP. Los drones precedieron la entrada de la infantería israelí, limpiando el área y neutralizando objetivos con misiles[40].

Elbit Systems es junto con IAI una de las principales empresas pioneras y líderes del sector de la seguridad en general y el desarrollo de drones en particular. La tecnología de Elbit utiliza el muro de separación a través sistemas de detección de intrusos. El producto "Torch" está manufacturado específicamente para ser utilizado en el Muro de Incautación. También produce vehículos armados a control remoto para vigilar zonas alrededor del Muro. En los asentamiento ilegales de Ariel y Ar Ram en Cisjordania, Elbit y sus subsidiarias proveen del sistema de vigilancia de cámaras LORROS. Elbit es también uno de los principales proveedores de sistemas de seguridad en las Fuerzas Armadas Israelíes por ejemplo mejorando la tecnología de los F-16 israelíes o los tanques Merkava. También provee de barcos controlados de forma remota que han sido utilizados en las costas de Gaza. Por último, los drones armados Hermes 900 de Elbit fueron utilizados durante el ataque a Gaza de 2014.

Según un informe de 2015 del grupo de vigilancia basado en la Unión Europea Privacy International, la empresa israelí **Verint Systems Inc**. suministró hardware y software para funciones de espionaje en líneas fijas y móviles de telefonía, así como redes de internet a los Gobiernos de Kazhastan y Uzbekistán[41] que fueron finalmente utilizados para identificar y capturar opositores a los Gobiernos. Privacy International también relaciona a la empresa Verint con el escándalo de las escuchas de la NSA[42]

Nikuv International estuvo presuntamente implicada en la manipulación de listas de votantes y resultados finales de las elecciones en Zimbabwe favoreciendo la reelección del Mugabe y su partido PF [43].

36 http://www.export.gov.il/files/cyber/CyberPresentation.pdf?redirect=no
37 EL primer dron de vigilància és va llençar l'any 1979 sota el nom de Scout
38 HRW, Report Precisely Wrong, Disponible a: https://www.hrw.org/report/2009/06/30/precisely-wrong/gaza-civilians-killed-israeli-drone-launched-missiles
39 Drone Wars UK, Israel and the Drones War. Examining Israel's production, use and proliferation of UAVs, 2010, pp.10
40 Ídem., pp.11.
41 https://www.privacyinternational.org/node/429
42 https://www.privacyinternational.org/node/61
43 http://www.diamondintelligence.com/magazine/magazine.aspx?id=12033

NSO Group Technologies fabricó Pegasus, un malware que permite el monitoreo remoto y la extracción completa de datos de los Iphone. Según Privacy Internacional, organización que se dedica a la denuncia de violaciones de privacidad por parte de los Estados y empresas, Pegasus podría haber sido utilizado[44] por Emiratos Árabes Unidos, Turquía, Israel, Tailandia, Qatar, Kenia, Uzbekistán, Mozambique, Marruecos, Yemen, Hungría, Arabia Saudí, Nigeria y Bahrein.

[44] http://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#e9c6464e3d65

Recomendaciones a las instituciones y empreses catalanas

A la luz de las informaciones anteriores, invertir o colaborar con la industria militar, la seguridad privada y la seguridad tecnológica de Israel implica potenciales violaciones del derecho internacional y los derechos humanos, dado que es una industria basada en la experiencia de la ocupación de Palestina y la infraestructura de apartheid en Cisjordania y la Franja de Gaza.

Para evitar complicidades con las graves violaciones de derechos humanos y del derecho internacional humanitario; y con espíritu del fomento de la paz y de la transformación pacífica de los conflictos, el Observatorio de Derechos Humanos y Empresas del Norte de África y Oriente Medio recomienda:

- Que las administraciones tomen conciencia de que participando en eventos que promuevan el desarrollo tecnológico del ejército israelí y de otros actores ligados a éste, están enviando un claro mensaje de aprobación de las agresiones por parte de Israel, incluídos sus crímenes de guerra y posibles crímenes contra la humanidad

- En ninguno de los documentos elaborados por ACCIÓ en relación a la promoción empresarial en Israel, se ha encontrado información relativa a los riesgos y los impactos sobre los derechos humanos y el derecho internacional humanitario a la hora de cooperar a nivel empresarial con Israel. Incluso, algunos documentos de ACCIÓN identifican Jerusalén como capital de Israel [45]. En este sentido, es parte fundamental de la responsabilidad de organismos públicos de promoción empresarial y su obligación facilitar a las empresas informaciones completas, claras y adecuadas sobre el conflicto israelo-palestino y las implicaciones legales y éticas que conlleva establecer colaboraciones con determinados actores que actúan en el mercado israelí.

- Que las instituciones catalanas establezcan mecanismos efectivos de control y monitoreo de las empresas catalanas que participen en proyectos de doble uso y de otros agentes empresariales que realicen actividades cómplices con la ocupación del territorio palestino y con las violaciones de derechos humanos.

[45] ACCIÓ. (2016): Programa d'Innovació Internacional