# La indústria de la Ciber-seguretat a Israel

**Novembre del 2016**

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

## Abstract

Entre el 14 i 17 de novembre s'ha organitzat a **Tel Aviv la 4a Conferència Internacional sobre Seguretat Nacional i Ciber-seguretat**[1]**,** cita a la qual han assistit agències de seguretat governamentals i empreses de tot el món atretes per la indústria militar i securitària israeliana. Catalunya no és una excepció. **L'Agència per la competitivitat de l'empresa de la Generalitat de Catalunya, ACCIÓ, ha preparat durant els últims mesos una missió comercial**[2] **que promou la participació catalana en aquesta conferència** amb l'objectiu de crear llaços de cooperació empresarial i institucional en aquest camp. Aquesta missió empresarial compta –segons ACCIÓ[3]- amb l'encaix en la línia estratègica del Govern per fer créixer i potenciar el sector català de la ciber-seguretat 'com un sector econòmic dinàmic amb una projecció de futur altament positiva'. Cadascuna de les 8 empreses o entres tecnològics catalans participants a aquesta missió empresarial rebran o han rebut un ajut financer de 760,28€ com a borsa de viatge.

El Govern d'Israel és el principal promotor d'aquesta conferència ja que aquest sector és clau per a l'economia del país. Hi ha aproximadament 250 empreses de ciber-seguretat que operen a Israel[4] que han captat 500 milions de dòlars durant el 2015 i que ja sumen més de 200 milions de dòlars captats durant els primers dos mesos del 2016[5]. **El 2014 les vendes mundials de les empreses ciber israelianes van ascendir a 6 mil milions de dòlars**. Aquesta xifra va representar aproximadament el **10% de totes les vendes mundials del sector**.. Es calcula que hi ha 16.000 professionals cibernètics a Israel (empresaris i personal contractat), tant en el sector de la defensa com en el sector privat. Una de les claus principals d'aquest èxit internacional és la seva capacitat d'innovació, un avantatge comparatiu basat en l'estreta relació que existeix entre la indústria militar i seguretat tecnològica i les Forces Armades d'Israel.

Aquest sistema s'alimenta i justifica pel manteniment de l'ocupació a Palestina i les tensions amb el Líban, Síria i altres països àrabs, així com per la proliferació dels actors armats no estatals a la regió. Els territoris ocupats palestins són un veritable laboratori on corporacions privades, centres d'investigació, incloent universitats i l'exèrcit proven noves armes i sistemes tecnològics de seguretat per després incorporar-los al mercat global. La marca "Made in Israel" anuncia freqüentment aquesta experiència provada en "combat", però obvia el greu impacte en la societat civil i les violacions sistemàtiques dels drets humans de la població palestina que cometen.

Aquest document té per objectiu identificar els riscos i potencials violacions del dret internacional i els drets humans que implica invertir a Israel a través de l'anàlisi de: 1) les noves polítiques de seguretat globals; 2) la investigació europea en Homeland Security i la participació israeliana; 3) les relacions entre la indústria militar i de seguretat tecnològica amb les Forces Armades d'Israel; 4) Complicitats amb l'ocupació de palestina; 5) Recomanacions a les institucions i empreses catalanes.

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

## Noves polítiques de seguretat: Homeland Security, ciber-seguretat i privatització de la seguretat

Els atacs de l'11 de setembre del 2001 als Estats Units no només van servir com a justificació per bombardejar i ocupar l'Afganistan l'any 2001 i l'Iraq al 2003, sino que també va permetre imposar una nova política de Homeland Security que reforçava els poders del Govern per **neutralitzar les amenaces internes del país** i va contribuir a l'explosió, en termes econòmics, de les empreses militars i de seguretat privada, i la indústria de la seguretat tecnològica. El desenvolupament del complexe industrial de la Homeland Security va evolucionar paral·lelament a l'increment de la **demanda** en seguretat, una demanda basada en la creació d'un sentit de perill en la societat especialment present durant l'Administració de Bush[6]. Des de llavors, la despesa en seguretat nacional no ha parat de créixer arreu del món; s'estima que **només el 2009 els governs van gastar al voltant de 141.600 milions de dòlars en serveis de "Homeland Security"**[7].

**El concepte de "Homeland Security" treballa sobre l'avaluació, mitigació i gestió de les amenaces en el interior de les societats, incloent les fronteres.** Els actuals models de Homeland Security s'assemblen als esquemes "Full Spectrum Dominance" típic de les lògiques de combat, es a dir, el control de tots els elements de la batalla: mar, aire, terra i ciber-món. En la pràctica les polítiques de Homeland Security englobarien la protecció de fronteres, infraestructures crítiques (plantes nuclears, aeroports, edificis governamentals, ports, etc.), macro-esdeveniments (incloent manifestacions), ciber-seguretat, ciber-crim, gestió d'emergències, tecnologies de la vigilancia, etc.

> El concepte de 'Homeland Security implica la securitització de les societats per neutralitzar les amenaces internes, i hi cooperen agents policials amb l'exèrcit i agents de seguretat privada.

Davant del nous reptes per assegurar la seguretat, actors polítics van afirmar que els Estats no tenien prou capacitats per donar resposta a aquests reptes i que necessitaven de la participació de corporacions privades en aquest sentit. Franco Frattini, ex-vicepresident de la Comissió Europea va afirmar en la conferència europea sobre investigació en el sector de la seguretat de 2007 que **la seguretat, com a bé públic, ja no és només responsabilitat de l'Estat, si no que ha de ser compartida per actors privats** [8] . Aquestes paraules testificaven una realitat que ja havia començat anys enrere, concretament l'any 2003 a Iraq, però que ara s'estenia també als àmbits de la seguretat nacional: **la privatització de la seguretat i la guerra.**

En efecte**, l'ocupació d'Iraq va ser el gran escenari de la privatització de la guerra on moltes empreses militars i de seguretat privada van proliferar**. El director general de l'Associació Britànica d'Empreses de Seguretat Privada, Andy Bearpark, feia aquestes declaracions durant una entrevista l'any 2010: "a Iraq el 2003 i 2004 el diner era bàsicament gratis, això significava que els contractes s'adjudicaven per rídicules quantitats de diner –milions i milions de dòlars en contractes van ser bombejats a la indústria"[9].

En la pràctica, **la privatització de la guerra i la seguretat implica la transferència de funcions inherents als Estats a mans privades**. Activitats consistents amb el principi del monopoli legítim de l'ús de la força i que tradicionalment executaven els Cossos i Forces de Seguretat de l'Estat sota la lògica de l'escrutini democràtic i públic. Ara, empreses militars i de seguretat privada, incloent empreses tecnològiques, realitzen funcions d'ordre públic, formació de policies, gestió de presons, control de fronteres, serveis de intel·ligència, entre d'altres. Concretament, la participació de corporacions privades que es guien per lògiques lucratives funcions d'intel·ligència per la seguretat nacional són doblement preocupants: per una banda, suposa l'accés, captura i tractament de milions de dades de caràcter personal amb els potencials abusos de drets humans que pot suposar; i per una altra banda, la definició de les amenaces i el nivell de risc de les mateixes. L'autora Lou Pingeot en el seu anàlisi sobre la política de contractació de Nacions Unides del serveis d'empreses militars i de seguretat, conclou que les empreses privades acaben definint la pròpia política de seguretat del client. Segons Pingeot, les empreses militars i de seguretat privada realitzen anàlisis i gestió de riscos que marginalitzen les dinàmiques socials i polítiques del contextos, prioritzen les respostes

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

de "hard security" per damunt d'accions de mediació o construcció de pau, ja que són àrees que escapen de la seva experiència i per tant, no podrien continuar renovant el seus contractes.[10]

Per tant, **existeix un alt risc de que les corporacions de l'àmbit de seguretat distorsionin el nivell dels riscos d'amenaçes al seu favor**. Un exemple clar, seria l'últim informe sobre riscos globals de l'empresa militar i de seguretat privada Control Risks. En aquest informe Control Risks afirma que el Corn d'Àfrica és una les regions més perilloses pel transport marítim[11]. Malgrat que a principis d'any la principal Associació de Seguretat Marítima del món (SAMI), anunciava el seu fi afirmant que les amenaces de pirateria havien desaparegut en aquelles regions i com a conseqüència oltes empreses de seguretat marítima havien tancat produint-se la caiguda en picat dels membres de l'Associació[12].

## La investigació europea en Homeland Security

L'any 2003, la Unió Europea va encomanar al Grup de Personalitats (GoP en el seu acrònim en anglès) definir les línies estratègiques del "Programa Europeu de Recerca en Seguretat" (ERSP). Aquest grup estava format per pels Comissaris Europeus d'Investigació i Societat de la Informació, Relacions Exteriors i Comerç, l'Alt Representant de la UE de la Política d'Afers Exteriors i Seguretat; representants de l¡OTAN, l'Associació d'Armament de l'Oest d'Europa, el Comitè Militar de la UE, 8 empreses multinacionals del sector armamentístic (EADS, BAE Systems, Thales, Leonardo Finmeccanica) i les més grans empreses del sector tecnològic (Ericsson, Siemens, Diehl i Indra), així com centres d'investigació com Rand Corporation. Destaca la total absència de la Organització Internacional per les Migracions, l'Agència de Nacions Unides pels Refugiats o organitzacions de la societat civil especialitzades en els conflictes i les dinàmiques polítco-socials de les regions veïnes de la UE. Com a conseqüència 3 de les companyies participants en aquest Grup són els majors beneficiaris del ERSP. És per tant, obvi **com les corporacions privades estan definint la política de seguretat de la Unió Europea i donant respostes que estan contribuint a la militarització de les fronteres** i per tant, requereixen de la seva pròpia contractació per part les institucions europees i els seus Estats membre.

> Les corporacions privades estan definint la política de seguretat de la Unió Europea i donant respostes que estan contribuint a la militarització de les fronteres.

**Israel és l'únic país no europeu que participa en els programes de finançament de la UE per a la investigació**. Durant l'anterior programa d'investigació europeu (FP7) de 2007-13, actors públics i privats d'Israel van participar en 1.500 projectes[13]. A l'àmbit d'investigació en seguretat, **la UE ha canalitzat 26 milions de euros a través de 49 projectes de recerca directament al sectors de defensa i seguretat de l'Estat d'Israel**. 23 empreses israelianes s'han beneficiat d'aquest programa incloent a Elbit Systems, Israel Aerospace Industries (IAI), Aeronautics. Defence Systems i Opgal Optronics Industries[14]. Només Elbit Sytems i IAI van rebre 393.900.149,00 euros, una gran majoria d'ells destinats a la desenvolupar drons[15]. En el actual programa europeu Horizon 2020, Israel participa en un total de 576 projectes[16], dels quals 18 són l'àmbit de seguretat[17].

L'interès d'Israel en aquests programes és clau ja que guanya accés a projectes i coneixement; permet treballar en xarxa amb universitats i empreses europees; i avançar econòmicament la investigació acadèmica al país. Però quin interès té la UE a col·laborar amb un aliat com Israel?

**Israel és un referent en seguretat, no només per l'alt desenvolupament de la seva indústria, sinó perquè cristal·litza el model d'economia de la vigilància de 'Homeland Security' que han anat adquirint països occidentals.** Però cal tenir en compte de quina manera Israel ha adquirit aquest estatut internacional: tot aquest 'know how' procedeix de la política d'ocupació i l'intent de vigilar i controlar la població palestina. 'Made in Israel' s'ha convertit en garantia de serveis o productes 'provats en combat', fins al punt que és comú trobar CEO d'empreses que així ho exposen en entrevistes i conferències, com a marca de qualitat. Un exemple és Saar Koursh, CEO de l'empresa israeliana Magal Security Systems Ltd que en una entrevista va afirmar recentment: "Qualsevol pot

[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
14http://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 Per més información veure: http://www.iserd.org.il/_Uploads/dbsAttachedFiles/ISERD_STAT_JULY_2016.pdf
17 http://www.iserd.org.il/?CategoryID=443

mostrar-li un bon powerpoint, però pocs poden mostrar-li un projecte tan complex com Gaza que està constantment provat en batalla".[18].

Com explica l'informe NeoConOpticon del Transnational Institute "malgrat la seva existència hiper-militarista 'i les seves' despeses desmesurades en acords il·legals, carreteres il·legals, el mur il·legal i per descomptat, l'ocupació il·legal, Israel, mitjançant el manteniment dels símbols de la democràcia liberal moderna, ha aconseguit posicionar-se com l'Estat de la Seguretat nacional per excel·lència.'[19] (p.12)

Alguns del projectes més rellevants en el marc de la seguretat nacional amb participació israeliana i espanyola són:

- GLOBE (2008, FP7): per la lluita contra tot tipus d'immigració il.legal des de qualsevol àmbit, liderat per Telvent i la participació de Indra[20]. Telvent aporta el sistema de vigilància marítima AMASS amb participació de IAI[21].
- TALOS (2008-12): Desenvolupament d'un nou sistema de protecció de les fronteres europees mitjançant l'ús de vehicles no tripulats, amb la participació de IAI, l'empresa espanyola TTI i la col·laboració amb agents espanyols de seguretat pública[22]
- CAPER (2011-14, FP7): creació d'una plataforma virtual per la prevenció i detenció del crim organitzat mitjançant l'ús de les tecnologies de la informació, amb la participació del Ministeri de Seguretat Pública d'Israel, Technion – Israel Institute of Technology, Conselleria d'Interior de la Generalitat de Catalunya, Guardia Civil Espanyola, Universitat Autonoma de Barcelona, S21SEC Information Security Labs SL, entre d'altres.
- DESURBS (2011-14, FP7): anàlisi i dissenyn d'eines per a la detecció d'amenaces a la seguretat en espais urbans. Les ciutat de Jerusalem, Nottingham i Barcelona serviran com a casos d'estudi de referència. Participants: The Hebrew University of Jerusalem, Bezalel Academy of Arts and Design i el Centre Internacional de Métodes Numérics en Ingenieria.
- EUROSUR – SeaBILLA (2010-14, FP7): Disseny d'un nou sistema de vigilància de fronteres marítimes Europees que integri el control espacil, aeri, terrestre i marítim. El projecte pretén crear una cooperació efectiva entre els diversos Estats membre en la lluita contra el tràfic de drogues en el Canal de la Mànega, la immigració i.legal al sud del Mediterrani i les activitats considerades il.lícites en aigües de l'Atlàntic des de les Illes Canàries fins a les Açores. Participants: Indra, Universitat de Murcia, TTI Norte SL., Eurocopter España S.A., i l'empresa israeliana Correlation Systems.
- FOCUS (2011-13, FP7): Disseny d'una estratègia de recerca en l'àmbit de la seguretat europea. L'objectiu central és poder analitzar el rol de la UE dins dels nous reptes derivats dels riscs i de les amenaces en un món globalitzat (tals com atacs a ciutadans europeus o a infraestructures considerades crítiques). Participants: University of Haifa, Atos Apsin SA, INTA, Ingeria de Sistemas para la Defensa de España.
- FORENSOR (2015-18, H2020): orientat a la creació de sensors intel·ligents, miniaturaitzats, de baix cost, inalambric, autònom per la recopilació de proves. El sensor inclourà una càmera ultra-sensible i intel·ligència integrada que permetrà operar en ubicacions remotes, identificar automàticament esdveniments criminals predefinits, alertar en temps real, i emmagatzemar l'evidència rellevant en vídeo, ubicació i temps. Participants: Emza Visual Sense (Israel), Policia Local de Valencia i altres entitats públiques i privades de la UE.
- LAW TRAIN (2015-18, H2020): Disseny d'una plataforma tecnològica per unificar las metodologies per interrogatoris. Unitat de policia practicaran la interrogació amb sospitós en un medi realitat virtual. Participans. Israeli Bar Ilan Univeristy, Ministeri de Seguretat Pública de Israel, Compedia Software & Hardware Development Ltd., Ministeri de Justícia de Portugal, Ministeri de Justícia de Bélgica, Ministeri d'Interior d'Espanya, Optimització orientada a la Sostenibilitat, INESC-ID, USECON, University of Leuven.

És important destacar que la investigació europea permet el desenvolupament de tecnologia que posteriorment és oferta als Estats i altres agències de seguretat. Això és especialment visible en els projectes on participen entitats israelianes on s'inclouen demostracions de projectes, on els prototips de sistemes de seguretat són manufacturats i provats; i infraestructura de projectes, per exemple sistemes de comunicació, infraestructures crítiques i capacitat de gestió de crisis. Aquests projectes estan clarament destinants a la compra pública[23].

Això entra en contradicció amb el compromís de la Unió Europea[24] de no finançar a través d'aquests programes projectes que tinguin aplicacions de doble ús militar, atès que moltes de les empreses que participen en aquests programes formen part del complex industrial israelià de seguretat militar i de seguretat interna. El Programa

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 més 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
23 Transnational Institute, NeoConOpticon, 2009, pp19
24 http://horizon2020projects.com/global-collaboration/israel-boycott-petition-receives-irish-support/

Horizon2020 ho deixa ben clar[25] "Només les activitats de recerca i innovació que es centren en aplicacions civils són elegibles per al finançament en Horizon 2020. La investigació destinada a ser utilitzada en aplicacions militars, no es pot finançar pel programa marc". També ho defineix el document de la comissió europea d'ètica per a investigadors del programa FP7[26]. No obstant això, la investigació i desenvolupament proposat per moltes d'aquestes empreses implica inevitablement el doble ús militar de la tecnologia i el coneixement, atès que estan profundament implicades en les violacions israelianes del dret internacional.

Per posar un exemple vinculat amb el doble ús de la indústria de la vigilància, en any 2014 va sortir a la llum un cas d'escoltes per part de reservistes de la unitat 8.200 que van rebre ordres de vigilar a població civil palestina [27] Segons declaracions de un grup de reservistes, alguns d'ells veterans, que van denunciar aquesta pràctica. el personal va rebre instruccions de registrar qualsevol detall nociu de la vida dels palestins que vigilaven, incloent informació sobre preferències sexuals, infidelitats, problemes financers o malalties familiars que podrien ser "utilitzades per extorsionar la persona i convertir-la en col·laboradora".

## Relacions entre la indústria militar i de seguretat tecnològica amb les Forces Armades d'Israel

Israel es troba entre els 10 països majors exportadors d'armes del món. La seva indústria armamentística té una forta dependència del mercat global. Almenys ¾ de la seva producció s'exporta, fet que permet reduir les depeses de la seva producció interna. **El sector de la tecnologia securitària representa una quarta part del total d'exportacions d'Israel, al voltant de 25 milions de dòlars durant el 2014**. Només al 2014 es van crear 20 centres de Recerca i Desenvolupament establerts per empreses multinacionals a Israel per desenvolupar solucions de seguretat pel mercat global. **Israel destina mes del 4% del seu PIB a la recerca i desenvolupament**[28], recerca que es desenvolupa en partneriat amb el món acadèmic i l'empresa, una fórmula que els permet tenir una taxa de patents anual molt elevada, un ratio de 250 aproximadament per milió d'habitants a l'any[29].

**El Govern Israelià juga, per tant, un rol clau en la promoció del entramat de la economia de la seguretat**. L'any 1993 el programa Yozma[30] va permetré la atracció d'alguns del majors fons de capital risc d'Estats Units i altres països per invertir en empreses isralianes. Aquest programa ha permés financiar projectes i empreses del sector de la tecnologia i innovació en general i la securitària en particular.

Es calcula que hi ha 16.000 professionals cibernètics a Israel (empresaris i personal contractat, tant en el sector de defensa com en el sector privat que és distribueixen en arquitectes i consultors, sistemes SCADA, malware i enginyeria inversa[31]. Els empresaris cibernètics a Israel provenen d'una varietat d'antecedents professionals: Forces Armades Israelianes i agències de seguretat (25%); professionals d'alta tecnologia i hackers (22%); professionals d'empreses líders de telecomunicacions (18%), altres empresaris (12%); acadèmics i professors universitaris (6%).

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


Font: Informe del sector de la ciber-seguretat de l'Embaixada de l'íIndia, Tel Aviv[32]

L'exèrcit israelià ha estat una peça fonamental en el procés de desenvolupament de la indústria Homeland Security i tecnologia de la seguretat. Concretament, la Unitat 8200 dels Cossos d'Intel·ligència de les Forces de Defensa de Israel. La missió de la Unitat és la captació de senyals d'intel·ligència i desxifrat de codis**. La unitat 8200 funciona com una incubadora tecnològica on es formen els futurs directius de les start-ups de seguretat d'Israel**. Primer, es realitza una cerca de talents en les escoles secundàries del país per després incorporar-los a la unitat on s'aprofita la més avançada tecnologia SIGINT (intel·ligència de senyals), utilitzar tècniques sofisticades de mineria de dades, i concebre tecnologies altament avançades. Companyies clau del sector de la seguretat com Checkpoint, Imperva, Nice, Gilat, Waze, Trusteer, Wix o Fortscale tenen els seus orígens en la Unitat 8200.

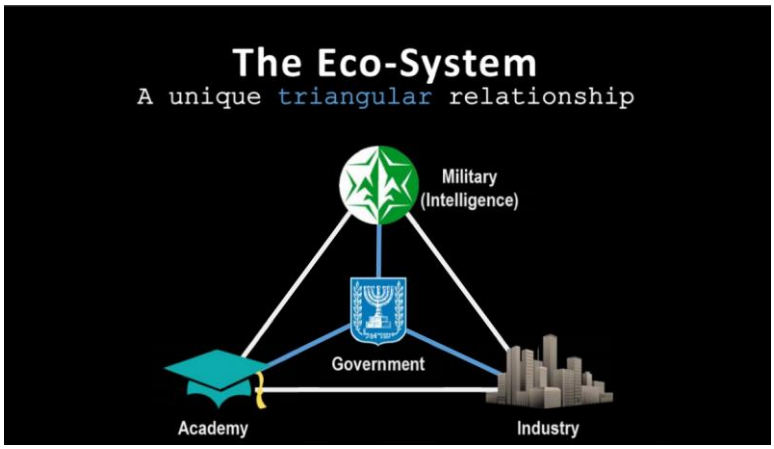
També cal destacar la **Divisió Tecnològica Lotem-C4i** de les Forces Armades Israelianes que s'encarrega de la gestió dels camps de batalla virtuals i ciber-espionatge. Des de 2012, la Divisió s'enfoca en la lluita contra el terrorisme a través de la formació de ciber-comands contra països hostils a Israel com Iran i els seus aliats. Un dels seus èxits va ser el llançament del virus Flame[33] que va afectar en 2012 els sistemes informàtics que controlen la industria petrolera de Iran.

## Complicitats amb l'ocupació de Palestina

**El complex industrial israelià de seguretat militar i de seguretat interna, la intel·ligència militar, el Govern i les universitats conformen un ecosistema col·laboratiu** que té com a inevitable conseqüència el doble ús de la tecnologia de la ciber-seguretat i de defensa. D'una banda, gran part d'aquestes empreses proporcionen la seva tecnologia i saber a l'exèrcit israelià i al Ministeri de Defensa.

D'altra banda, **hi ha tot un sistema de "portes giratòries" entre les unitats israelianes d'elit militar com la unitat 8200 i el sector privat,** beneficiant directament de la tecnologia i els coneixements adquirits en els abusos sistemàtics contra els drets humans i els crims de guerra comesos per aquestes unitats. Per posar un parell d'exemples il·lustratius d'aquestes portes giratòries: El fundador de Verint és Jacob "Kobi" Alexander[34], l'ex oficial de la intel·ligència israeliana; un dels directors de Natural Speech Communication (NSC) és l'excap del Mossad, Shabtai Shavit[35].

32 The Cybersecurity Sector in Israel http://www.indembassy.co.il/pages.php?id=666670o#.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




Font: Israel Export Institute[36]

**Alguns exemples d'empreses que participen de la complicitat amb l'ocupació:**

**Israel Aerospace Industries (IAI)** és de les empreses pioneres en la tecnologia de drones i la primera en llençar un dron de vigilància[37]. Però també ha estat una de les empreses que més s'ha beneficiat de l'ocupació. El model Heron 1 i Heron TP de IAI són freqüentment utilitzats sobre el Territoris ocupats Palestins i especialment sobre la Franja de Gaza. Són drons amb capacitat de llançament de projectils, concretament fins 4 míssils Spike. Segons Human Rights Watch, Israel hauria utilitzat drones Heron d'IAI i Hermes d'Elbit Systems, equipats amb míssils Spike i altres sobre Gaza[38]. Però també amb funcions de vigilància i identificació d'objectius. Existeixen evidències que asseguren que els drones Heron 1 van ser utilitzats durant l'Operació Pluges d'Estiu de 2006 sobre Gaza on van morir més de 400 palestins/es[39]. L'any 2008 durant la Operació Plom Fos sobre Gaza, amb més de 1330 palestins/es morts es van tornar a fer servir drons de IAI, model Heron TP. Els drones van precedir l'entrada de la infanteria israeliana, netejant l'àrea i neutralitzant objectius amb míssils[40].

**Elbit Systems** és juntament amb IAI una de les principals empreses pioneres i líders del sector de la seguretat en general i el desenvolupament de drons en particular. La tecnologia de Elbit s'utilitza al mur de separació a través sistemes de detecció d'intrusos. El producte "Torch" està manufacturat específicament per ser utilitzat al Mur de Confiscació. També produeix vehicles armats a control remot per vigilar zones al voltant del Mur. En els assentament il.legals d'Ariel i Ar Ram a Cisjordània, Elbit i les seves subsidiàries proveiexen del sistema de vigilància de càmeres LORROS. Elbit és també un dels principals proveïdors de sistemes de seguretat a les Forces Armades Israelianes per exemple millorant la tecnologia dels F-16 israelians o els tancs Merkava. També proveeix de vaixells controlats de forma remota que han estat utilitzats en les costes de Gaza. Per últim, els drons armats Hermes 900 d'Elbit van ser utilitzats durant l'atac a Gaza de 2014.

Segons un informe de 2015 del grup de vigilància basat en la Unió Europea Privacy International, la empresa israeliana **Verint Systems Inc**. va subministrar hardware i software per funcions d'espionatge en línes fixes i mòbils de telefonia, així com xarxes d'internet als Governs de Kazhastan i Uzbekistan[41] que van ser finalment utilitzats per identificar i capturar opositors als Governs. Privacy International també relaciona a l'empresa Verint amb l'escàndol de les escoltes de la NSA[42]

**Nikuv International** va estar presumptament implicada en la manipulació de llistes de votants i resultats finals de les eleccions a Zimbabwe afavorint la reelecció del Mugabe i el seu partit PF[43].

**NSO Group Technologies** va fabricar Pegasus, un malware que permet el monitoreig remot i la extracció completa de dades dels Iphone. Segons Privacy Internacional, organització que es dedica a la denuncia de violacions de

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

privacitat per part dels Estats i empreses, Pegasus podria haver estar utilitzat[44] per Emirats Àrabs Units, Turquia, Israel, Tailandia, Qatar, Kenia, Uzbekistan, Mozambic, Marroc, Iemen, Hongria, Arabia Saudia, Nigeria i 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

## Recomanacions a les institucions i empreses catalanes

A la llum de les informacions anteriors, invertir o col·laborar amb la indústria militar, seguretat privada i seguretat tecnològica d'Israel implica potencials violacions del dret internacional i els drets humans, donat que és una indústria basada en l'expertesa de l'ocupació de Palestina i la infraestructura d'apartheid a Cisjordània i la Franja de Gaza.
Per tal d'evitar complicitats amb les greus violacions de drets humans i del dret internacional humanitari; i en esperit del foment de la pau i de la transformació pacífica dels conflictes, l'Observatori de Drets Humans i Empreses al Nord d'Àfrica i Orient Mitjà recomana:

- Que les administracions prenguin consciència que participar en esdeveniments que promoguin el desenvolupament tecnològic de l'exèrcit israelià i d'altres actors lligats a aquest, estan enviant un clar missatge d'aprovació de les agressions per part d'Israel, inclosos els seus crims de guerra i possibles crims contra la humanitat

- En cap dels documents elaborats per ACCIÓ en relació a la promoció empresarial a Israel, s'ha trobat informació relativa als riscos i als impactes sobre els drets humans i el dret internacional humanitari a l'hora de cooperar a nivell empresarial amb Israel. Així, fins i tot, alguns documents d'ACCIÓ identifiquen Jerusalem com a capital d'Israel[45]. En aquest sentit, és part fonamental de la responsabilitat d'organismes públics de promoció empresarial i obligació facilitar a les empreses informacions completes, clares i adequades sobre el conflicte israelo-palestí i les implicacions legals i ètiques que comporta establir col·laboracions amb determinats actors que actuen en el mercat israelià.

- Que les institucions catalanes estableixin mecanismes efectius de control i monitoreig de les empreses catalanes que participin en projectes de doble ús i d'altres agents empresarials que realitzin activitats còmplices amb l'ocupació del territori palestí i amb les violacions de drets humans.

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