ODHE Observatori de
Drets Humans i Empreses
Nord d'Àfrica i Orient Mitjà

Date: 17 November 2016

The cybersecurity industry in Israel

November 2016
Observatory on Human Rights and Business
North Africa and the Middle East

Abstract

The **4th International Conference on Homeland Security and Cyber**[1], held in Tel Aviv 14 - 17 November, was attended by government security agencies and enterprises from around the world, attracted by the Israeli military and security sector. Catalonia is no exception. Over recent months the **Agency for Business Competitiveness of the Government of Catalonia, ACCIÓ, prepared a trade mission to promote Catalan participation in this conference**[2], with the aim of creating business and institutional cooperation in this field. According to ACCIÓ[3] this trade mission is aligned with the strategic policy of the Government to boost the Catalan cybersecurity sector "as a dynamic economic sector with a very positive outlook". Each of the eight Catalan companies and technology centres participating in this mission will receive or have already received financial support of €760.28 towards travel expenses.

The Government of Israel is the main promoter of this conference, since this sector is key to the country's economy. There are approximately 250 cybersecurity companies operating in Israel[4], capturing $500 million during 2015 and over $200 million in the first two months of 2016[5]. **In 2014 worldwide sales of Israeli cyber companies amounted to $6 billion dollars.** This figure represents approximately 10% of worldwide sales in the sector. It is estimated that there are 16,000 cybernetics professionals in Israel (entrepreneurs and staff), both in the defence sector and in the private sector. One of the keys to this international success is capacity for innovation, a comparative advantage based on the close relationship that exists between the military and technological security sector and Israeli armed forces.

This system is fueled and justified by the maintenance of the occupation of Palestine and tensions with Lebanon, Syria and other Arab countries, together with the proliferation of non-state armed groups in the region. The Occupied Palestinian Territories are a real laboratory for private corporations and research centres, including universities, for the army to try out new weapons and security technology systems and then launch them on the global market. The "Made in Israel" brand frequently boasts of this "tested in combat" experience, passing over the negative impact on civil society and systematic violations of human rights of Palestinian inhabitants.

This document aims to identify the risks and potential violations of international law and human rights involved in investing in Israel through analysis of: 1) new global security policies; 2) European research in homeland security and Israeli participation; 3) relations between the

military and technological security sector and Israeli armed forces; 4) complicity with the occupation of Palestine; 5) recommendations for Catalan institutions and enterprises.

New security policies: homeland security, cybersecurity and security privatisation

The attacks on the United States of 11 September 2001 not only served to justify bombardment and occupation of Afghanistan in 2001 and Iraq in 2003, but also ledt to a new homeland security policy that strengthened the government's powers to neutralise internal threats in the country and contributed in economic terms to the explosion of military and private security companies, and the technological security sector. The homeland security industrial complex grew with the increasing demand for security, a demand based on the creation of a sense of danger in society, especially during the years of the Bush administration[6]. Since then, spending on national security has continued to grow all over the world; it is estimated that in 2009 governments spent about $141.6 billion on homeland security[7].

The concept of homeland security is based on assessment, mitigation and management of threats within society, including on borders. Current models of homeland security are similar to the full spectrum dominance schemes typical of combat logic, that is, controlling all battle components: sea, air, land and cyberspace. In practice, homeland security policies include frontier protection, critical infrastructure (nuclear plants, airports, government buildings, ports, etc.), macro events (including demonstrations), cybersecurity, cybercrime, management of emergencies, surveillance technology, etc.

> *The concept of homeland security involves securitisation of society to neutralise internal threats with police services, the army and private security agencies cooperating on this.*

In the face of new challenges to ensuring security, political agents have affirmed that States do not have sufficient capabilities to respond to these challenges and that they need the participation of private corporations in this regard. Franco Frattini, former vice-president of the European Commission stated at a European conference on research in the security sector of 2007 that security, as a public asset, is no longer the sole responsibility of the State, but must be shared by private agents[8].These words testify to a reality that emerged years earlier, specifically the year 2003 in Iraq, and has now spread to fields of national security: the privatisation of security and war.

Indeed , the occupation of Iraq was the great scenario of war privatisation, in which many military and private security companies proliferated. The director-general of the British Association of Private Security Companies, Andy Bearpark, made the following statement in an interview in 2010: "In Iraq in 2003 and 2004 money was basically free. That meant [private security] contracts went for ridiculous amounts of money - millions and millions of dollars of contracts being pumped into the industry."[9]

In practice, the privatisation of war and security implies the transfer of functions inherent to States into private hands. Such activities are consistent with the principle of legitimate monopoly on the use of force traditionally executed by the security forces of the State under the logic of democratic, public scrutiny. Now military and private security companies, including technology companies, carry out public order functions, police training, prison management, border control and intelligence services, among others. Specifically, the participation of profit-seeking private corporations in intelligence functions for national security are of twofold concern: on the one hand, it involves access, capture and treatment of a great amount of personal data, with the potential for human rights abuses; and, on the other hand, they define threats and the level of risk involved. In her analysis of the politics of United Nations contracts for the services of military and security enterprises, the author, Lou Pingeot, concludes that the private enterprises end up defining their client's own security policy. According to Pingeot, military and private security companies carry out analysis and risk management that marginalise social and political dynamics of contexts, giving priority to "hard security" responses over and above actions of mediation or peacebuilding, since these are fields that are beyond their experience and, therefore, they would otherwise not be able to renew their contracts[10].

Therefore, there is a high risk that corporations in the security field distort the level of threat in their favour. A clear example would be the latest report on global risks of the military and private security company Control Risks. In the report, Control Risks states that the Horn of Africa is one of the most dangerous regions for maritime transport[11]. Though at the beginning of the year the world's leading maritime safety association (SAMI) announced that threats of piracy had disappeared there and as a result many other maritime security enterprises had closed, causing a great decline in the number of members of the association[12].

European research in homeland security

In 2003 the European Union commissioned the Group of Personalities (GoP) with establishing the cornerstones of the European Security Research Programme (ESRP). This group was made up of European Commissioners for Research and the Information Society, Foreign Affairs and Trade, the EU's High Representative for Foreign Affairs and Security Policy; representatives of NATO, the Western European Armaments Group, the EU Military Committee, eight multinational arms sector companies (EADS, BAE Systems, Thales, Leonardo Finmeccanica) and the largest companies in the technology sector (Ericsson, Siemens, Diehl and Indra), together with research centres such as Rand Corporation. Noteworthy absences are the International Organisation for Migration, the United Nations Refugee Agency and civil society organisations specialising in conflicts and the social and political dynamics of EU neighbouring regions. Consequently, three of the companies in this group are the largest beneficiaries of the ESRP. It is therefore evident that private corporations are defining the security policy of the European Union and giving responses that contribute to the militarisation of borders, consequently requiring contracts with them from European institutions and Member States.

> *Private corporations are defining the security policy of the European Union, with responses that contribute to the militarisation of borders.*

Israel is the only non-European country that participates in EU research funding programmes. During the previous European research programme (FP7), for the period 2007 - 2013, public and private agents in Israel participated in 1,500 projects[13]. In the field of security research, the EU has channeled €26 million through 49 research projects directly to Israeli defence and security sectors. 23 Israeli companies have benefited from this programme, including Elbit Systems, Israel Aerospace Industries (IAI), Aeronautics. Defence Systems and Opgal Optronics Industries[14] . Elbit Sytems and IAI alone received €393,900,149, principally for development of drones[15]. In the current European programme Horizon 2020, Israel participates in a total of 576 projects[16], 18 of which are in the security sector[17].

Israel's interest in these programmes is clearcut because it gains access to projects and knowledge; it allows networking with European universities and companies; and it economically promotes academic research in the country. But what is the EU's interest in working with an ally such as Israel?

Israel is a benchmark in security, not only because of the high level of development of its industry, but because it crystallises the homeland security surveillance economic model that has gathered force in western countries. But we must take into account how Israel has acquired this international status: all this know-how derives from the policy of occupation and the effort to supervise and control the Palestinians. Made In Israel has become a guarantee of services and products 'tested in combat', to the point where it is common to find enterprise CEOs referring to this in interviews and speeches as a quality brand. An example is Saar Koursh, CEO of the Israeli enterprise Magal Security Systems Ltd, who in a recent interview stated that "Anybody can give you a very nice PowerPoint, but few can show you such a complex project as Gaza that is constantly battle-tested."[18].

As explained in the NeoConOpticon report of the Transnational Institute, "Despite its hyper-militaristic existence and massive expenditure on illegal settlements, illegal roads, the illegal wall and, of course, the illegal occupation itself', Israel has, by retaining the trappings of modern liberal democracy, successfully positioned itself as the Homeland Security State par excellence."[19]

Some of the largest national security projects with Israeli and Spanish participation are:

- GLOBE (2008, FP7). For the fight against all types of illegal immigration in any context, led by Telvent and with the participation of Indra[20]. Telvent provides the AMASS maritime surveillance system, with the participation of IAI[21].
- TALOS (2008 - 2012). Development of a new European border protection system through use of unmanned vehicles, with the participation of IAI, the Spanish enterprise TTI and collaboration with Spanish public security agencies[22].
- CAPER (2011 - 2014, FP7). Creation of a virtual platform for prevention and detention in the field of organised crime through the use of information technology, with the participation of the Israeli Ministry of Public Security, Technion - Israel Institute of Technology, the Department of Internal Affairs of the Government of Catalonia, the Spanish Civil Guard, the Universitat Autònoma de Barcelona, and S21SEC Information Security Labs, S.L., among others.

- DESURBS (2011 -2014, FP7). Analysis and design of tools for the detection of threats to security in urban areas. The cities of Jerusalem, Nottingham and Barcelona will serve as benchmark case studies. Participants: the Hebrew University of Jerusalem, Bezalel Academy of Arts and Design, and the International Centre for Numerical Methods in Engineering.
- EUROSUR - SeaBILLA (2010 - 2014, FP7). Design of a new surveillance system for European maritime borders, integrating space, air, land and maritime control. The project aims to create effective cooperation among Member States in the fight against drug trafficking in the English Channel, illegal immigration in the south of the Mediterranean and activities considered illegal in the waters of the Atlantic from the Canary Islands to the Azores. Participants: Indra, the University of Murcia, TTI Norte S.L., Eurocopter España S.A., and the Israeli company Correlation Systems.
- FOCUS (2011 - 2013, FP7): Devising a research strategy in the field of European security. The central objective is to analyse the role of the EU in new challenges deriving from risks and threats in a globalised world (such as attacks on European citizens or infrastructure considered critical). Participants: the University of Haifa, Atos Apsin S.A., INTA, Engineering Systems for the Defence of Spain.
- FORENSOR (2015 - 2018, H2020). For the creation of smart, miniaturized, low cost, wireless, autonomous sensors for trial data gathering. The sensor will include an ultra-sensitive, integrated smart camera allowing operation in remote locations, automatically identifying predefined criminal events, with alerts in real time, and storage of relevant video evidence, and location and time. Participants: Emza Visual Sense (Israel), the Valencia local police force, and other public and private bodies in the EU.
- LAW TRAIN (2015 -2018, H2020). Design of a technology platform to unify interrogation methods. The police unit will carry out interrogation of a suspect in a virtual reality environment. Participants: Bar-Ilan University (Israel), Ministry of Public Security of Israel, Compedia Software & Hardware Development Ltd., Ministry of Justice of Portugal, Ministry of Justice of Belgium, Ministry of the Interior of Spain, Optimizacion Orientada a la Sostenibilidad S.L., INESC-ID, USECON, University of Leuven.

European research facilitates development of technology that is subsequently offered to States and other security agencies. This is especially visible in projects where Israeli entities are involved, where project demonstrations are included, where prototype security systems are manufactured and tested; and in project infrastructure, for example, communication systems, critical infrastructure and crisis management capacity. These projects are clearly aimed at public procurement[23].

This contradicts the commitment of the European Union not to finance through these programmes projects that have applications for dual military use[24], since many of the companies participating in these programmes are part of the Israeli military and internal security industrial complex. The Horizon2020 programme makes it very clear that "Only research and innovation activities focusing on civil applications are eligible for funding under Horizon 2020. Research intended to be used in military applications, cannot be funded under this framework programme."[25] This is also defined in the document of the European Ethics Commission for FP7 researchers[26]. However, the research and development proposed by many of these companies inevitably involves dual military use of the technology and knowledge, since they are deeply involved in Israeli violations of international law.

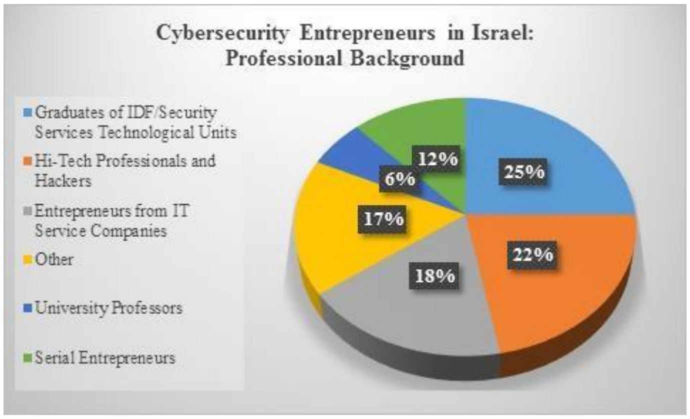
To give an example linked to dual use of the surveillance industry, in 2014 it emerged that reservists in Unit 8200 received orders to monitor the civilian Palestinian population[27]. According to statements from a group of reservists, some of them veterans, who denounced this practice, staff were instructed to record any detrimental details of the lives of the Palestinians they monitored, including information on sexual preferences, infidelities, financial problems and family illnesses, which could be "used to blackmail people and turn them into collaborators".

Relations between the military and technological security sector and the Israeli armed forces

Israel is among the top ten arms exporting countries in the world. Its arms industry depends on the global market. At least 75% of production is exported, offsetting the cost of internal production. The technological security sector accounts for 25% of total Israeli exports, about $25 million in 2014 . In 2014 alone, 20 research and development centres were established by multinational companies in Israel to create security solutions for the global market. Israel destines over 4% of its GDP to research and development[28], research that is carried out in partnership with the academic and business world, a formula that allows them to have a very high annual patent rate, with a ratio of about 250 per million inhabitants per year[29].

The Israeli Government therefore plays a key role in promoting the security sector. In 1993 the Yozma programme helped to attract some of the largest venture capital funds in the United States and other countries to invest in Israeli companies[30]. This programme has helped to finance projects and enterprises in the technology sector, in innovation in general and security in particular.

It is estimated that there are 16,000 cybernetics professionals in Israel (business people and staff), both in defence and in the private sector, with architects and consultants, SCADA systems, malware and reverse engineering[31]. Cyber business operators in Israel come from a variety of professional backgrounds: the Israeli armed forces and security agencies (25%); high tech professionals and hackers (22%); professionals in leading telecommunications companies (18%); other business people (12%); academics and university teachers (6%).



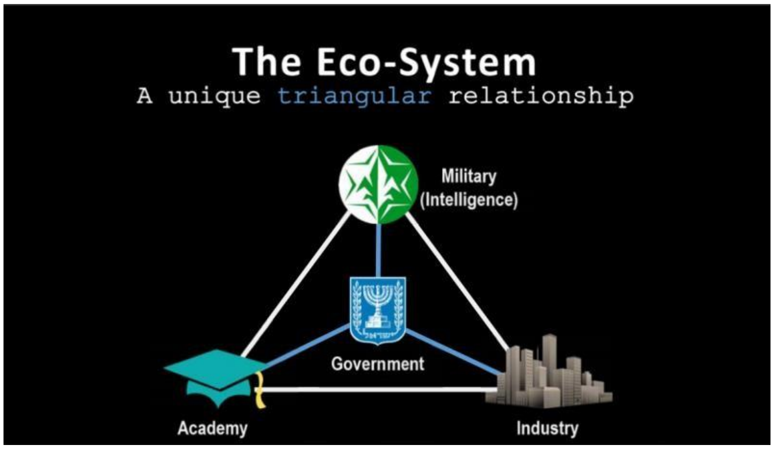
Source: Report on the cyber security sector of the Indian Embassy, Tel Aviv[32]

The Israeli army has been a key player in the process of creating the homeland security sector and security technology. Specifically, Unit 8200 of the Israel Defence Forces Intelligence Corps. The mission of this unit is to capture signals intelligence and decryption of codes. Unit 8200 operates as a technology incubator, where future managers of Israeli security start-ups are trained. First, there is talent spotting in secondary schools around the country, leading to incorporation of subjects into the unit, taking advantage of the most advanced SIGINT technology (signals intelligence), using sophisticated data mining techniques, and devising advanced technology. Key companies in the security sector such as Checkpoint, Imperva, Nice, Gilat, Waze , Trusteer, Wix and Fortscale have their origins in Unit 8200.

Furthermore, there is Technology Division Lotem-C4i of the Israeli armed forces, which is in charge of the management of virtual battlefields and cyberespionage. Since 2012, the Division focuses on the fight against terrorism through training of cyber units against countries hostile to Israel, such as Iran and its allies. One of its achievements was the release of the Flame virus in 2012[33], which attacked computer systems controlling the oil industry in Iran.

Complicity with the occupation of Palestine

The Israeli military security and internal security industrial complex, military intelligence, the Government and universities make up a collaborative ecosystem that has the inevitable consequence of dual use of cybersecurity and defence technology. First, most of these companies provide technology and knowledge to the Israeli army and the Ministry of Defence. Secondly, there is a whole system of revolving doors between elite Israeli military units such as Unit 8200 and the private sector, directly benefitting from the technology and knowledge acquired in systematic violations of human rights and war crimes committed by these units. To give a couple of illustrative examples of the revolving doors, the founder of Verint is Jacob "Kobi" Alexander[34], a former officer in Israeli intelligence; and one of the directors of Natural Speech Communication (NSC) is the former head of Mossad, Shabtai Shavit[35].



Source: Israel Export Institute[36]

Examples of enterprises that are complicit in the occupation

Israel Aerospace Industries (IAI) is a pioneering enterprise in drone technology and was the first to launch a security drone[37]. It is also one of the enterprises that has most benefitted from the occupation. IAI models Heron 1 and Heron TP are frequently used in the Occupied Palestinian Territory and in particular in the Gaza Strip. They are drones with the capacity to launch projectiles, specifically up to four Spike missiles. According to Human Rights Watch, Israel used IAI Heron drones from IAI and Elbit Systems Hermes drones, equipped with Spike missiles and others, in Gaza[38]. They are also used for tasks of surveillance and target identification. There is evidence that Heron 1 drones were used during the Operation Summer Rains in Gaza in 2006, in which over 400 Palestinians died[39]. In the 2008 Operation Cast Lead in Gaza, when over 1330 Palestinians died, IAI Heron TP drones were again used. The drones preceded the entrance of Israeli infantry, clearing the area and neutralising targets with missile strikes[40].

Elbit Systems, together with IAI, is one of the main pioneering companies and leaders in the security sector in general and the development of drones in particular. Elbit technology is used at the separation wall in intrusion detection systems. The Torch product is specifically manufactured to be used at the Confiscation Wall. It also makes remote-controlled armed vehicles to carry out surveillance of areas near the Wall. At the illegal settlements of Ariel and Ar Ram in the West Bank, Elbit and its subsidiaries have provided the LORROS surveillance system. Elbit is also one of the main suppliers of security systems for the Israeli armed forces, for example, enhancing the technology of Israeli F-16s and Merkava tanks. It also provides remote-controlled vessels that have been used off the coast of Gaza. Lastly, Elbit Hermes 900 armed drones were used in the attack on Gaza in 2014.

According to a 2015 report by the watchdog Privacy International based in the European Union, the Israeli company Verint Systems Inc. provided hardware and software for spying on landlines and mobile telephone lines, and on internet networks for the governments of Kazakhstan and

Uzbekistan[41], in the last instance being used to identify and capture opponents of the regimes. Privacy International also connects the Verint company to the NSA phone tapping scandal[42].

Nikuv International was allegedly involved in the manipulation of voter lists and final results of the elections in Zimbabwe, favouring the re-election of Mugabe and his PF party[43].

NSO Group Technologies manufactured Pegasus, a malware that permits remote monitoring and full data extraction on iPhones. According to Privacy International, an organisation that reports violations of privacy by States and companies, Pegasus may have been used by the United Arab Emirates, Turkey, Israel, Thailand, Qatar, Kenya, Uzbekistan, Mozambique, Morocco, Yemen, Hungary, Saudi Arabia, Nigeria and Bahrain[44].

Recommendations for Catalan institutions and companies

In the light of the above information, investing or collaborating with military industry, private security and technological security in Israel implies potential violations of international law and human rights, given that it is a sector based on expertise acquired in the occupation of Palestine and the infrastructure of apartheid on the West Bank and in the Gaza Strip.

To avoid complicity with serious violations of human rights and international humanitarian law, and in the spirit of promoting peace and peaceful transformation of conflicts, the Observatory for Human Rights and Business in North Africa and the Middle East finds:

- That authorities should become fully aware that, by participating in initiatives that promote the technological development of the Israeli army and agencies linked to it, they are sending a clear message of approval of Israeli aggression, including war crimes and possible crimes against humanity.
- That in none of the documents prepared by ACCIÓ in relation to business promotion in Israel has any information been found about the risks and impact in terms of human rights and international humanitarian law when doing business with Israel. Some ACCIÓ documents even identify Jerusalem as the capital of Israel[45]. It is a basic responsibility and duty of public agencies for business promotion to provide enterprises with complete, clear and suitable information about the Israeli - Palestinian conflict and the legal and ethical implications involved in establishing partnerships with certain agents in the Israeli market.
- That Catalan institutions should establish effective mechanisms for monitoring Catalan enterprises that participate in dual-use projects and with business agents that carry out activities that are complicit with the occupation of Palestinian territory and with violations of human rights.

[1] <https://www.israelhlscyber.com/> (Retrieved 1 November 2016)

[2] Notes de premsa | ACCIÓ. (2017). Accio.gencat.cat. <http://accio.gencat.cat/cat/empresa-ACC1O/premsa/noticies-notes-premsa/2016/israel_ciber-seguretat.jsp> (Retrieved 20 August 2017)

[3] Idem.

[4] Embassy of India, Tel Aviv. The Cybersecurity Sector in Israel 2015. Indembassy.co.il. https://www.indembassy.co.il/pdf/Report-on-the-Cybersecurity-Industry-in-Israel.doc (Retrieved 20 August 2017)

[5] Notes de premsa | ACCIÓ. (2017). Accio.gencat.cat. <http://accio.gencat.cat/cat/empresa-ACC1O/premsa/noticies-notes-premsa/2016/israel_ciber-seguretat.jsp> (Retrieved 20 August 2017)

[6] Klein, N. (2007). The Shock Doctrine: The Rise of Disaster Capitalism (London: Allen Lane, Penguin). p. 306

[7] Hayes, B., Rowlands, M., & Buxton, N. (2009). NeoConOpticon: the EU security-industrial complex (p. 5). Amsterdam: Transnational Institute.

[8] European Commission - PRESS RELEASES - Press release – Franco Frattini, European Commissioner responsible for Justice, Freedom and Security, "New challenges, new opportunities", Security Research Conference, Berlin, 26 March 2007. Europa.eu. <http://europa.eu/rapid/press-release_SPEECH-07-188_en.htm> (Retrieved 20 August 2017)

[9] The rise of the UK's private security companies - BBC News. (2010). BBC News. <http://www.bbc.com/news/business-11521579> (Retrieved 20 August 2017)

[10] Pingeot, L. (June 2012). Dangerous partnership: private military & security companies and the UN. In New York: Global Policy Forum.

[11] RiskMap 2016 of ControlRisks. <https://riskmap.controlrisks.com/> (Retrieved 9 October 2016)

[12] Maritime Cyprus Admin (19 April 2016). The Security Association for the Maritime Industry (SAMI) Announces Voluntary Liquidation. Maritime Cyprus. <https://maritimecyprus.com/2016/04/19/the-security-association-for-the-maritime-industry-sami-announces-voluntary-liquidation/> (Retrieved 20 August 2017)

[13] European Commission - PRESS RELEASES - Press release - EU, Israel sign Horizon 2020 association agreement. Europa.eu. <http://europa.eu/rapid/press-release_IP-14-633_en.htm> (Retrieved 20 August 2017)

[14] Vrede.be (3 June 2013). European Commission confirms: Millions of EU-Research Money flows to Israeli Arms Industry. Vrede.be. <https://www.vrede.be/nieuws/european-

commission-confirms-millions-eu-research-money-flows-israeli-arms-industry> (Retrieved 20 August 2017)

[15] European Commission CORDIS : Projects and Results : Home. Cordis.eu. <http://cordis.europa.eu/projects/home_en.html> (Retrieved 20 August 2017)

[16] Further information at Iserd.org.il. <http://www.iserd.org.il/_Uploads/dbsAttachedFiles/ISERD_STAT_JULY_2016.pdf> (Retrieved 20 August 2017)

[17] Projects. Iserd.org.il. <http://www.iserd.org.il/?CategoryID=443> (Retrieved 20 August 2017)

[18] Russ Read (2 August 2016). The Israeli Company That Fenced In Gaza Wants To Build Trump's Border Wall Via @dailycaller. The Daily Caller. <http://dailycaller.com/2016/08/02/this-israeli-company-that-fenced-in-gaza-wants-to-build-trumps-border-wall/> (Retrieved 20 August 2017)

[19] NeoConOpticon - The EU Security-Industrial Complex (6 Jul. 2015.). Tni.org. <https://www.tni.org/files/download/neoconopticon_0.pdf> (Retrieved 20 August 2017)

[20] Further information (21 Aug. 2017) at European Commission CORDIS : Projects and Results : European Global Border Environment. Cordis.eu. <http://cordis.europa.eu/project/rcn/88217_en.html> (Retrieved 20 August 2017)

[21] Further information at European Global Border Environment (GLOBE). 2020-horizon.com. <http://www.2020-horizon.com/GLOBE-European-Global-Border-Environment(GLOBE)-s13095.html> (Retrieved 20 August 2017)

[22] Further information at European Commission CORDIS : Projects and Results : Final Report Summary - TALOS (Transportable Autonomous patrol for Land bOrder Surveillance). Cordis.eu. <http://cordis.europa.eu/result/rcn/140453_en.html> (Retrieved 20 August 2017)

[23] NeoConOpticon - The EU Security-Industrial Complex (6 July 2015). Tni.org. <https://www.tni.org/files/download/neoconopticon_0.pdf> (Retrieved 20 August 2017)

[24] Horizon 2020 Projects (19 August 2014). Israel boycott petition receives Irish support - Horizon 2020 Projects. Horizon 2020 Projects. <http://horizon2020projects.com/global-collaboration/israel-boycott-petition-receives-irish-support/> (Retrieved 20 August 2017)

[25] Guidance note — Research with an exclusive focus on civil applications (6 November 2015). European Commission, Directorate-General for Migration and Home Affairs. Ec.europa.eu. <http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-civil-apps_en.pdf> (Retrieved 20 August 2017)

[26] Ethics for researchers (28 October 2013). European Commission, Directorate-General for Research and Innovation. Ec.europa.eu.

<http://ec.europa.eu/research/participants/data/ref/fp7/89888/ethics-for-researchers_en.pdf> (Retrieved 20 August 2017)

27 Peter Beaumont (12 September 2014). Israeli intelligence veterans refuse to serve in Palestinian territories. The Guardian. <http://www.theguardian.com/world/2014/sep/12/israeli-intelligence-reservists-refuse-serve-palestinian-territories> (Retrieved 20 August 2017)

28 OECD (12 July 2017). Research and development (R&D) - Gross domestic spending on R&D - OECD Data. <http://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm> (Retrieved 20 August 2017)

29 Global Competitiveness Index. Competitiveness rankings. Global Competitiveness Index. <http://wef.ch/2do4yfC> (Retrieved 20 August 2017)

30 Yozma Homepage. Yozma.com. <http://www.yozma.com/home/> (Retrieved 20 August 2017)

31 Embassy of India, Tel Aviv. The Cybersecurity Sector in Israel 2015. Indembassy.co.il. <https://www.indembassy.co.il/pdf/Report-on-the-Cybersecurity-Industry-in-Israel.doc> (Retrieved 20 August 2017)

32 Embassy of India, Tel Aviv. The Cybersecurity Sector in Israel 2015. Indembassy.co.il. <https://www.indembassy.co.il/pdf/Report-on-the-Cybersecurity-Industry-in-Israel.doc> (Retrieved 20 August 2017)

33 Washington Post (19 June 2012). U.S., Israel developed Flame computer virus to slow Iranian nuclear efforts, officials say. Washington Post. <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> (Retrieved 20 August 2017)

34 Jonathan Webb (24 August 2016). Fugitive CEO Kobi Alexander Returning To U.S. After Decade On The Run. Forbes. <https://www.forbes.com/sites/jwebb/2016/08/24/fugitive-ceo-kobi-alexander-indicted-to-us-after-decade-on-the-run/> (Retrieved 20 August 2017)

35 NSC Natural Speech Communication Ltd. Iaesi.org.il. <http://www.iaesi.org.il/Eng/?CategoryID=329&ArticleID=918> (Retrieved 20 August 2017)

36 Israel's Cyber Security Sector Overview. Israel Export Institute. Export.gov.il. <http://www.export.gov.il/files/cyber/CyberPresentation.pdf?Redirect=no37> (Retrieved 20 August 2017)

37 The first surveillance drone was launched in 1979 under the name of Scout.

38 Human Rights Watch (30 June 2009). Precisely Wrong. Human Rights Watch. <https://www.hrw.org/report/2009/06/30/precisely-wrong/gaza-civilians-killed-israeli-drone-launched-missiles> (Retrieved 20 August 2017)

[39] Dobbing, M. & Cole, C. (10 January 2014). Israel and the Drone Wars. p. 10 Dronewarsuk.files.wordpress.com. <https://dronewarsuk.files.wordpress.com/2014/01/israel-and-the-drone-wars.pdf> (Retrieved 20 August 2017)

[40] Idem., p. 11

[41] Privacy International uncovers widespread surveillance throughout Central Asia, exposes role of Israeli companies. Privacyinternational.org. <https://www.privacyinternational.org/node/429> (Retrieved 20 August 2017)

[42] Rice, M. Not just the NSA: Surveillance company selling system to spy on mobile phones worldwide. Privacyinternational.org. <https://www.privacyinternational.org/node/61> (Retrieved 20 August 2017)

[43] Tacy Ltd - Israeli company at center of Zimbabwe election-rigging allegations. Diamondintelligence.com. <http://www.diamondintelligence.com/magazine/magazine.aspx?id=12033> (Retrieved 20 August 2017)

[44] Thomas Fox-brewster (25 August 2016). Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. Forbes. <https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/> (Retrieved 20 August 2017)

[45] For example, International Innovation Program (23 March 2016). Accio.gencat.cat. <http://accio.gencat.cat/cat/binaris/Mapa%20ISRAEL%20TIC_tcm176-226629.pdf> (Retrieved 20 August 2017)