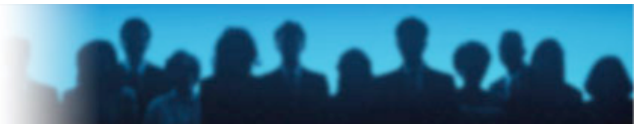
thenewtransparency
surveillance and social sorting



Working Paper III:

The Political Economy of Israel's Homeland Security/Surveillance Industry

by Neve Gordon*

April 28, 2009

* Ben-Gurion University, Beer-Sheva, Israel, ngordon@bgu.ac.il

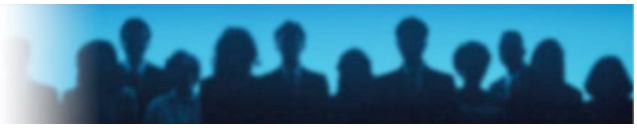
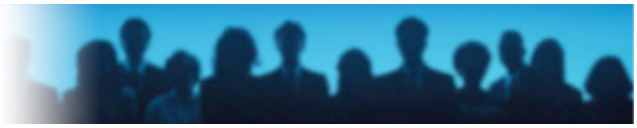


Table of Contents

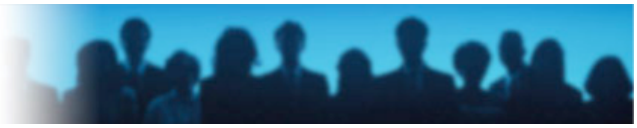


Introduction: Experiencing Horror

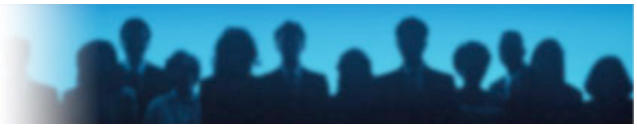
"No other advanced technology country has such a large proportion of citizens with real time experience in the army, security and police forces," reads a glossy government brochure entitled Israel Homeland Security: Opportunities for Industrial Cooperation.[1] In the brochure's chapter called "Learning from Israel's Experience" one reads that, "Many of these professionals continue to work as international consultants and experts after leaving the Israel Defense Forces, police or other defense and security organizations. Typically, these former officers, who also include scientists and engineers, not only have hands-on experience and know-how of traditional security activities, they are also familiar with the broad range of high-tech technologies and equipment, which are available to enhance safety and make security systems more efficient and effective."[2] The Israeli experience, in other words, is considered to be integral to Israel's homeland security, one that provides it with a comparative advantage as it competes in the global markets. Indeed, experience is a pervasive trope in the brochures and websites marketing Israeli homeland security products and services.

Nonetheless, the Israeli experience is deployed in an interesting way, a way that is rarely discussed in the "experience economy" literature.[3] "Experience economy" routinely refers to the phenomenon of people purchasing experiences from fitness clubs, touring agencies, theaters, concert halls, and the like, where these businesses promise to engender memorable events for their customers. It is the experience itself as well as the subsequent memory of the experience that are being sold.[4] Joseph Pine and James Gilmore mention the Disney World experience as a paradigmatic example, and Martin Jay discusses the fear we feel when watching horror films or the thrill we get from an amusement park ride. "We experience these emotions second hand," Jay says, "knowing that we are safe even as we scream. In the horror movie, for example, we self-consciously watch a virtual horror and can hide our eyes while we sit in our seats rather than run away."[5] Thus, the "experience economy" tends to denote both real and virtual experiences created by businesses, which people pay to undergo for a certain period of time.

The "experience economy" of the Israeli homeland security industry seems to be quite different since it introduces the process of packaging and selling Israel's own lived experience to someone else. Israel's homeland security industry, in other words, sells its products and services by maintaining that Israel has experienced the horror -- not virtually, but first hand -- and consequently both knows how to deal with such horror and has developed the appropriate instruments to do so. The rationale is, no doubt, similar to the one used when selling expertise, but it is also distinct in that the homeland security expertise is a product of an "Israeli experience" that is, at least ostensibly, the result of political circumstances not governed by those who undergo the experience – not unlike the experience of the protagonist in a horror film who finds him or herself in an unwelcome situation. The expert is a product of controlled training, while the Israeli experience with suicide bombers developed as a result of many years of confrontation with the unpredictable. In the parlance of Israel Livnat, the president of a leading homeland security company called Elta Systems, "Israel has been meeting the challenge of terror for decades before 9/11, and in those years of hands-on, real-time experience in overcoming terror lies our country's first competitive advantage."[6]



In this report, I argue that the "Israeli experience," in its various manifestations, has played a pivotal role in the formation of Israel's homeland security industry and helps explain the industry's subsequent transformation into a global success story. But before examining how the Israeli experience has operated, I begin with a historical overview. In Chapter One, I describe the Israeli homeland security and surveillance industry, and situate it within the Israeli economy. I also briefly contextualize it within the global security industry. In Chapter Two, I discuss the historical processes leading to the emergence of the homeland security sector in Israel, focusing on the Israeli military, the military industry and the high-tech industry. Finally, in the Third Chapter I explain Israel's comparative advantage, showing how the success of this industry is intimately tied to different kinds of Israeli experiences that have been created by the security forces and military industry. An analysis of the political economy of Israel's homeland security industry accordingly reveals that there is an economic motivation to produce and reproduce the so-called security related experiences and to diversify them. By way of conclusion, I claim that the Israeli experience is perceived as extremely valuable and attractive because it manages to connect between a hyper-militaristic existence, a neoliberal economic agenda, and democracy.



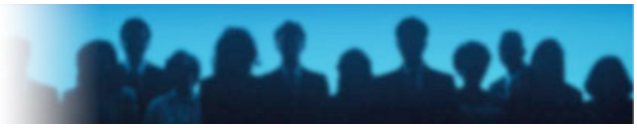
Chapter One: Israel as a Homeland Security/Surveillance Capital

In preparation for the 2008 Beijing Olympics several Israeli companies received contracts to help provide security during the games. Nice Systems was selected to upgrade the security network in 20 subway stations in Beijing. A company press release noted that Nice will connect the subway stations to a security system, which "will be monitored from the station monitoring room and from the central command and control center, giving security personnel the power to identify risk, make optimal decisions, and take action that improves security. Nice's advanced real-time distributed digital video solution will spot suspicious packages left behind on a crowded subway platform and automatically alert security personnel. The solution will also be utilized to automatically detect unauthorized entry into secured areas. The result is a better control of potential threats and enhanced commuter safety."[7]

DDS was awarded the contract to supervise access control in ten Olympic facilities. Since its foundation in 1986, DDS has installed over 45,000 systems in 40 countries. Its clients include major international firms such as Airbus Industries, Lucent, Motorola, Intel, Nokia, City Bank and Oxford University. In Beijing, DDS installed its one-card-solution managing system (smart cards) in 2000 doors. Among the ten sites it was responsible for is the residential area of the Olympic Village which accommodated 15,000 athletes in 42 buildings. In this site alone there are 700 doors and 190 elevators that need to be supervised as well as a clinic, restaurants, a library, a recreation center and sports facilities. Another site is the Media Center, which will function as the technology support and communication center of the games, and will provide services for an estimated 20,000 journalists, all of whom will use DDS solutions to access 200 doors.[8]

ClickSoftware Technologies, which has headquarters in Israel and Massachusetts, and offices in Europe and Asia Pacific, was also contracted by the Chinese government; its responsibility was to manage the field activities of hundreds of telecommunication technicians during the Olympics. The company provides mobile workforce management and service optimization software, and has over 100 customers across a variety of industries and geographies. In Beijing, its software was used to optimize the scheduling operations of several hundred technicians responsible for break/fix, installation and maintenance work. The activities of these technicians were centrally managed from the Olympic Games telecommunications control center.[9]

The fact that Israeli companies were chosen to supply such services is not only a reflection of Israel's military relations with China but also of the visibility of Israeli security firms in the global arena.[10] Already in the 2004 Athens Olympic Games, fifteen Israeli companies were involved in a $200 million project that included venue protection, command and control rooms, maritime and airport security, urban security, crowd control, preparation of law-enforcement units, access control, and communications. The Olympics, moreover, are merely one of many international venues that Israeli homeland security and surveillance companies are routinely involved in.[11] Others include professional fairs, financial institutions, airports, nuclear plants and borders. Israeli high-tech companies specialize in site protection, command and control rooms, maritime and airport security, urban security, crowd control, preparation of law-enforcement

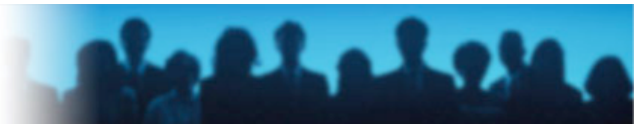


units, access control, and communications. They are among the pioneers of biometric technologies for ID verification, radio frequency identification (RFID) technologies, computer security and electro-optical night vision systems. Their customers include governments, police and security agencies, banks and commercial corporations, airlines, oil, energy and utility companies as well as private consumers in well over one hundred countries.[12] Nice, for example, currently boasts over 24,000 customers in 100 countries, with 85 of the Fortune 100 companies on its list. American Express, JP Morgan and Federal Express are among its clients, as are an array of Police Departments, the Federal Aviation Authority in the United States and the European Space Agency. In 2007, the company's revenues reached $519 million, well above the $418 million revenues of 2006.[13] All incoming telephone calls to the Los Angeles and New York City police departments are recorded on Nice technology, as are roughly 90 percent of the transactions at brokerage firms worldwide. Israel, in other words, has successfully positioned itself as a global homeland security capital.

It is important to underscore at this point that I conceive homeland security and surveillance not merely and perhaps even primarily as guaranteeing security against terrorism or criminal offences. The exponential global growth of this industry should be considered as a manifestation of the evolvement of surveillance societies, whereby surveillance, in Lyon's words, "has spilled out of its old nation-state containers to become a feature of everyday life, at work, at home, at play, on the move. So far from the single all-seeing eye of Big Brother, myriad agencies now trace and track mundane activities for a plethora of purposes. Abstract data, now including video, biometric, and genetic as well as computerized administrative files, are manipulated to produce profiles and risk categories in a liquid, networked system. The point is to plan, predict, and prevent by classifying and assessing those profiles and risks."[14]

Two points should be stressed here. First, one should be cautious about concluding that surveillance societies are constituted by the new security industry and its innovations. The notion of surveillance society does not refer to technological improvements, but rather as Lyon argues to the idea that a "certain kind of watching, both literal and (more often) figurative, have become the preferred means of maintaining – indeed creating – social order."[15] Second, although the declared objective of the security industry is to sell safety by taming different kinds of risks, the products and services it offers also fulfill a less obvious (and some might say more pernicious) role. The industry's overall objective is to help governments and businesses conduct their operations more efficiently and cost-effectively by using new and ever more sophisticated surveillance and authentication technologies in order to advance what Lyon has called "social sorting."[16]

Social sorting refers to a variety of surveillance practices that both create various databases and have access to others – public services, police, intelligence, business, consumers – in order to categorize people for different treatment. Codes, usually processed by computers, Lyon explains, "sort out transactions, interactions, visits, calls, and other activities; they are the invisible doors that permit access to or exclude from participation in a multitude of events, experiences and processes."[17] Thus, both homeland security and surveillance are being extensively deployed not only to monitor – an array of activities ranging from terrorist suspects to critical infrastructure sites, gated communities, hospital and schools, and consumer behaviour – but as a prime instrument of social sorting that discriminates between one person and another on the basis of a



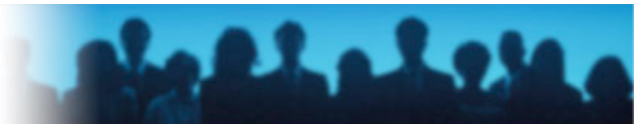
computer profile or data image.[18] So while homeland security and surveillance are deployed (often without the person's knowledge) to catch criminals and terrorists, the very same technologies are also used, for example, to identify suitable customers for specific products. The notion of "taming risks," mentioned above, should accordingly be considered not only in the security sense of the term, but in a much broader sense that includes the financial risks of the corporation and the like. The point is that the global security industry as well as the Israeli one actually produce the products and provide the services that facilitate social sorting in its broadest sense, but they tend to present themselves merely as a supplier of safety in its circumscribed anti-terrorist/criminal security sense.

Before examining how Israel managed to secure such a prominent place in this global market, it is first important to map out this industry, while paying special attention to its foremost component, surveillance.

1.1 The Size of Israel's Homeland Security/Surveillance Industry

Israel's homeland security industry, which is currently featured on the homepage of numerous government websites, is part of what Barrie Stevens defines as the global security industry, an "aggregation of hundreds of thousands of businesses and individuals whose aim is to sell safety from malevolent acts threatening life, property and other assets, and information. The products and services generated range from fire and burglar alarms, locks and safes, through electronic access control and biometrics, electronic article surveillance and security consulting, to armored car services, guard equipment and security fencing."[19] The market for this industry is estimated to have reached $150 billion in 2007, and is predicted to grow substantially over the next decade.[20] Its remarkable expansion is firmly tied to the 9/11 terrorist attacks and the ensuing war on terror, and, as the above citation from Livnat intimates, the Israeli companies have capitalized on these developments. But the growth of this industry is also intricately linked to global political, social, economic, and cultural processes. On the one hand, it is tied to the increasing movement of people, goods and services across political borders, and the ongoing attempt of different government agencies and businesses to find ways of decreasing the risk of smuggling, theft, drug trafficking, counterfeiting, illegal entry, disruption to global supply networks, and so on.[21] These processes call for the introduction of more sophisticated forms of social management and control, some of which are unrelated to the transnational movement of people and goods. On the other hand, there is a growing perception that governments alone are incapable of adequately addressing the risks, which has led to the rise of private security contractors and to the development of new technologies whose objective is to offer protection.[22]

Israel's homeland security industry is characterized by a decentralized and diffused production process. Its major component, as mentioned, is surveillance, by which I mean, following David Lyon, the production of goods, services, technologies and mechanisms that facilitate "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."[23] By surveillance industry, I mean an industry that manufactures products, provides services, and carries out R&D directly related to the surveillance of behavior of individual subjects, social trends and classifications, as well as biological, ecological and environmental processes. Here I examine only the surveillance industry which is part of Israel's homeland security industry, while refraining from touching



upon industrial developments relating to medical supervision or environmental monitoring. At least with respect to medical supervision, Israel has made considerable headway as well.

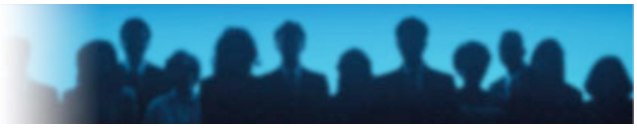
Israel's homeland security and surveillance industries are not considered a distinct sector according to the country's Central Bureau of Statistics (which is tied to an international coding system), and therefore it is difficult to obtain precise data about these industries. An indication of the size of these industries can be deduced from a website that advertises jobs in Israel. One sector is entitled "Security, Safety, Defense" and lists 334 homeland security companies looking for employees, the vast majority of which are surveillance companies.[24] More importantly, the Israel Export and International Cooperation Institute (IEICI), a government funded organization that facilitates trade opportunities, joint ventures, and strategic alliances between international businesses and Israeli companies, divides Israel's export industries into different categories than those used by the Central Bureau of Statistics and includes homeland security as a sector. This in itself is interesting since the categories used by IEICI are more flexible and dynamic and reflect existing market trends rather than the all too static categories determined by the different bureaus of statistics around the world. Also interesting to note is that similar trade institutes in Ireland, Taiwan and India – countries that have also enjoyed a high-tech boom similar to Israel's – do not consider homeland security as a separate sector within the high-tech industry, thus intimating that at least in this sense the Israeli case is unique.[25]

IEICI offers a glimpse into Israel's homeland security/surveillance industry, both in terms of the number of companies that deal directly with surveillance and the vast variety of surveillance products and services which these companies offer. On its website, which can be accessed in Hebrew, English, Arabic and Chinese, Israel's exports industries are divided into 18 general categories. One category is defined as Security and Safety (subtitled Security and Homeland Security Industry) and includes a total of 18 sub-categories almost all of which are tied to surveillance. They include Access Control, Biometrics, C4I, Consulting Training and Services, Intrusion Detection, Observation and UAVs, Perimeter Security, Sensors Detection and Screening, Tracking and Motion Detection, and Video Surveillance. According to IEICI the Security and Homeland Security (HLS) industry includes over 600 companies employing about 25,000 people, while over 300 of these companies export products and services.[26]

An IEICI brochure, which provides a general overview of this industrial sector, explains that,

The events of September 11, 2001 changed the global perspective on terrorism. Countries around the world are now searching for tools to combat the threat of terrorism, and many of these technologies can be supplied by Israel's security and HLS industry. Hundreds of Israeli companies offer sophisticated security solutions ranging from automated speech recognition systems and remote sensors, to video image location and identification, early warning devices and advanced tactical imaging systems.[27]

The brochure goes on to note that "Israeli security and HLS companies are successfully partnering with key world players to ensure public safety, protect airports, seaports, government offices, financial institutions, recreational centers, and more."[28] The fact that these companies provide services to financial institutions, recreational centers as well as other civilian facilities underscores that the HLS has gone a long way in undermining the distinction between the military and civilian spheres. Indeed, non-military related exports from Israel's HLS industry, which include products to schools, banks, shopping malls, and hospitals, amounted to about $3



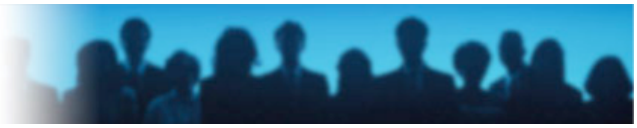
billion, $1 billion for security products (for civilian use) and another $2 billion for Information Technologies (IT).[29] This is one of the ways in which the HLS industry and within it the surveillance industry is very different from the more traditional military industry (more about this below), since the latter continues to cater primarily to military and security institutions.

But the Security and Safety category is not the only one on IEICI's list that deals with homeland security and surveillance. Another seemingly unrelated category called Automotive and Subcontracting includes the sub-category Innovative Technologies, Driver Assistance and Security Systems. Under this sub category one finds companies like Cellocator that produce automotive vehicle location equipment and E-Drive Technology, which allows "fleet managers to monitor practically all driving activities and serviceability of their vehicles."[30] The list of companies providing similar car surveillance mechanisms goes on and on.

Then there is the Aviation and Aerospace category, which lists companies that manufacture numerous kinds of unmanned aerial surveillance, reconnaissance and target acquisition products as well as border and coastal surveillance equipment. Israel is one of the leading producers of unmanned aerial vehicles (UAVs), which are currently used mostly for military surveillance, but which, according to Rand Corporation, could be deployed in the near future to monitor resources such as forest and farm lands, wetlands, dams, reservoirs, wildlife (e.g., in nature reserves) or traffic.[31] According to (incomplete) data from the Stockholm International Peace Research Institute (SIPRI), of all UAV systems transferred internationally between 2001 and 2005, 68 percent were Israeli-supplied. With the US's Predator and Pioneer models both based on Israeli designs, and IAI and Elbit cornering most of the remainder of the export market, UAV transfers overwhelmingly involve Israeli-designed systems.[32] Under the Aviation and Aerospace category one also finds companies that manufacture products such as surveillance pods and aerostat balloons that boast user friendly 360 degree observation coverage, 24-hour unmanned aerial surveillance capability, quick deployment, and low maintenance and operation costs. [33]

In addition, the sub category of Airport Equipment and Services lists companies that export perimeter intrusion and detection systems, all of which are part of the surveillance industry. In a government brochure called "Securing the Skies" one reads that "it is highly unlikely that a 9/11-style attack could be perpetrated against Israel." This, the brochure explains, is due to Israeli experience in fighting terrorists and the ability to develop strategies and technologies to deal with terrorist threats. Nice Systems, for instance, developed products that broadcast video signals to ground control centers during the flight as well as video recorders installed in airplanes enabling pilots to continually monitor events in the passenger cabin.[34]

Even before the plane takes off a comprehensive screening of passengers and their baggage has for many years been routine practice in Israel. A government brochure notes that an "important aspect of passenger screening is passenger profiling, so that security staff can devote more time to those travelers who arouse greater suspicions." The brochure goes on to maintain that the "large numbers of civilian staff working at the airport must be carefully vetted, prior to being hired and monitored on a regular basis. It is especially important to thoroughly scrutinize maintenance, cleaning and catering professionals, who regularly board the aircraft between flights."[35] In terms of passenger baggage, the security staff can then use software developed by A-EYE Advanced Vision Technologies whose applications include more efficient operation of



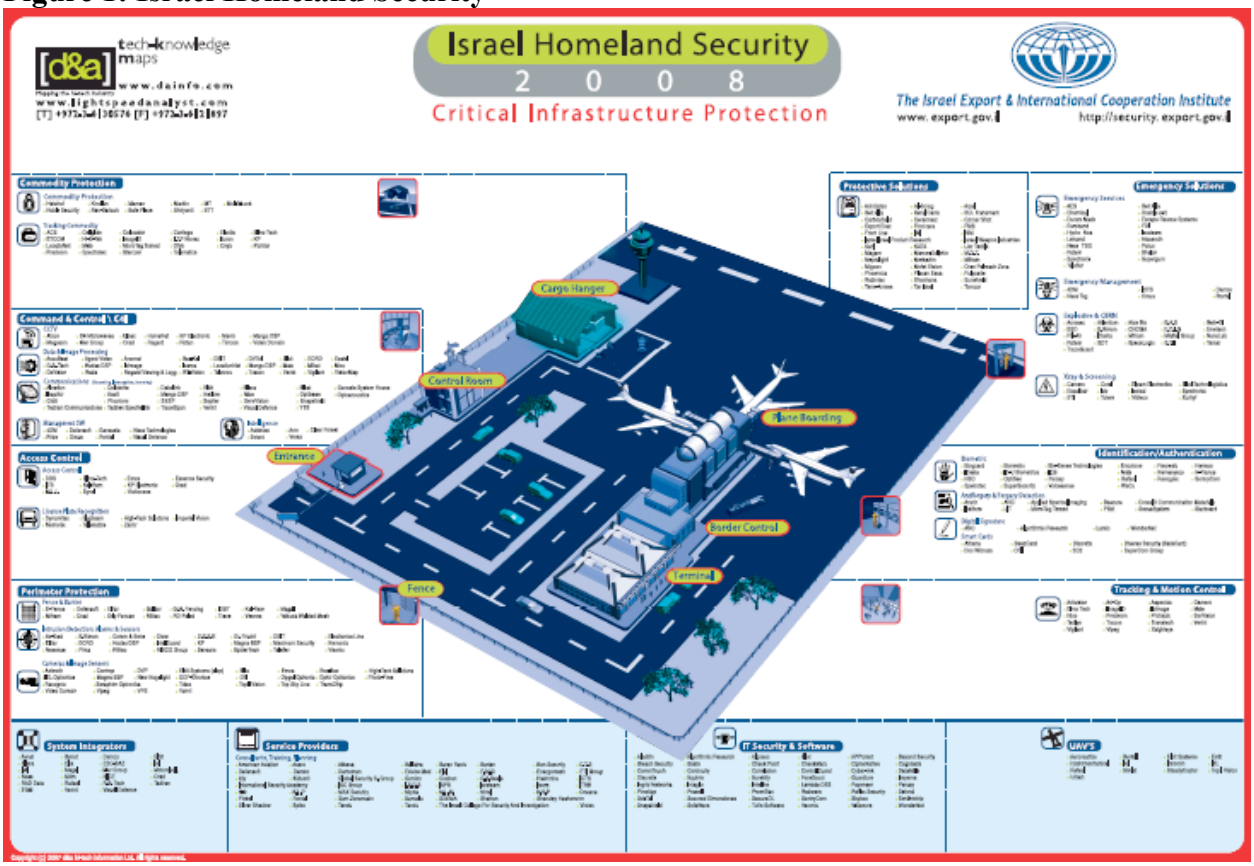
x-ray security scanning systems for detecting concealed weapons and explosives, or the systems developed by SpaceLogic to ensure more efficient and secure baggage handling at airports. Israel has also developed strategies and technologies for securing the airport itself, which include perimeter fencing integrated with comprehensive command and control systems, alarms, and sensors as well as trained manpower to handle any threat.[36]

It is therefore not surprising that following an international meeting on homeland security which convened in Jerusalem, US Homeland Security Secretary, Michael Chertoff, signed an agreement with Israel to share technology and information on methods to improve homeland security.[37] He announced that he would like to adopt some of Ben Gurion airport's security measures - like behavior detection screening, which is considered the cornerstone of the airport's security.[38] In addition to training "behavioral detection officers," the US Transportation Security Administration is examining the Israeli pioneered technology produced by MagShoe, which is designed to detect concealed weapons in shoes and around ankles.[39] The product has already been sold to "one of the world's largest commercial cruise lines, which will use MagShoe on its ships to significantly reduce passenger waiting lines while improving security – especially in high-pressure situations like re-boarding from a port of call in time for departure."[40] These examples provide yet another glimpse into the global standing Israeli enjoys when it comes to homeland and surveillance.

Finally, IEICI website includes Software as a category, which has a sub-category of IT security that includes 104 companies of which 24 deal with surveillance and administration, four with digital signatures, four with biometrics, eight with tokens and smart cards, five with workstation security and surveillance, and 33 with enterprise perimeters. Just like the Software category, Electronics and Telecommunications also include companies that develop products and services for surveillance.

Another source of information about Israel's homeland security and surveillance industries is the Israeli High-tech Knowledge Portal, produced by D&A Visual Insights, a business information company that specializes in creating visualization platforms of data collected from industries. One of its clients is the Israeli government, for which it provides an overview of Israel's high-tech industry. D&A has a database of 1,967 Israeli high-tech companies that is divided into seven categories, of which Homeland Security is one (see Figure 1). Homeland security includes 416 companies or 21 percent of the high-tech sector and is the second largest group after Telecommunications. Under homeland security one finds numerous sub-categories, such as access (17), authentication (40), command and control (74), commodity (28), emergency services (46), IT security and software (11), perimeter (77), protective solutions (5), service providers (78), system integrators (30), and UAV'S (10). The authentication category includes, in turn, its own sub-categories of biometrics (19), smart cards (7), digital signatures (4) and anti-forgery and forgery detection (10). [41] What becomes clear from reading the list and examining the company profiles is that surveillance is by far the most important component of the HLS industry.

Figure 1: Israel Homeland Security

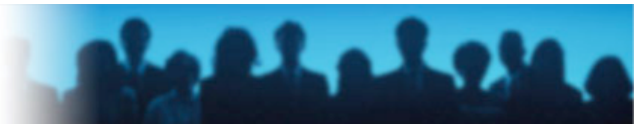


Source: www.dainfo.com

1.2 The Industry's Revenues

In this study, I examined 312 companies that were listed in the 2007 IEICI database as those making up Israel's export oriented homeland security industry. Of these, I found 237 companies (amounting to over 75 percent of the total) that focus on some kind of surveillance (a full list of these companies and their websites is in Appendix 1). Of the surveillance companies, only twelve do not have any high-tech component. These include companies like K-9 Solutions, a company that provides "the most comprehensive and professional canine [dog] security available" and the Mifram Group that builds observation towers.[42] The remaining 225 companies either develop and manufacture high-tech surveillance products or provide services that use sophisticated technologies. Twenty-one of them, comprising almost 10 percent, are traded on NASDAQ.

The amount of revenues generated from Israel's surveillance industry is unclear, and beside the unaccounted for $3 billion round figure provided by IEICI only rough estimates can be produced based on data from Israel's Central Bureau of Statistics. First, many of the companies making up the surveillance industry are part of what the Central Bureau of Statistics, following internationally recognized definitions, calls Information and Communication Technologies (ICT), which is made up, in turn, of two major components: service industries and manufacturing



industries. The service industries include start-up companies, computer and related services and R&D, and telecommunication services. The manufacturing industries include industrial equipment for control and supervision, electronic communication equipment, and electronic components.[43]

In 2006, Israeli ICT exports comprised 30 percent of all of Israel's exports (excluding diamonds),[44] amounting to $15.67 billion, with $8.66 billion coming directly from manufacturing and $7.01 from services.[45] Although not all ICT services and products are directly related to surveillance technologies, certain sub-sectors that appear under ICT like "equipment for control and supervision," include systems for security control, equipment for control towers, and a variety of other products and services that are almost all directly related to surveillance. In 2006, exports from this sub-sector amounted to $2.3 billion, 17.8 percent more than in 2005.[46] Exports of telecommunications, sounds recording and reproducing apparatus and equipment, many of which are also part of the surveillance industry, amounted to $3.58 billion in 2006.[47] These numbers help us gain a sense of the size of Israel's surveillance industry, and yet it is important to emphasize that the data is vague both because we do not know exactly how much of ICT is actually surveillance related and also because surveillance includes companies that are not part of this sector. We can safely assume, though, that the high esteem that Israel's surveillance industry enjoys translates directly into economic profit.

In this context it is important to note that the 237 surveillance companies which I examined do not include companies that produce such technologies -- like InfiniBand and Orthogonal Frequency Division Multiplexing -- which serve as the basis for many surveillance solutions (as well as for a variety of other uses).[48] Eighteen of these companies are traded on NASDAQ, from a total of 67 Israeli companies and some of them have done particularly well in the past years.[49] For example, the 2007 Touche "Fast 500" survey of the fastest-growing firms in the technology, media and telecommunications industries in Europe, the Middle East and Africa, ranked three Israeli firms that produce precisely this kind of technology at the very top of the pyramid: Voltaire, Celltick and Runcom. Voltaire develops software and switching network infrastructure products based on grid and InfiniBand technologies for storage and server systems. It recorded a 50,612 percent growth in sales from 2002 to 2006, with sales increasing from $60,000 to $3 billion over a period of five years. Celltick has developed a product called "livescreen media" which allows one to broadcast targeted content and marketing messages to millions of mobile idle screens, while Runcom has introduced new wireless technology that allows for improved digital video broadcasting.[50] The growth of these two companies during the same five year period was 29,627 and 27,950 percent, respectively. Of the 45 Israeli companies featured on the "Fast 500" list, only two deal directly with surveillance (Ness and Audiocodes), but many produce technologies that have the capacity to substantially improve surveillance capabilities.

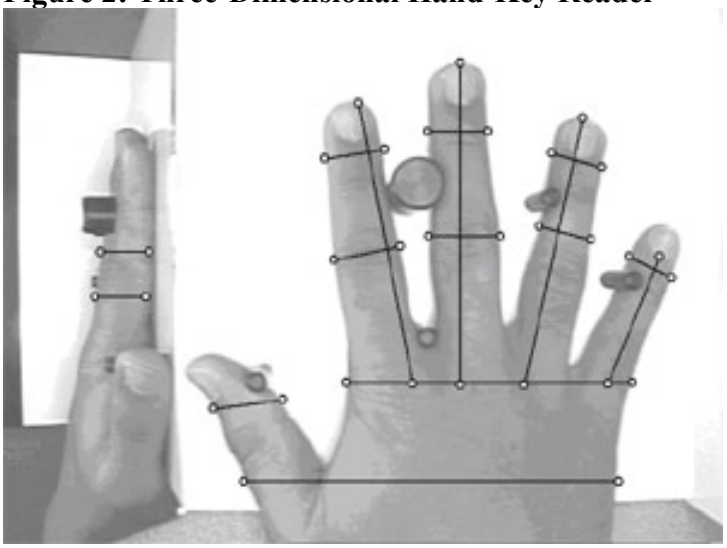
Despite the fact that it is virtually impossible to determine this industry's precise revenues, it seems tenable to assume that Israel's homeland Security/Surveillance industry is comparable and has perhaps even surpassed the revenues of Israel's well-known military industry, whose exports in 2006 amounted to $5 billion and constituted about 10 percent of the global arms sales.[51]

1.3 The Industry's Structure

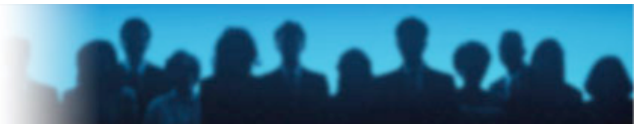
Optisec, one of Israel's smaller biometric companies (it employs seven people), provides a glimpse into the makeup and structure of Israel's surveillance industry. One reads on its website that "one of the major problems facing management today is stolen work hours." The website explains that in the time and attendance market this phenomenon is known as "buddy punching" where one employee swipes two smart cards; first his own card, then the card of a friend who is not at work or late returning to work. According to the American Payroll Association, buddy punching has become an accepted practice and is costing companies 2-7 percent of the payroll, while Business Solution Magazine states that "Employee time theft costs resulting from buddy punching, early or late arrivals are estimated to be $98 billion a year in the United States alone." Optisec concludes that there is only one technology that is capable of eliminating the high cost of buddy punching: Biometrics.[52]

Optisec is a software company that is using biometric know-how mainly for work-force management. Its most important product is software that processes the data from a hand-geometry reader, which uses an infrared light source, much the same as the light used in a typical television remote control, along with a camera chip. People place their hand on the hand-key's reflective surface and when the hand is positioned correctly, the camera records an image which both enables one to enter or exit a facility and records the time and date of entry. Optisec's innovation is its hand-geometry software, which can process a three-dimensional view of the hand in order to determine the geometry and metrics of the finger length, width and other details (Figure 2). The software is an add-on which measures up to ninety different parameters and processes the information via a propriety algorithm. According to the website there are currently an estimated 80,000 hand-key readers being used daily by millions of people clocking in or out of work or accessing facilities and countries.[53]

Figure 2: Three-Dimensional Hand-Key Reader



Source: Optisec Systems



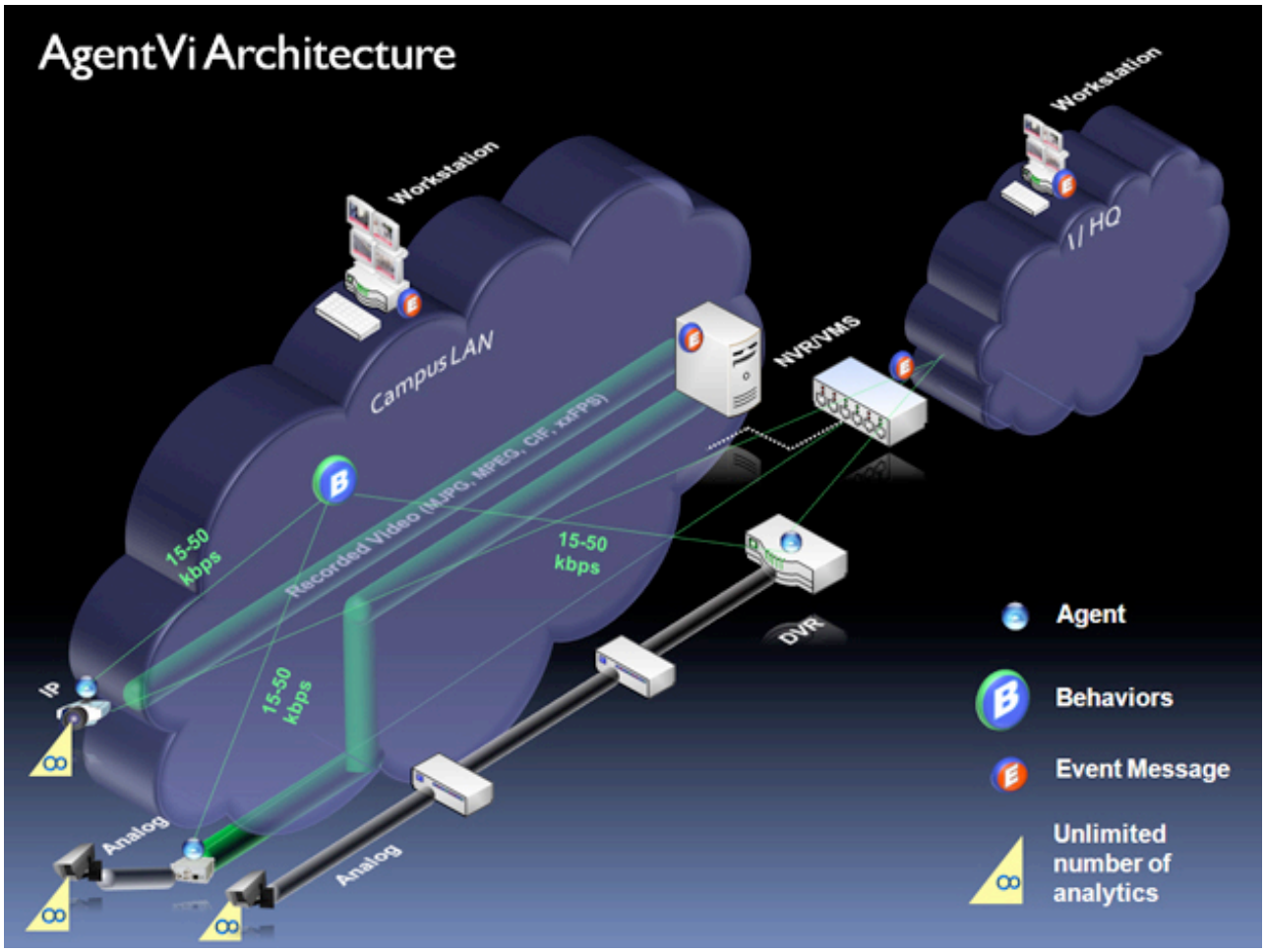
Another Israeli company that gives a sense of this industry is Agent Video Intelligence, which was established in 2003 and in 2007 had 20 employees. The company opens its website with the provocative question: "What is Freedom?" After two seconds the answer appears on the screen: "From one camera, to hundreds of cameras." This slogan reflects the assumptions of many Israeli surveillance companies, which not only conceive surveillance as facilitating and augmenting freedom but also consider the computer as having an emancipatory potential. This particular company has developed software which processes raw images that have been captured by numerous cameras in the field and enables the transmission of images into the network as ultralow bandwidth data packets (usually less than 20Kbps; see Figure 3). Other software is then used to analyze the data, providing "pre-configured detection missions in real time" that generate "meaningful events based on rules defined by the user." Currently this software is used in over 25 countries in retail stores, educational institutions, financial institutions, critical infrastructure sites such as utility, airports, and railway stations, and government offices. The important point in the context of our discussion is that Agent Video Intelligence developed technology that "seamlessly integrates with existing video equipment and IT infrastructure, making video analytics feasible, affordable and scalable." In other words, it is an "add-on" software that aims to improve surveillance capabilities.[54]

The software developed by these and numerous other Israeli companies helps accomplish the specific goals set out by the companies (like the reduction of "buddy punching") but also advances the more general project of social sorting, since such software facilitates both the identification of the subject and the categorization according of social criteria like man, muslim, black, immigrant or woman, student, citizen.

Companies like Optisec and Agent Video Intelligence characterize the majority of firms within Israel's homeland security and surveillance industry, and are very different from the companies that make up the military industry. Indeed, almost all of the arms produced in Israel (over 95 percent) are manufactured by six companies. Four of these companies are state owned (ELTA, IAI, IMI and RAFAEL) and are responsible for about 75 percent of the arms sales, while the two private companies (Elbit systems and Elisra) make up the rest of the sales.[55] The size of the workforce in the military industry (approximately 35,000) is still greater than the size of the workforce in the homeland security/surveillance industry (an estimated 25,000). This indicates that the structure of the military industry is very different from the homeland security and surveillance industry: whereas companies in the military industry employ thousands of workers, most of the companies in the surveillance industry have less than a hundred employees, and many employ between five and thirty people.

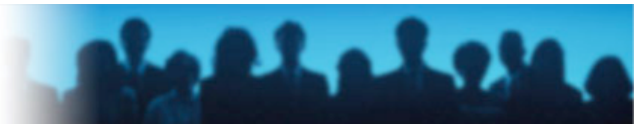
Government regulations pertaining to companies that want to be part of the military industry dictate that during processes of privatization ownership must remain Israeli. Although more research about these regulations is needed, it is obvious from comparing the number of companies in each sector that such regulations do not affect the surveillance industry. Otherwise we would expect to see fewer companies in the surveillance industry as well as less foreign investment. Moreover, some surveillance companies were bought over the years by foreign companies, while others were transformed by their owners into US companies (primarily for tax and sales purposes).

Figure 3: Agent Video Intelligence



Source: Agent Video Intelligence

Another factor that helps shape the difference between the two industries has to do with the products they produce. The production of arms, which is a major component of the military industry and includes ammunition for aircraft and helicopters, artillery rockets, tanks and missiles boats are not products that can be manufactured by companies that employ twenty people. Along similar lines, the production of UAVs and satellites require vast amount of resources, not least in R&D, that companies in Israel's surveillance industry tend not to have. In certain fields the state-owned military industry bears the brunt of paying for R&D and thus subsidizes the so-called private sector. Thus, the high-cost surveillance products tend to be manufactured by Israel's military industry, while the large majority of surveillance companies produce "add-ons" to already existing platforms, offer integration solutions for a variety of existing products, or provide services and training.



1.4 Post-Fordist Mode of Production

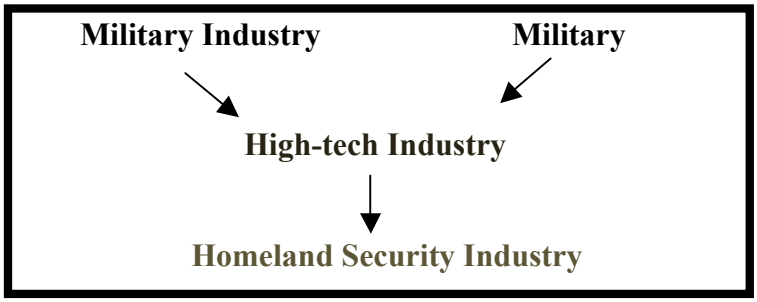
The different structure of these two industries not only suggests that the Israeli homeland security/surveillance industry is more diversified than the military industry, but that they are actually based on different modes of production. Whereas the military industry emerged and developed during the Fordist-era (even though it has over the years adopted numerous post-Fordist traits), the homeland security/surveillance industry was from the very beginning structured along post-Fordist lines. The surveillance industry, in other words, can be characterized as a sector informed by flexible specialization; that is, a flexible production process which is dependent on flexible systems and equipment as well as a more skilled and more flexible workforce. Its crucial hardware is microelectronics-based information, electro-optics and communications technologies.

Furthermore, the post-Fordist industries are also different from the Fordist ones in that they aim to meet the growing demand of increasingly differentiated and segmented markets rather than long runs of standardized commodities for stable mass markets. Theirs is a demand rather than supply driven industry.[56] The diversification and flexibility of this industry along with a few other factors that will be discussed in the next chapter, such as the movement of employees and R&D from the military to the surveillance industry, provides insight into the latter's exponential growth and successful penetration into the expanding post-9/11 surveillance markets.

Chapter Two: The Emergence of Israel's Homeland Security Industry

Obviously, the success of Israel's homeland security and surveillance industry is firmly linked to the shift in demands following the terrorist attacks of 9/11 and the ensuing war on terror as well as the political, economic, social and cultural global processes briefly mentioned in the previous chapter. But the industry's impressive achievements are also due to numerous internal factors. In this chapter, I analyze the impact of Israel's military and military industry on the growth of the country's homeland security/surveillance industry. Following numerous scholars, I maintain that Israel's military and military industry were instrumental in the creation of both a successful high-tech sector and helped shape its orientation so that relatively large segment focuses on homeland security/surveillance (Figure 4).

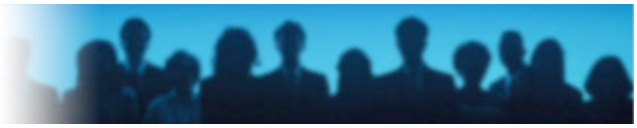
Figure 4: Historical Roots of the Homeland Security Industry



Such internal factors explain the difference between Israel and the high-tech industries in Ireland, Taiwan and India – countries that have also enjoyed a high-tech boom similar to Israel's – but do not have a homeland security sector worth noting. I also accept the widespread claim that the entrepreneurial spirit, the problem-solving attitude and the system-oriented approach characterizing most of the successful high-tech firms in Israel originated in Israel's military and the military industry.[57] I go on to argue that the influence of Israel's two governmental security institutions (military and military industry) helps explain the economic success of Israel's homeland security/surveillance industry as well as why Israel is currently being branded as a global homeland security capital.

2.1 The Military Industry

The foundation of the military industry can be traced back to the pre-state Zionist struggle. The production of weapons and ammunition had already begun in the 1920s, and in 1933 TAAS, which was later renamed the Israeli Military Industries (IMI), was officially established in order to manufacture rifles, mortars, hand grenades and ammunition in underground workshops. The Israel Aerospace Industry (IAI originally called Bedek Aviation Company) was founded in 1953 and is currently Israel's largest military exporter, boasting a record high of $2.8 billion in sales during 2006. In addition, some privately owned firms were established in the 1950s, including Soltam, which manufactures artillery, and Tadiran, which has become the largest military



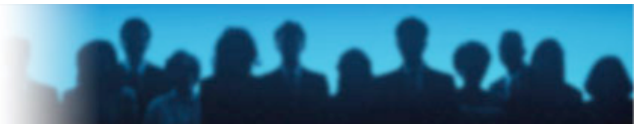
communications equipment manufacturer in Israel. Currently, Israel is considered the sixth largest military exporter.[58]

The success of Israel's military industries is intricately tied to its large investment in R&D. A few years following Israel's creation in 1948, the Ministry of Defense established a research and development division as part of the state-owned military industry, which was subsequently called RAFAEL (Armament Development Authority). RAFAEL was organized like an academic institution and only in 1990 was transformed into a commercial enterprise that also produces and sells weapons.[59] In the mid-1950s the Israeli military initiated its own computing program within RAFAEL and in 1959, RAFAEL, the military intelligence agency, the air force, and the military's logistics department all joined forces to call for the acquisition of a large-scale mainframe computer.[60] At about the same time, the military, which worked closely with RAFAEL, opened a computer school that facilitated the diffusion of computer skills in Israel.

Despite relatively large investments in R&D, until the mid-1960s the military industry employed about 15,000 workers, or roughly 2 percent of Israel's fulltime workforce. On the eve of the June 1967 War, Charles de Gaulle declared a military embargo on Israel due to France's decision to ally itself with the Arab countries. France had been Israel's major supplier of weaponry, including nuclear technology, and De Gaulle's decision put Israel in a bind, since it desperately needed to acquire critical weapons. Following the war, the Israeli government decided to shift vast amounts of resources to Israel's military industry in order to reduce the country's dependency on other states for military equipment. Accordingly, the Israeli government designated the military industry a national priority sector and channeled large sums of money both directly to the industry and to the military, which then purchased products from the industry.[61] By 1975, the number of people employed in the military industry had tripled, reaching approximately 45,000 or 5.5 percent of the fulltime workforce.[62]

As a way of maintaining strategic superiority over the country's Arab neighbors, Israel's military industry focused on high-tech development, concentrating on computer and electronic technologies, electro-optics, aeronautics, mechanical design and metal works, as well as chemical and software engineering. The Israeli government was always heavily involved in the military industry, both as owner of a large segment of this industry and the industry's main customer (through the military). The government also controls military export via a special division in the Ministry of Defense called "Sibat," which is in charge of authorizing export of classified products.[63] For security reasons, however, the military discouraged the commercialization of the new technologies developed in the industry, and worker movement from the state-owned industry to the emerging private sector was negligible. For about a decade the size of the industry's workforce remained relatively static, but in the mid-1980s it was downsized. The downsizing was originally precipitated by an economic crisis in Israel and later by the end of the Cold War.[64]

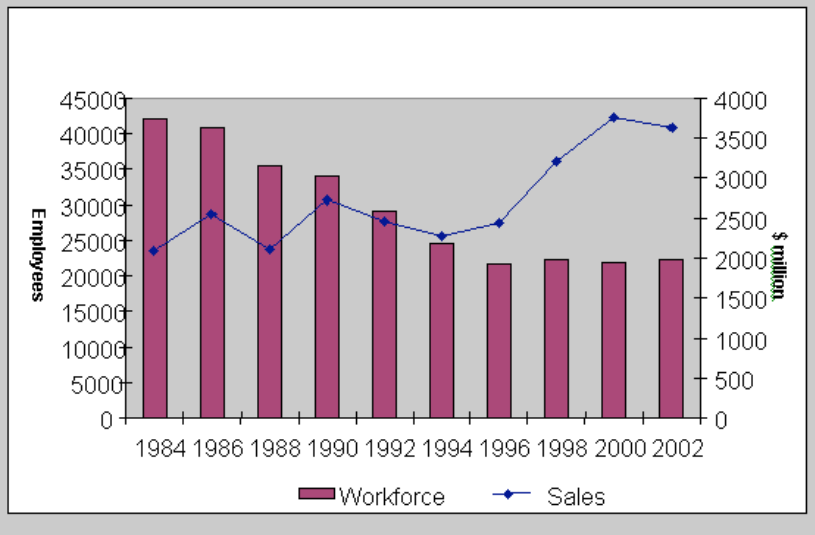
The internal economic crisis led to a structural adjustment program that included a massive reduction in public expenditure and downsizing of the public sector, which helps explain, in Moshe Justman's opinion, Israel's "high-tech revolution."[65] According to Justman, the structural adjustment program precipitated a shift of economic resources from a technologically advanced but commercially unprofitable defense sector to a civilian industry based on similar technologies.



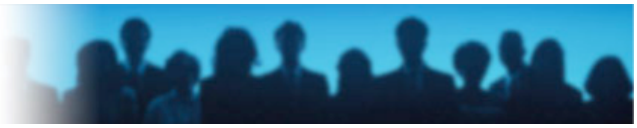
As seen in Figure 5, a "deliberate reduction in domestic defense procurement after 1985 released tens of thousands of skilled workers into the labor market, providing an abundant supply of skilled labor for an emerging high-tech sector and allowing more efficient exploitation of the commercial potential of Israeli R&D."[66]

While Justman underscores several important processes that led to the emergence of a robust high-tech sector in Israel, he fails to acknowledge a variety of significant factors that led to the so-called "high-tech revolution." One of these factors is the global crisis in the weaponry industry, which was caused by the end of the Cold War and the demise of the former Soviet Union. World military spending in 1997 amounted to $740 billion, the lowest level since 1966 and 40 percent below its 1987 peak. The Stockholm International Research Institute (SIPRI) estimate of arms sales for the 10-year period 1988–1997 worldwide shows a decline of slightly more than one-third in real terms, corresponding to an average annual decrease of 4.5 percent. In 1986, armament industries worldwide employed 17.5 million people; by 1995, the figure had dropped to 11.1 million.[67] Thus, the downsizing of Israel's military industry reflects and is intricately tied to global trends and is not merely a reflection of internal structural adjustments. For instance, Israel Military Industries, which makes the Uzi submachine gun and Merkava tank, had shrunk from 14,000 employees in 1990 to 5,000 employees in 1995. RAFAEL, the military's top-secret weapons development authority, ended the 1995 year with 3,000 employees, down from 8,000 in the 1980s.[68] As we will see many of these workers, particularly those with technological skills, helped spur Israel's high-tech industry.

Figure 5: Israeli State-Owned Military Industries -- Employees and Exports



Sources: Sharon Sadeh, "Israel's Defense Industry in the 21st Century: Challenges and Opportunities," *Strategic Assessment,* Vol. 7. No. 1, 2004. IAI, IMI, and Rafael corporate reports; State Comptroller, Ministry of Finance, and Government Companies Authority reports. Figures include subsidiaries, but exclude former employees on companies' payroll.



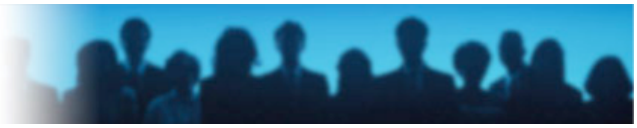
As the sales line in Figure 5 reveals, the military industry was able to expand its markets at a period of global economic decline and personnel downsizing. If in the 1970s exports amounted to between $40-70 million annually, thirty years later exports were eighty times higher and currently amount to over $5 billion.[69] This remarkable shift has to do with the fact that in the 1970s certain corporations (most prominently IAI) decided to shift their research and production interests from major platforms to technologically advanced systems and components. To support the industry's shift and to promote technological innovation, R&D grants were allocated to the military industry from the Chief Scientist's Office within the Ministry of Trade and Industry as well as from other government organs. Indeed, military R&D during the early 1980s amounted to more than half of the total government funded R&D (which also includes both civilian R&D in the business sector and civilian R&D in universities and government laboratories). If in the seventies the military industry's share in total national R&D was about 40 percent, by 1981 it had risen to 65 percent.

Two other issues should also be mentioned. First, the military industry's success in developing cutting edge technology was not only a result of investment in national R&D funding, although that is indeed a key factor, but is also due to the relationship the industry established with US, German and French industries with which it shared technological knowledge.[70] The military industry's cooperation with the U.S. has been particularly instrumental in this regard. Filling the vacuum that France created in the midst of the 1967 War, the US has provided Israel with substantial funds, advanced technologies and military hardware.[71] The industry's decision to begin focusing not only on military markets but also on civilian ones also contributed to its economic growth.[72] By 1999, for example, IAI reported that 39 percent of its revenues came from the civilian sector.[73] Along similar lines, Elbit, which originally specialized in UAV's as well as in aircraft retrofit and modernization of aircraft and helicopters (comprising 38 percent of its sales), currently designs, develops, manufactures, markets and provides services for advanced electronic and imaging systems and products for medical (45 percent), industrial and commercial applications (17 percent).[74]

We now know that the strategic decision to concentrate on military R&D with an emphasis on technologically advanced systems proved advantageous, since it ultimately served to facilitate the foundation of a solid technology-orientated economic base for Israel. While I discuss this issue at greater length below, I can already say here that many engineers, scientists, and managers who were initially employed in the state-owned military industries eventually moved into the private sector where they applied the knowledge and training they had acquired to new projects.

2.2 The Military

The effect of the military industry on Israel's high-tech industry, and by extension homeland security and surveillance industry, will become clearer in a moment. First, though, it is important to highlight the influence of the Israeli military, which has also provided a fertile breeding ground for future generations of high-tech workers and entrepreneurs. In order to understand the impact of Israel's military on its high-tech industry and, more specifically, its homeland security and surveillance industries, it is vital to briefly examine the military's role in Israel's computing history. In 1960, a newly established military unit called MAMRAM (Hebrew acronym for the

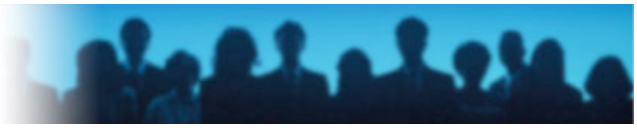


Center of Computers and Automated Recording) was set up and the Philco Transac 2000 mainframe – one of the earliest computers available outside the defense establishments in the US, USSR and UK – was purchased.[75] "With this platform, modern record keeping became part of military management for personnel and logistics." [76] Thus, nine years before the first computer science programs were introduced in Israeli universities and before the official birth of the Israel's software industry in 1969, the Israeli military was already developing software.

In the late 1960s, MAMRAM replaced the Philco with an IBM mainframe, and, as Dan Breznitz points out, it became the largest and most sophisticated computing center in the country While MAMRAM's primacy has eroded over the years, it continues to maintain a key position within the Israeli computing scene simply because it is the largest information technology user and producer in Israel as well as one of the primary customers of software products and main trainers of information technology professionals.[77]

An integral part of MAMRAM is an internal training unit, the first such unit to be created in Israel. This unit became independent in the second half of the 1990s and is now known as the School of Computer-Related Professions; it is, Breznitz explains, the main programming, software engineering and computer users training unit in the military. The School for Computer-Related Professions trains about 300 programmers each year, and they end up serving a minimum of 5-6 years in the military. These programmers receive extensive advanced training throughout their service, including professional courses on specific platforms, systems, and languages (e.g. Oracle, Sun, Linux), basic and advanced software design courses, systems analysis courses as well as infrastructure courses. By the age of 21, the average MAMRAM programmer has extensive experience and has worked on multiple projects, where he or she has served as a team leader. Indeed, approximately one in four programmers acquires extended (i.e. 1–2 years) experience as a manager of a full-scale programming team and 1 in 10 becomes section head who is responsible for a specialized subunit with long-term project management and control. As one school official, who has been working in the private industry for a few decades, observed: "These 21 year old kids have already worked on multiple projects, sometimes even in different units; they are efficient and experienced programmers by that stage."[78]

The School for Computer-Related Professions also trains about 500 application instructors per year, who then train users throughout the military. It trains systems managers for both small and large systems and provides systems analysis courses to military commanders so that they, in turn, can define requirements to systems analysts and programmers in their own units.[79] Breznitz adds that "because the military has tended to define its programming needs for many years in terms of specific software products, and because the computer units have always been defined as service providers, a high level of attention has been given to training these programmers to understand and define their customers' needs. Accordingly, a MAMRAM programmer leaving the army already has several years of experience in analyzing and defining the needs of the 'market' she operates in and in developing products to meet those needs."[80] It is therefore not surprising that Israelis who work in the high-tech industry and carry out their reserve duty in the School for Computer-Related Professions often screen and recruit young soldiers from the unit even before these soldiers are officially released from their active duty – these young computer programmers are, after all, a desirable commodity.[81]



The marketable skills acquired in MAMRAM are apparent also to the heads of this military unit. One of its former commanders put it this way in an interview:

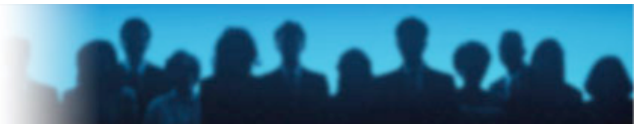
I saw my role as the commander of MAMRAM in the national perspective. In addition to the primary and pure military aims of MAMRAM, another goal is to take part in the building of the human capital of Israel. This is a role that is highly important due to the fact that the universities do not train people in the practical side of software programming in the same way that MAMRAM does. I did not always have the support for that from other parts of the military, but we did it all the same. What we mainly did was (1) push the use of new technologies, (2) establish standard setting and methods using decisions that diffused throughout the industry, and; (3) build infrastructure technologies and pass them on to the whole industry. We stuffed the School for Computer-Related Professions consciously with the best manpower available and used a lot of reserve personnel, which was good for both sides, the industry and us, and created a lot of information flows… the School for Computer-Related Professions has always been seen as the main way to fulfill our national duty—the building of human infrastructure.[82]

In addition to MAMRAM, the air-force, 8200 (i.e., the electronic warfare unit) and other military intelligence agencies have their own computer training programs, which are not as big as MAMRAM, but train, nonetheless, hundreds of young Israelis each year. Indeed, many of the new surveillance entrepreneurs are graduates of these two schools. In 1979, the military also developed a program called Talpiot, which accepts 50 of the most promising high-school students in science and submits them to three years of grueling study in physics, computers and other sciences followed by another six years of military service where they are charged with helping to improve the armed forces through technological innovation. Studies show that most of Talpiot's graduates do not remain in the military and many of them move on to work in Israel's vibrant high-tech industry.[83]

Thus, the military is a conveyor belt for literally hundreds of programmers and application instructors who join the Israeli high-tech industry each year. A study conducted in 1998 by the Center for Technological Forecasts at Tel-Aviv University estimated that 35 percent of the start-up entrepreneurs in Israel were trained in R&D during their military service and that 57 per cent of these entrepreneurs had served as officers in the military.[84] A different study based on twenty-five in-depth interviews with Israeli high-tech entrepreneurs found that the most significant influence on the entrepreneurs' careers was the military experience.[85] All of which helps explain the orientation of Israel's high-tech industry and its emphasis on communications and security.

2.3 Silicon Wadi

Like Japan, Israel lacks natural resources. Its economy is consequently dependent on human capital, which over the past two and a half decades has been channeled into the high-tech industry. The decision to invest in technological innovations within the business sector can be traced back to 1969 when Israel established the R&D Industrial Fund. However, the money allocated to this fund was meager and during the early years most of the R&D projects supported by the fund did not aim to generate knowledge capabilities; rather these projects concentrated on directly marketable outputs.[86] Nonetheless, a few foreign multinational corporations did identify the potential of human capital in Israel. By 1964, Motorola had already opened a R&D branch in Israel, while IBM, Intel, Digital Equipment and others followed suit in the 1970s and 1980s.[87] These multinational corporations understood the advantage of Israeli R&D and introduced a model that was very different from the bottom-up development process, whereby a foreign corporation first opens assembly and manufacturing plants and only later develops more



technologically advanced operations, culminating with R&D centers. Many if not all of the corporations first moved to Israel in order to open R&D branches (see Table 1).[88]

The homegrown industry, however, only received its first real boost in 1984, with the legislation of the R&D law that supported knowledge intensive industries, which significantly increased Israel's R&D grants to science and technology infrastructure.89 This change coincided with the economic restructuring processes within Israel and the ensuing downsizing of the workforce in Israel's military industries.90 While the workers who left the industry and the thousands of Israelis who completed their military service in high-tech related jobs did indeed serve as the necessary core for the private high-tech surge throughout the 1990s, their move from military to civilian enterprises does not tell the whole story.

Table 1: Multinational companies with R&D centers in Israel (partial list)

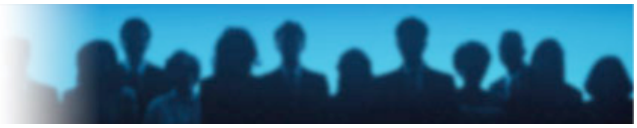
Alcatel
Analog Devices
AMCC
Avaya
BMC Software
Boston Scientific
Broadcom
Computer Associates
CEVA
Cisco
Conexant
Freescale Semiconductor
GE Medical Systems
HP (including HP Labs)
IBM
Infineon
Intel
Interpharm
KLA-Tencor
Kollmorgen Servotronix
Marvell Semiconductor
Microsoft
Motorola
National Semiconductor
Oracle
Orgenics
Paramic Technology
Pfizer
Phillips
QUALCOMM
Samsung
SAP
Siemens
Silicon Graphics
Sun Microsystems
SunGard
Texas Instruments
Veritas Software

Source: Israel Venture

One cannot fully understand the growth of Israel's high-tech industry without taking into account the role of Israeli universities and the immigration of scientists and engineers from the former Soviet Union. Over the years the universities had developed cutting-edge computer science departments and were training hundreds of programmers each year. And although homegrown talent was no doubt crucial, more engineers arrived in Israel in the 1990s than Israel's Technion University had produced since its foundation in 1924.[91] This immigration helps explain why Israel claims the highest proportion of scientists and engineers with postgraduate education in the world: 135 per 10,000 compared with 78 per 10,000 in the US.[92]

A distinct private high-tech sector that modeled itself on the Silicon Valley (and is therefore called Silicon Wadi) emerged in the late 1980s and early 1990s. Indeed, one of the prominent features of the Israeli high-tech world was its close integration with high-tech clusters in the United States; this integration intensified in the second half of the 1990s as more and more Israeli companies moved their headquarters to the US, turning themselves into quasi-American multinationals with their main R&D hubs in Israel. According to Breznitz, for legal, and more importantly for taxation, purposes they wanted to be treated as US companies with an Israeli subsidiary.[93]

By the year 2000, an estimated 3,500 to 4,000 start-ups were operating in Israel, more than one start-up per 1,500 people. From 1990 to 2000 there was a four-fold increase in high-tech sales from over $3 billion to $12 billion and a five-fold increase in high-tech exports from $2.2 billion to $11 billion. The share of the high-tech industries in manufacturing employment increased from 14 percent in 1980 to 19.5 percent in 1998, which was considerably higher than the share of



high-tech employees in most OECD countries.[94] And, in 2000, the information technology industry accounted for over 70 percent of Israel's GDP growth.[95]

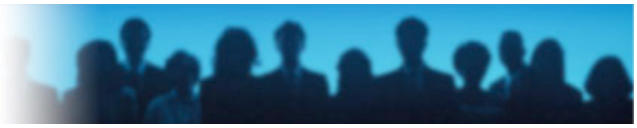
That same year, however, the upward trend changed as a result of the second intifada and the bursting of the global tech bubble. But by 2002, the high-tech industry began climbing back up and has grown rapidly ever since. Currently, Israel boasts the highest concentration of high-tech start-ups per capita, and the second largest in the world in absolute numbers after Silicon Valley. Israeli high-tech has ever-growing net-gains which reached $6.7 billion in 2006 (as compared to a surplus of $2.5 billion in 2002).[96] The Israeli potential was not missed by venture capitalists as can be seen by the dramatic increase in the number of Venture Capital Funds investing in the industry: from two in 1991 to over one hundred in 2001. In 2007, 462 Israeli high-tech companies raised $1.76 billion from local and foreign venture investors, 8.5 percent above the $1.62 billion raised in 2006 and 31.5 percent above 2005 levels.[97] The Israeli high-tech industry's presence in the international arena is also notable; in NASDAQ, for example, 67 out of the 298 non-US companies listed are Israeli, thus positioning Israel in first place among foreign companies.[98]

2.4 Military + High-tech = HLS + Surveillance Industry

Clearly not all or even a majority of Israel's high-tech industry focuses on homeland security and surveillance. And yet, in terms of the number of homeland security/surveillance companies and the revenues these companies accrue there is no comparison between Israel and other countries like Ireland, Taiwan, and India, all of which have experienced a similar high-tech boom. Israel's governmental Export and Cooperation Institute as well as several other organizations consider the country's homeland security and surveillance industry as a high-tech subsector in its own right and highlight Israel's global leadership in this field. Israel's High-tech Knowledge Portal maintains that after telecommunications it is the second largest high-tech subsector in terms of the number of companies.[99] By contrast, comparable institutions in Ireland, Taiwan, and India do not even mention homeland security or surveillance and do not consider the two as subsectors within the high-tech industry.[100] The only two other countries that appear to have such robust homeland security and surveillance high-tech sectors are the United States and England, but further comparative research is needed to corroborate this claim.

As mentioned above, the military and military industry served as incubators for the high-tech industry. I also claimed that because many of the people who joined the private high-tech industry were trained in developing products and offering services relating to security it is not surprising that the high-tech industry developed a homeland security and surveillance sector. But the military and military industry have helped shape Israel's surveillance industry in other ways as well. Strikingly different from other domestic software industries in India and Ireland, both of which relied on exports from the beginning, the Israeli software industry relied initially on local demand, primarily from the military and security establishments. Thus, as the major buyer of high-tech products and services the military helped to promote the security orientation of Israel's high-tech industry.[101]

One company called the Fourth Dimension (later changed to New Dimension) acquired from the Ministry of Defense a product for operations automation in exchange for a promise to update and



maintain it. It then developed a few more products until the US software giant BMC bought out New Dimension for $675 million. Along similar lines, a team of former officers from the School for Computer-Related Professions established Magic Software Enterprises, and its first breakthrough sale was to the Israeli military.[102] Among Magic's newer customers is Access Data Corporation, which provides software solutions for the law enforcement community, including comprehensive integrated database management solutions for communications, corrections/detentions and emergency service providers throughout the United States. Recently, Access Data was awarded a federally-funded contract from the City of Phoenix to provide the Phoenix Police Department with a system for reporting in real-time crime statistics and data to the FBI.[103]

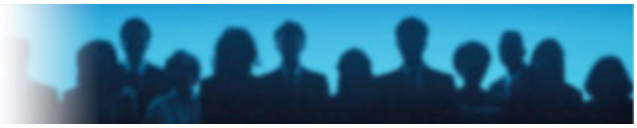
In addition to the movement of labor and the acquisition of products, one can identify three other ways by which the military and military industry encouraged the development of a robust homeland security/surveillance industry in Israel. These include the conversion of products and ideas from military to civilian use, the creation of a collaborative public space that facilitates the sharing of ideas and collective learning, and the incorporation of security personnel who have had experience in combat and are part of Israel's security network into the high-tech industry.

2.4.1 Military Conversion and Technological Spin-offs

There is no dispute that many of Israel's homegrown technological skills were honed inside secret military labs and that military research has given Israel a clear lead in vital aspects of telecommunications and software technology. According to the Governmental Export and International Governmental Institute, "what grew out of a direct military need with a high-tech edge has developed into a core element of the Israeli economy and placed Israel at the forefront of the global security and homeland security industry."[104] Thus, the military and military industry are not only responsible for providing a skilled labor force to Israel's high-tech industry, but have also supplied it with specific technological knowledge that has enabled private entrepreneurs to manufacture a variety of spin-offs.

Following F. Chesnais, I understand the transfer of technology not only to mean the transfer of the "technical knowledge needed to produce the products, but also of the capacity to master conceptually, develop and later produce autonomously, the technology lying behind these products."[105] Studies have shown that in other parts of the world military R&D is frequently used as a source for spin-offs or new technologies that are diffused into the civilian markets and that, at times, the same technologies deployed in the military can be used without any modifications for civilian markets.[106] Hence, the transfer from military industries to civilian markets is in no way unique to the Israeli case. Interestingly, though, the Israeli government never adopted a national policy that would facilitate the conversion of military technologies and has consistently ignored the military and military industry's potential as primary sources for technological knowledge and development capable of contributing to civilian industry and to small businesses.

As mentioned above, the state-owned military industry did undertake conversion initiatives, but, according to Daniel Vekstein and Abraham Mehrez, its efforts "fell short of providing a meaningful impact to many economic actors across industries and regions in Israel due to the lack of a comprehensive national technology policy linking [military] firms, with many small businesses and potential entrepreneurs so as to turn know-how and capabilities that were



accumulated in the defense industry… into practical, commercially relevant technologies..."[107] In sum, military technology transfer to civilian industry in Israel has not been due to policy choices or even the initiatives of the military industry; rather, this conversion has been the result of the private initiatives of individual entrepreneurs who left the military industry or units within the military.[108] And this is unique to the Israeli case, since as Yoram Oron, an Israeli venture capitalist points out, "If you leave Cisco and start a company with what you've picked up, you'll face their lawyers. Here, if you leave the army and start a company, you'll get government support. There are no intellectual-property issues."[109]

A well-known example of private conversion involves Given Imaging, a Nasdaq-listed Israeli company that is currently redefining the field of gastrointestinal diagnosis. Given Imaging sells a video capsule called PillCam. It is a disposable miniature video camera contained in a capsule that can be easily ingested by the patient. The capsule transmits high quality color images of the gastrointestinal tract, which allows physicians to visualize the small intestine and esophagus while sparing patients more uncomfortable endoscopies.[110] The know-how behind this vitamin-sized camera can be traced back to Israel's military industry. The tiny camera was originally developed as a device that was meant to be attached to missiles and that could beam back pictures to military controllers.[111] Given Imaging's story is characteristic of many high-tech firms in Israel, some of which produce gadgets for medical supervision, but many of which create products for homeland security and surveillance.

Geotek, a company that specializes in communications software that allows small companies with fleets of vehicles, like local delivery services or even hotel chains with airport shuttles, to communicate with drivers and track fleets using satellite tracking technology, developed its product using software licensed from RAFAEL.[112] Haifa-based Fibronics was founded by engineers who had worked together in military intelligence. The company got off to a good start in the 1980s with a data-networking technology called Fiber Distributed Data Interface, but since it lacked a U.S. distribution arm it was eventually taken over by Elbit Computers. Enigma did better. Founded by veterans of a military intelligence unit, the company developed software that provides maintenance information about complex products, such as jet engines, construction machinery, automobiles and telecommunications equipment and currently boasts annual sales in the hundreds of millions of dollars.[113]

These stories are not coincidental. A survey of Israel's high-tech industry reveals that various applications developed by private civilian surveillance companies were derived directly from military R&D in the areas of sensors, information-gathering technologies, image enhancements, video and audio compression applications, high-speed image analysis and optical inspection systems.[114] Specific examples of technology transfer from the military industry to commercial use are listed in Table 2.

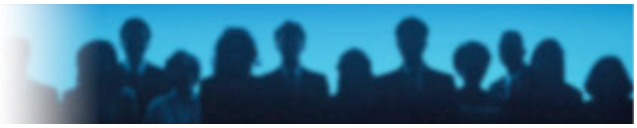


Table 2: Technology Transfer from Military Industries to Commercial Use

Firm	Technology Transferred	Commercial Use
EVS	Computerized Pattern Recognition	Defect identification in fabrics
Frutonics	Computerized Pattern Recognition	Defect identification in fabrics
Comverse Communications	Voice Recognition and Logging	Voice Logging Systems
Nice Systems	Voice Recognition and Logging	Computer Telephony Integration
Geotech	Frequency Hopping Communication	Cellular Telephony
DSP	Speech Recognition	Speech Compression for Telephony
Tadiran Systems	Electro-Optic Surveillance	Wide Area Protection
Motorola Israel	Satellite Positioning Technology	Vehicle Positioning
Ituran	Direction Finding and Positioning	Vehicle Positioning
Madacom	Frequency Hopping Communication	Wireless Wide Area Paging
ISORAD	Nuclear Radation	Metal Detectors for Air Fields

Source: Dov Dvir and Asher Tishler, "The Changing Role of the Defense Industry in Israel's Industrial and Technological Development," in Judith Reppy, ed., *The Place of the Defense Industry in National Systems of Innovation*, Cornell University Peace Studies Program, Occasional Paper #25, 2000.

Along similar lines, some of the better-known high-tech companies like Checkpoint, Comverse, Nice Systems, Alvarion, ECI, Audiocodes and MetaLink were established by people who served together in the Israeli military.[115] Table 3 provides a very partial list of firms managed or initiated by people who were trained in the military or military industry. Moreover, information-security software players like Aladdin and Check Point continue to draw much of their talent from elite military units. The significant point, one should stress, is that the know-how is transferred individually by military personnel and employees of the military industry who eventually became private entrepreneurs.

The fact that there has been no national policy for transferring military know-how to the civilian sector helps explain the diffused structure of Israel's homeland security and surveillance industry, which is currently made up of hundreds of companies (as opposed to the 6 firms that make up the military industry). And yet, contrary to the commonly held view, which sees the military and military industry as mere suppliers of skilled labor and technological spin-offs to the private high-tech sector, Dan Breznitz adds a whole new dimension to the discussion. Breznitz shows that the military plays an additional role in shaping the high-tech industry by providing it with what he refers to as "collaborative public space."

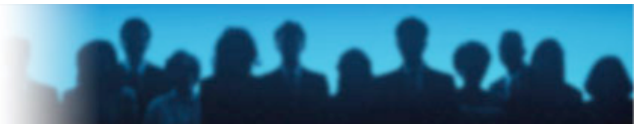


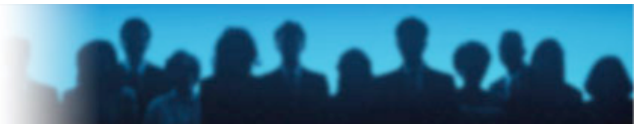
Table 3: Firms Managed or Initiated by Personnel Previously Employed in the Military or Military Industry

Firm	Area
Gilat Communications	Very Small Aperture Satellite Terminals
NICE Systems	Computer Telephony Integration
Check-Point Fire-walls	Fire-walls for Internet Communications
Orckit High	High speed Modems
BVR Simulators,	Simulators, Virtual Studios
Technomatics	CAD/CAM Software for the auto industry
ESC	Laser Surgery Equipment
Medis-EL	Cancer Diagnosis Equipment
Cubital	Fast Prototyping Machines
Magic Computers	General Database Software
Teldor Computers	Software Development
RAD Computers	Data Communication Equipment
Lannet	Data Communication Equipment
DSP	Speech Processing Devices
Nexsus	Two-way Paging Systems
Optrotech	Printed Board Inspection Systems
Tadiran	Communication and Telephone Equipment
Telrad	Telephone Switching Systems
Elbit	Defense, medical instrumentation and communication systems

Source: Dov Dvir and Asher Tishler, "The Changing Role of the Defense Industry in Israel's Industrial and Technological Development," in Judith Reppy, ed., *The Place of the Defense Industry in National Systems of Innovation*, Cornell University Peace Studies Program, Occasional Paper #25, 2000.

2.4.2 Collaborative Public Space

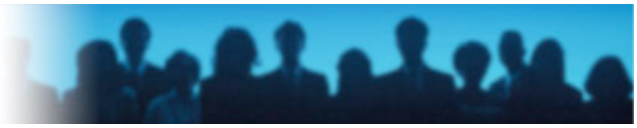
The notion of a collaborative public space adds a spatial dimension to existing theories that emphasize the importance of social networking, systems of flexible production, and the creation of formal and informal institutions for the development of technological innovation. As Breznitz



points out, these theories all assume that innovation is a socially embedded process, i.e. it cannot be understood solely through neo-classical economic theories that frame the market as a constellation of atomized actors who seek to maximize their utility functions. Breznitz's contribution lays in his ability to show that the different theories either assume or are dependent on the creation of multiple informal and formal venues where people can meet to share, discuss and process ideas and, in this way, advance cooperation and collective learning. Social network theory, for example, suggests that technologically proficient people coming from both the military and military industry create dense networks that enable the diffusion of knowledge, facilitate the recruitment of new talent, and help attract venture capital, but it does not conceptualize how the networking is carried out. In Breznitz's opinion it occurs through the creation of a collaborative public space.

By collaborative public space, Breznitz means a "structured social space imbued with high mutual trust within which different actors and groups regularly study, cooperate, share information, and partake in collective learning. Collaborative public spaces are, therefore, the institutions that both stimulate and enable the different actors and organizations in a system to meet, discus, transfer, interpret, and develop ideas, knowledge, and information that are inherent to their industry."[116] The existence of such vibrant public space where people from different walks of life meet enhances not only the capabilities and economic capacities of individual actors, but also the industrial sector as a whole. Participation in these meetings, Breznitz adds, helps diffuse information throughout the industrial system through formal and informal transactions and collaborations between individual actors, which augments, in turn, the capacity for collective action, and spurs ideas for public policy. It also facilitates a sense of a shared future. To be sure, this so called collaborative space fosters elite formation and the crystallization of social class formations. It is "public" in a limited sense, limited to those who are Jews, have the necessary military experience, and can count on the old boy network. Jews who do not share this experience have a hard time joining this "collaborative public space." This phenomenon which may very well be unique to Israel might also help explain upward class mobility in Israel.[117]

The interesting point from the perspective of this report is that, according to Breznitz, the Israeli military provides a collaborative public space for Israel's high-tech industry. It "acts as an important center of information gathering, processing, and dissemination for the Israeli software innovation system, as the originator and strengthener of many social networks, and as the connecting node between various weakly tied social networks."[118] The military is able to do so because the close relationship between it and civilian sectors in Israel is not limited to the common denominator (among Jews) of compulsory military service, but rather to the constant cultivation of this relationship due to the long years of service in the reserves that many Israelis carry out and to which they are committed.[119] Breznitz shows that the military is able to create a public space in which the reserve forces are the connecting node between the military and civil society. First, the military sponsors multiple activities of collective learning by creating and disseminating IT teaching and learning material. The School for Computer-Related Professions, which has at its disposal around 400 reserve personnel (which amounts to about 20,000 days of reserve duty per year), serves as a point of contact for the reserve personnel, regular duty personnel, and students, creating a strong multi-cohort network, which is rare among teaching



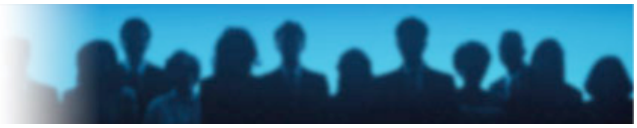
institutions. Small project teams composed of active duty soldiers and civilian experts from a multitude of firms and academic institutions, doing their reserve duty, are gathered together in order to share their knowledge in a way that would not be possible outside the military.[120]

Second, Israel's experts in various IT and R&D fields teach and publish textbooks and instruction material as part of their reserve military duty. Third, the reserve personnel themselves are constantly exposed to the knowledge produced in the military, knowledge they take back to and utilize in their private firms or in the universities. Thus, the reserve personnel serve as a conduit, among the industry, academia, and the military via the School for Computer-Related Professions. This two-way exchange was captured by one of the school officers who recounted to Breznitz an incident with one of his reserve soldiers, who, when not on duty, directs a professional civilian computer school. This person "called me and told me that they lack a specific set of classes, [and] I immediately gave him a booklet of 120 pages with questions, examples, and instructions written by our best instructors. This is a guy who when we did not manage to develop something in-house forced three industry leaders to volunteer for a whole day to come and help us."[121]

Fourth, the military also serves as an important point of contact for knowledge acquired from foreign software tools and IT technology development companies, such as Oracle, Sun, Novell, Cisco, and Microsoft. Thus, before a new development tool is released, the military has often already acquired knowledge of its use from abroad and organized courses to train professionals, enabling faster diffusion of the latest software development techniques in Israel. The Israeli case differs from other countries where technological knowledge is diffused through private schools or internal training units, such as that of IBM, because the military creates a nationwide public space that helps enhance the skills and knowledge of the whole Israeli IT industry and not just a specific organization or set of organizations.[122] Since the space where many high-tech experts meet to process and share new ideas is the Israeli military it is not surprising that the ideas which are diffused relate to security and surveillance, ideas that naturally preoccupy such an institution.

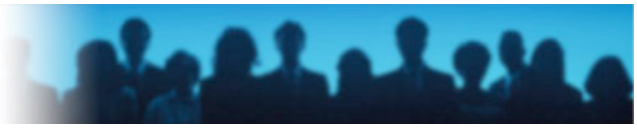
2.4.3 The Security Network and Military Credit

Finally, the military has facilitated the exponential growth of Israel's homeland security and surveillance industry not only by enhancing the technological capabilities of this high-tech sector, but also as a result of the penetration of people with combat-related experience into this industry. Of the 237 surveillance companies I examined, a total of 166 companies provided a list of either members of the management team or board, and 156 of these provided short biographical notes near each person. Of these, 102 companies mentioned on their website the security-related background (i.e., combat or intelligence gathering experience in the Israeli military, Mossad or Shabak) of at least one person on their management team or board. Thus, 65 percent of the websites that provide biographical notes and 44 percent of all the websites mention the security-related background of senior officers in the company. This again is unique to the Israeli case. A brief examination of the biographical descriptions of the management teams and board members in high-tech companies in countries like Ireland and India reveals that all of them emphasize the technological, management and sale skills of the officials (the Israeli companies do this as well) and not their background in combat units.



For instance, 4DM Technologies provides a software tool that allows organizations to "manage the daily routine and the crisis processes using one platform." The website notes that the company is led by Brigade General (Reserve) Israel Shafir who has had "many years of aviation experience both as a pilot, commander and in C4I systems operation. Mr. Shafir has over 5,000 flying hours in Jets, Transport planes and Helicopters."[123] The website reader of Algorithmic Research, a worldwide provider of digital signatures for financial, commercial, legal, and government sectors, is told that Ilan Patashnik, the company's chief operating officer "served as an officer in the IDF."[124] Aharon Aharon, the CEO of Camero, which manufactures a product that allows one to "observe multiple stationary and moving objects concealed by walls," served in an "elite intelligence unit."[125] Israel's former military chief of staff, Amnon Lipkin-Shahak, heads IDSST, a "leading provider of perimeter defense systems" that include vibration sensors, infrared detection, laser guard sensor, video detection and sesmic intrusion technologies.[126] Shabtai Shavit, the chairman of AthenaGS3 – which offers its clients the "latest security and detection systems" – is described on the company's website as an "internationally recognized authority, [who] has over 40 years of experience in international security and counter-terrorism as a member of Israel's prestigious intelligence agency, the Mossad, which he directed from 1989 to 1996."[127] Finally, Team 3, which provides services in a wide variety of areas such as corporate security, electronic protection, guarding, surveillance, cleaning and maintenance, was founded in 1990 by the late Brigadier General (Res.) Yoram Gilboa together with a team of several former military officers who have accumulated considerable knowledge and experience over a period of many years in the field of security and guarding.[128] The list goes on and on.

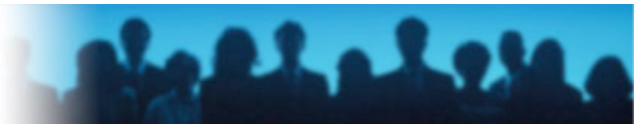
These people are part of Israel's informal security network, and they "joined" it after serving in the military, Shabak, Mossad, police, and government owned military industries. Obviously, their role is to bestow on the companies and their products a certain kind of social, cultural and symbolic capital that many of the technologically skilled people do not possess. Following Pierre Bourdieu, I understand social capital to be the power and resources that accrue to individuals or groups by virtue of their social networks.[129] Examining the penetration of these retired security officials into the private sector helps to explain some of the characteristics of Israel's high-tech industry.[130] First, it reveals that the orientation of a large segment of this industry towards homeland security and surveillance is not only a reflection of the movement of computer experts and technological know-how from the military and military industry to the private sector, but also reflects the movement of people with combat and intelligence background to the companies' boards and management teams. Second, Oren Barak and Gabriel Sheffer, who have studied Israel's security network at some length, show that these people have, among other things, access to policymakers in the political, military, civil and economic spheres.[131] This kind of access can benefit the company by facilitating the procurement of contracts with the military and other Israeli security agencies. It can also help the company attain governmental R&D funding. Finally, the retired security official can exploit their access to the corridors of power as well as their membership in the network in order to establish close economic ties not only with Israel's primary trading partners, such as the United States and European countries, but also Singapore, South Africa, Turkey, Slovenia, China and India, all of which have purchased Israeli weapons, obtained training by Israeli security experts, and in certain cases conducted joint research projects with Israel's military establishment.[132]



In addition to providing the companies with the benefits of being part of the security network, these people also bestow on the products cultural and symbolic capital. By cultural capital I mean the knowledge and skills acquired through early socialization, education and professional career, while symbolic capital "is the form that the various species of capital assume when they are perceived and recognized as legitimate" and desirable.[133] The prior careers within one of Israel's security institutions enables officials who are currently on the management team and board of surveillance companies to confer on the companies and their products a certain kind of credit that the people who have experience in technological innovation cannot. By credit I mean "the power granted to those who have obtained sufficient recognition to be in a position to impose recognition."[134] As recognized security experts, who for many years were members of the leading security institutions in Israel, these people help render the companies and products both legitimate and desirable, since, at least ostensibly, they are able to assess the usefulness of the product. Moreover, the credit that they have due to their capital bestows upon them the authority to impose a vision -- which in our case refers to ideas of what constitutes a "safe society" -- and what needs to be done in order to achieve it.[135]

2.5 Conclusions

The military and military industry, as we saw, have played a key role in the diffusion of IT skills in Israel, and have helped, more specifically, spur the evolution of the country's surveillance industry in five distinct ways. The first three relate directly to the fledgling surveillance industry's technological strength. The Israeli military and the military industry have served as an incubator for an extremely well-trained and skilled labor force, while simultaneously the incorporation of these employees into the high-tech industry has facilitated the diffusion of R&D and the production of technological spin-offs from products that were first developed in the military and military industries. Moreover, Israel's military provides a collaborative public space that serves as a center of information gathering, processing, and dissemination for the Israeli software innovation systems and a connecting node between the military and the surveillance industry. From a non-technological perspective, the Israeli security network also plays a crucial role within the surveillance industry by providing it with both connections to markets around the globe and conferring upon it credit and symbolic power in Pierre Bourdieu's sense of the terms, which benefits marketing efforts.

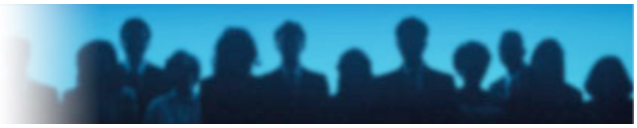


Chapter Three: Crossing Traditional Boundaries

Israeli companies are among the leaders of several products and services that make up the global homeland security/surveillance industry. The players involved include large military companies such as Elbit, Israel Aircraft Industries, RAFAEL, and ELTA. Other key players entered the homeland security and surveillance market from the telecommunications arena, including Nice Systems, Ness Telecommunications, and Mer Group. While still others were set up from the beginning as homeland security/surveillance companies that manufacture products and provide services relating to perimeter security, access control, image analysis and authentication to mention a few surveillance subsectors. Some of the large global firms in these areas include Dmatek, Magal Security Systems, and Orad.[136]

As mentioned, Israeli companies control about 70 percent of the global UAV market, which is expanding each year exponentially. Nick Denes maintains that UAV's have become a major component of border security technologies, and that they ultimately help shape the demarcation of international borders.[137] Borders are indeed a site where homeland security and surveillance technologies are extensively deployed. Israeli companies have developed efficient systems for checking baggage and cargoes. For instance, Hi-G-Tek has developed radio frequency identification (RFID) electronic seals for fast, automatic processing of secured cargoes and the comprehensive monitoring of the cargoes while in transit.[138] Other companies are also leading developers and manufacturers of threat detection systems especially for non-conventional materials. These include Rotem Industries which has developed a series of radiation detection and monitoring systems and emergency response kits, while Scent Detection Technologies has developed "flexible" technology "capable of learning to recognize new substances, thereby constantly adapting to new threats." Its sensors have the capacity to detect trace amounts of material in gaseous and liquid phases and are designed to work by independent remote operation, without human interference.[139]

Israeli companies are also making a mark is biometric technologies that are deployed to identify or "authenticate" individuals. On-Track Innovations combines the ability to support biometric identification with portable smart cards in such applications as a driver license, passport, social security information or other ID cards. IQS Identity Systems has developed a chipless biometrics solution that can be used for ID cards, air/seaport boarding cards, and even medical prescriptions. This company also produces a patented high resolution fingerprint reader that aims to solve all false fingerprint identifications.[140] Wondernet offers biometric authentication to digitally signed documents, while BioGuard developed a wireless RF-based fingerprint identification system. BioGuard's vision is to develop a universal personal biometric ID seal that will replace ordinary keys in our daily lives, thus "enhancing security while ensuring a high level of user-friendliness."[141] Vuance is also among the world leaders in contact-less smart card technology and has developed a family of cards that contain large quantities of securely stored data using laser and thermal printing transfer technologies. The company produces the passports in the UK, Hong Kong, Ethiopia and Iceland, the ID cards in Zanzibar, the drivers licenses in

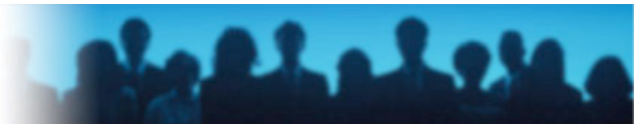


Israel and the entry permit from Gaza, as well as a variety of cards for airport security, correctional facilities and homeland security offices in the US.[142]

Biometrics is precisely the kind of technology that is being deployed as a mechanism of social sorting and is becoming more and more a feature of everyday life. It has become particularly prominent at borders, which have for some time been sites of hyper-surveillance. All non-US citizens flying into the United States must provide a biometric thumb imprint at passport control, where it enters and is cross-examined with the IDENT biometric database that stores and identifies the electronic fingerprints on all foreign visitors, immigrants and asylum seekers.[143] Along similar lines, Israel has devised a biometric fast-track for people entering and exiting the country. The idea is to allow "low risk" passengers to pass through without any form of human intervention so that the limited human resources can focus on the passengers that are considered a greater risk. The emergence of "biometric borders" signals, according to Louise Amoore, a dual-faced phenomenon: "the turn to digital technologies, data integration and managerial expertise in the politics of border management; and the exercise of biopower such that the body itself is inscribed with, and demarcates, a continual crossing of multiple encoded borders – social, legal, gendered, racialized and so on."[144]

Border control also includes perimeter security, a surveillance sector that originally developed to secure borders and high-risk facilities, but is currently spilling over to protect all kinds of property. It is used in gated communities, campuses, and corporations as well as vehicles and shops. Perimeter security is basically a system that was originally made up of conventional fencing, locks and alarms and currently includes a multiplicity of advanced technologies involving different forms of lighting, sensors, CCTV, electro-optic systems for night vision, electronic intrusion detection systems, and command and control equipment. The Israeli company IDSST provides comprehensive solutions for perimeter security after having developed a warning system that combines various technological abilities which boasts the lowest false alarm rate. Among its clients are the US Department of Defense, the US Department of Energy, over 40 correctional facilities, as well as industrial plants, refineries, energy facilities and US information agencies located in Kuwait and Morocco.[145] Along similar lines, Controp Precision Technologies has developed a real time, advanced panoramic intruder protection system that automatically detects motion within a wide panoramic view, while Opgal Optronics manufactures and markets thermal imaging systems.[146]

The Orad Group is a major player in the perimeter security field, with a specialty of integrating technologies pertaining to access control, biometrics, and Intelligent Video Surveillance. According to its deputy CEO, Orad is now looking into the creation of virtual or, more precisely, invisible security apparatuses. The idea is to transform cities or different facilities into military bases of sorts whereby people inhabiting a space are secured by all the technologies used to secure a military base but that these technologies are invisible. One will not need guards in booths at the entrance of the gated community, which might not be gated at all; the fences, cameras, sensors and other technologies that are used for perimeter security and safety (as well as social sorting) in a military base will all be there, but they will be unidentifiable from the surface so that the inhabitants can enjoy the serenity of the space.[147]

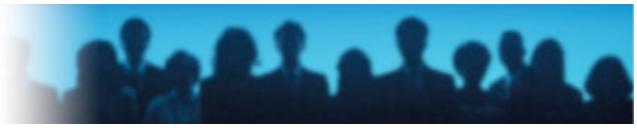


Another surveillance sector in which Israeli companies are among the world leaders is electro-optical and laser applications which help overcome the impediments caused by darkness or distance. A range of optronics technologies developed in Israel such as thermal imaging, lasers, and infra-red optics are used by fighter aircrafts to carry out reconnaissance missions and strikes as well as in unmanned air vehicles (UAVs).[148] They are also deployed in special cameras used in small satellites or industry automated optical inspection systems and binoculars as well as in a range of personal night vision devices for combat. Elop, a subsidiary of the Israeli military giant Elbit, manufactures an array of electro-optics products including thermal imaging devices which aim to "deliver a 24/7 observation and surveillance advantage" and a threat detection and countermeasure device for airborne platforms.[149]

IT software solutions in such fields as imaging, voice response and recognition and data communications also feature prominently among Israeli homeland security/surveillance companies. More specifically, Israeli firms specialize in security related IT systems including Internet security, e-mail surveillance, data mining, data fusion, situational awareness and pattern and image recognition.[150] Firms like Verint, which for tax and market purposes has been transformed from an Israeli to a US company, offers expertise in the sphere of information surveillance like communications interception, digital video security and business intelligence. Verint's software is "designed to integrate and analyze huge volumes of data — images captured by thousands of cameras, trends buried in millions of calls, threats hidden in billions of interactions." A range of Verint products sold to more than 10,000 government agencies and corporations in over 150 countries enable intelligent collection, storage, processing, monitoring, distribution and management of communications and images.[151]

Top Image Systems (TIS) also provides automated data capture solutions that aim to improve enterprise business processes by integrating data from multiple sources and of different types. Founded in 1991, TIS is a public company traded on NASDAQ and operates internationally with branch offices in the US, Germany, UK, Latin America, Singapore and Japan, and local representatives across Europe and the Pacific Rim. It enjoys the largest market share of worldwide census projects that utilize software technology to capture and validate data from population census forms.[152] In 2001 and again in 2005, it was selected as the information collection solution for the Irish Census, where it scanned and processed approximately 50 million images through its *eFLOW Unified Content Platform*. Other Israeli companies in this group include Synel Industries, which has developed software for data collection systems as well as solutions for management of time and attendance of a workforce.[153] ECtel, a subsidiary of ECI Telecom that is traded on NASDAQ, provides monitoring and anti-fraud assurance solutions for communications service providers and Aladdin Knowledge Systems, a leading innovator in enterprise content security.[154]

Finally, Israel's Armament Development Authority (RAFAEL) is now selling a new concept that it developed called Total Area Control System, which is effective for perimeter protection as well as shore and border defense. Total Area Control System includes "detection and identification of hostile activities; warning and alarm; surveillance and tracking of suspected targets; data collection and processing; data transmission; monitoring one's own forces; and command and control at all stages and levels."[155] Notwithstanding all the Israeli innovations mentioned as well as many others, a government homeland security brochure admits that "no



security is ever one hundred percent perfect." The brochure goes on to note that "in an era of growing terrorist and criminal threats, these innovative IT technologies do enable authorities and enterprises to provide considerably enhanced protection for their citizens."[156] The brochure says nothing about the fact that security is only one of the many objectives for which these technologies are deployed.

3.1 Integrating Security and Civilian Control

The possibility to remotely monitor and manage spaces and people may have been developed for security reasons but for a variety of reasons, not least economic ones, companies have been searching for ways to extend their technologies to the civilian sector. "Everything is Under Control," is the logo that appears on the website of Electronics Line 3000 (EL), a company that provides wireless security solutions. Publicly traded on Germany's Neuer Markt in Frankfurt, EL's systems enable people to remotely control and monitor an office, installation or home from anywhere in the world via a cellular network or the Internet. EL currently operates over 2.5 million control systems and has installed 15 million devices worldwide. The incorporation of remote monitoring systems alongside wireless capabilities within existing surveillance products such as sensors and CCTV characterizes many Israeli developers, some of which are no longer packaging and selling their products solely to security agencies and other institutions that want to detect and capture intruders.

Dmatek is a good example of a company that has managed to translate technologies that were originally developed for security purposes to technologies that are opening new paths in the civilian sector. Dmatek characterizes itself as a leading provider of "remote people monitoring technologies." It is among the larger Israeli surveillance companies, and employs 114 people with sales of $44 million in 2007, up from $26.8 million in 2006. The company has three major subsidiaries: Elmo-Tech, Pro-Tech and HomeFree Systems.

Elmo-Tech is a global provider of location verification technologies, designed for monitoring individuals in the law enforcement, corrections and security markets. It offers products to a variety of agencies in the US and Europe as well as several other countries, while its technologies serve several purposes ranging from remote alcohol monitoring, prisoner tracking, and GPS offender tracking, to "football hooligan monitoring," voice verification and a "domestic violence deterrent system."[157] Pro-Tech focuses on a GPS offender tracking system, providing services to over 120 government agencies that are interested in tracking the location and movement of offenders. The company claims that since 1997 its devices have helped track more than 100,000 offenders, while maintaining that in the future more agencies will require its services since "Public safety agencies are expected to know which supervised offenders were near or at a crime scene" and active "legislative efforts across the United States call for long-term tracking of sex offenders."[158]

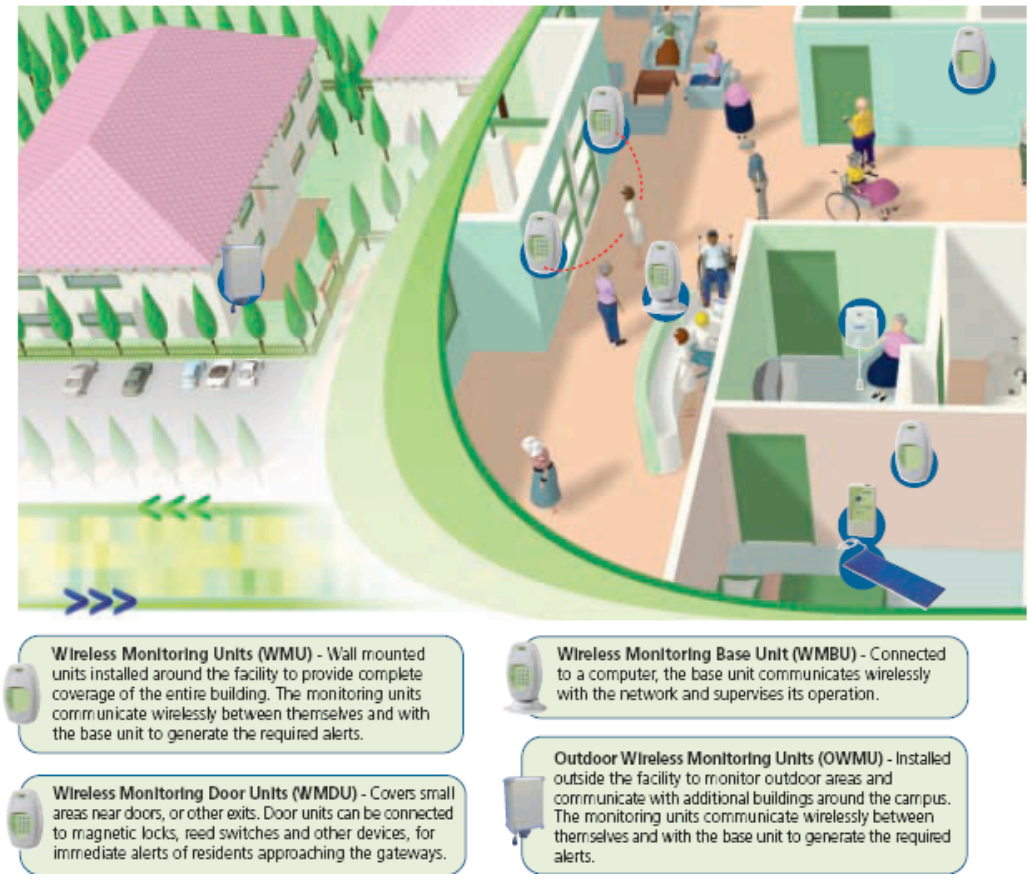
By contrast to these two companies, HomeFree Systems is one of the leading companies that focuses on the emerging elderly monitoring market. The company developed a single wireless platform that integrates advanced wandering and fall management alerts with resident and nurse call capabilities. The idea is to offer a comprehensive, cost effective communication platform, performing ongoing wireless monitoring of residents in various types of facilities as well as

surveillance of their surroundings. The monitoring systems can gather real-time data because sensors called personal tags are attached to a human body (Figure 6) and can be used to monitor whole areas through wireless data streaming units that communicate information to a monitoring center.[159]

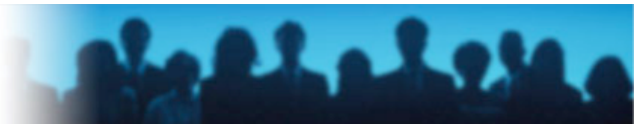
Figure 6: Personal Tag which monitors the elderly

Source: Homefree Elite Brochure

Figure 7: Resident Monitoring System



Source: Homefree Elite Brochure



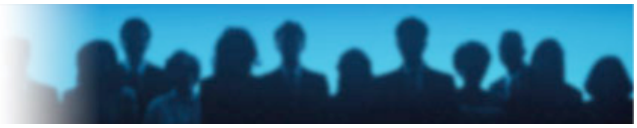
The sensors are based on a modular platform designed to continuously gather, analyze, act, and report on to a centralized monitoring unit the incoming information (Figure 7). This surveillance system can be used by an institution such as an elderly home and an Alzheimer inpatient clinic, or by an adult child who lives hundreds of miles from his or her elderly parents and would like to monitor their daily activities so as to ensure that they are alive and well.

3.2 The Logics of Surveillance

It is not only that Israeli companies, which traditionally manufactured surveillance technologies that were deployed for homeland security purposes, are now converting their technologies so that they can be used for civilian purposes, but that they are trying to combine two different logics of surveillance. The integration of security with civilian surveillance brings us back to the notion of surveillance as social sorting, since among its many contributions social sorting deconstructs the binary between the objectives of surveillance for military or security purposes and objectives of surveillance for marketing and other civilian purposes. This is crucial since traditionally surveillance was developed according to one of two distinct logics.

Marketing or consumer surveillance tended to follow what Francois Ewald has, in a totally different context, called an insurantial imaginary, which is informed by a certain type of rationality formalized by the calculus of probabilities.[160] This kind of surveillance focused on populations more than on individuals and on behavior patterns of sectors within society rather than the individual behavior of John and Jane. Consumer surveillance aimed to produce technologies whose goal was to register facts and produce data from which objective probabilities can be inferred. For example, it concentrated on patterns of consumption of certain populations (according to zip codes, place of employment, eating habits, reading habits, etc.) and used some kind of probability calculus to target the populations it was interested in. In addition, the logic informing this form of surveillance aimed not only to register and monitor existing patterns of consumption, but also to produce patterns of consumption by sending, for example, brochures and other advertizing information to certain marked groups.

The vital contribution of probabilities has not escaped security surveillance, but the overarching logic of this kind of surveillance aimed at identifying not merely a group within the population, but a specific individual – i.e., the person *responsible* for terrorist or criminal activities. In Ewalds words, "The sociological discovery of the regularity of criminality did not lead to the deduction that it was inadequate to treat the criminal in terms of responsibility."[161] Ewald contrasts the insurantial imaginary with the juridical logic, noting that the law is interested in the identity of the person who breached it, and not so much in patterns of behavior. My claim is that the security apparatuses developed surveillance technologies whose objective was to identify the specific person who carried out or might carry out the illegal action. So instead of surveillance technologies that examined population characteristics according to zip codes, security surveillance technologies focused on methods of enhancing night vision or voice recognition. The difference between these two logics becomes manifest when comparing the approach of a judge and an insurance company to a car accident. While the judge is interested in finding out who is to blame (security logic), the insurance company is interested in the annual pattern of car accidents and does not really care who is responsible for the specific accident (consumer logic).



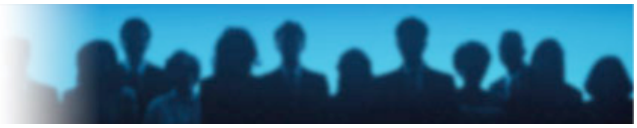
My claim is that social sorting reflects a concerted attempt to produce new technologies and to introduce novel practices that unite these two logics of surveillance. This, I also maintain, is one of the developments that distinguishes contemporary forms of surveillance from previous ones, and is the ultimate objective of social sorting. Amazon is a good example of a business which has made considerable headway in this direction; its surveillance system both recognizes the *individual* consumer and offers him or her merchandise according to *probabilities* of customers who have similar tastes. Amazon's major limitation is that it can recognize a customer only if he or she logs in and cannot totally authenticate if he or she is indeed who they claim to be. This "drawback" can be overcome using biometrics, and since most new laptops are now sold with a fingerprint identification device it is not long before one will be able to log into online stores using fingerprint identification to which an address, credit card, and an array of other information will be attached.

The paradigmatic example of this kind of surveillance was invoked in the science fiction film Minority Report. When customers enter a Gap store their retina is read by a monitor and a voice states that in the past they bought product X (one then understands that the Gap chain has a database of what each individual had previously purchased), and would they this time like to take a look at Y (and here enters the probabilities of consumption patterns, based on other customers). Amazon, Google and several other corporations have made impressive progress in achieving this goal. They market products to specific individuals (instead of sending a brochure to a certain zip code or placing the same ad on all their web pages, they send the brochure to a list of consumers whose specific buying habits they have in their database and place ads according to the preferences on the person who is logged in). This, of course, is also the dream of governments and security apparatuses, who are interested in identifying specific people, but also in knowing the patterns of behavior that can be associated with them.

3.3 The Aesthetics of Surveillance

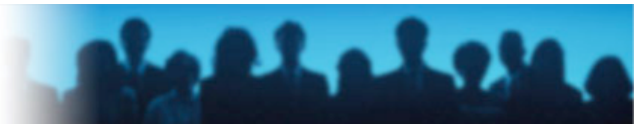
Since surveillance is deployed as a mechanism of social sorting, and not merely to minimize risk and ensure security, its aesthetics is extremely important. While this is not the place to discuss the aesthetics of surveillance at any length, I only mention the issue here in order to draw attention to another difference between the military industry, which is interested primarily in the function of the products without being overly concerned about their aesthetics, and the homeland security/ surveillance industry which often considers the aesthetics of the product as part of its function.

Ehud Ganani, an expert in missile technology, and chairman and outgoing CEO of TraceGuard Technologies put it tersely when he pointed out that "in the world of security screening facilities at airports… there is a conflict between the need to treat the passenger as someone who is entitled to service, and treating him as a suspect. The difference here is in the equipment and the way security checks are carried out, so as to not make them invasive. Even if, for instance, an airport has also screening cameras installed, they should blend into the background, so as not to make it look as though 'big brother is watching'. In military industries you don't have this tension between two conflicting interests. If Rafael develops a missile, it will be defined according to operational requirements alone…. In an era when lunatics place 500 kilograms of explosives in a car and then park it next to a private or public building, the development of perimeter protection



of buildings has come on in leaps and bounds. In the homeland security world, where the battlefield is a hotel lobby, design plays a highly significant role."[162]

Surveillance as a form of social sorting in the broadest sense must take into account the environment in which the surveillance product is deployed and therefore the manufacturers of surveillance often aim, at least to a degree, to minimize the visibility of their technologies. The invisibility of the surveillance is most apparent when one is surfing the internet (we are aware through the individualized ads that we are monitored but we do not see how it is done), but also at border crossings, shopping malls, banks, hospitals, schools and airports. The aesthetics of surveillance is indeed crucial; it is the aesthetics of play between invisibility and visibility, whereby the mechanisms deployed are frequently designed to be invisible to the subject of surveillance, but simultaneously the subject should be made aware that they are there.



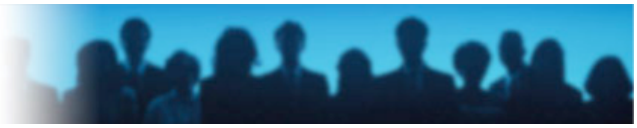
Chapter Four: The Art of Homeland Security and the Political Economy of Israeli Experience

Experience is always a fiction, something constructed, which exists only after it has been made, not before.

Michel Foucault

In order to gain a better understanding of Israel's homeland security industry (and, as we will see, of Israeli society, more generally), it is crucial to examine the role of Israeli experience. Experience, to be sure, is an elusive concept and does not lend itself to simple classifications. The Oxford English Dictionary offers over ten definitions for experience, and it is therefore not surprising that the experience linked to the development and advancement of Israel's homeland security denotes several kinds of practices and processes. Moreover, each form of experience needs to be deconstructed since, as Joan W. Scott convincingly argued, experience is never transparent nor foundationally given, because it is constructed and is always already saturated with ideological assumptions (I return to this idea later).[163]

We saw in Chapter Two that the military and military industry have helped engender and develop Israel's homeland security sector in six distinct ways. My claim is that they all involve the distribution, dissemination, and integration of different forms of an Israeli experience. The military and military industry 1) train and cultivate high-tech professionals with a specific set of experiences oriented towards security and have become a conveyer belt of these professionals to the homeland security industry. It is the ability of these professionals to integrate their technical experience with the experience accumulated by others in the field that 2) enables them to create spin-offs which private homeland security companies sell in the global market.[164] In both these cases, experience refers to "knowledge resulting from actual observation or from what one has undergone" as well as "a device drawn from or approved by experience; something expertly fashioned" (OED). Furthermore, the homeland security high-tech professionals and military personal 3) share their experiences in the military created collaborative public space and this interaction often leads to innovation.[165] In this case, experience refers to the discursive dissemination of existing practices and know-how, which in the OED is described as "to be informed or taught by experience." In addition, the shared experience of years of service within the Israeli security apparatuses helps create the community that makes up the security network. This corresponds to the definition "The state of having been occupied in any department of study or practice, in affairs generally, or in the intercourse of life… the aptitudes, skill, judgment, etc. thereby acquired" (OED). Having acquired security experience through the intercourse of life is not only necessary (but insufficient) for entering the security network, but provides its members (some of whom occupy the higher echelons of homeland security companies) 4) access to policymakers in the political and economic spheres. Their combative field experience also 5) confers on the companies different forms of capital that ultimately lend credit to the products and services that the companies offer. Finally, 6) when the Israeli military or other security institutions decide to use a product, the institutional experience bestows upon the product a stamp of approval. The power of Israeli experience derives from its multiple significations, the ability to create an artificial unity among them under the rubric of "Israeli experience," and to



deploy them in order to manufacture and sell homeland security products. As we will see this experience also engenders a regime of truth involving the management and control of populations that resonates among certain politicians and institutions particularly after 9/11.

Interestingly, the significant role played by Israeli experience, in its different manifestations, has not escaped the eyes of the corporate executives. Rami Bar Eyal, the CEO of Rontal, a homeland security company which was established by Israeli military pilots and provides a comprehensive incident management system, asserts that experience in the IDF "opens doors."[166] Guy Zuri, the business development manager of the homeland security sector within the Israel Export & International Cooperation Institute maintains that, "Many of the security doctrines in the world are based on Israel's doctrines. We are well-versed with suicide bombers, tunnels, missiles; all these problems have led the industry to produce new products."[167] Livnat from Elta Systems underscores the industry's ability to integrate the knowledge obtained in the field with existing high-tech expertise, thus enabling Israeli companies to provide attractive products and services. "Local firms," he says, "have added operational experience [taken from the ongoing combat against terrorism] to the country's technical expertise, in particular leveraging Israel's renowned high-tech know-how, to develop a unique range of products and systems that enhance the protection and safety of the public at large" (Israel Homeland Security, 2005: 14). Finally, Mena Bacharach, Homeland Security Business Development and Marketing Manager of RAFAEL Armament Development Authority, claims that "No other country has Israel's fundamental competitive advantage [sic passim] in Homeland Security of enduring the day-to-day effect of terror. As a result the country has a deep reservoir of experienced professionals, with a hands-on background in the security forces, and real-time expertise in developing concepts, products, solutions and systems that combat terror." "Too often when consulted by worldwide authorities," Bacharach continues, "we can see either inadequate security on the one hand, or overkill on the other hand. Getting it just right is an art that we in Israel have had to master through grim experience" (Israel Homeland Security, 2005: 18-20). The grim experience, it is important to emphasize, creates the art of homeland security, and as we will see the art of homeland security (re)produces the grim experience.

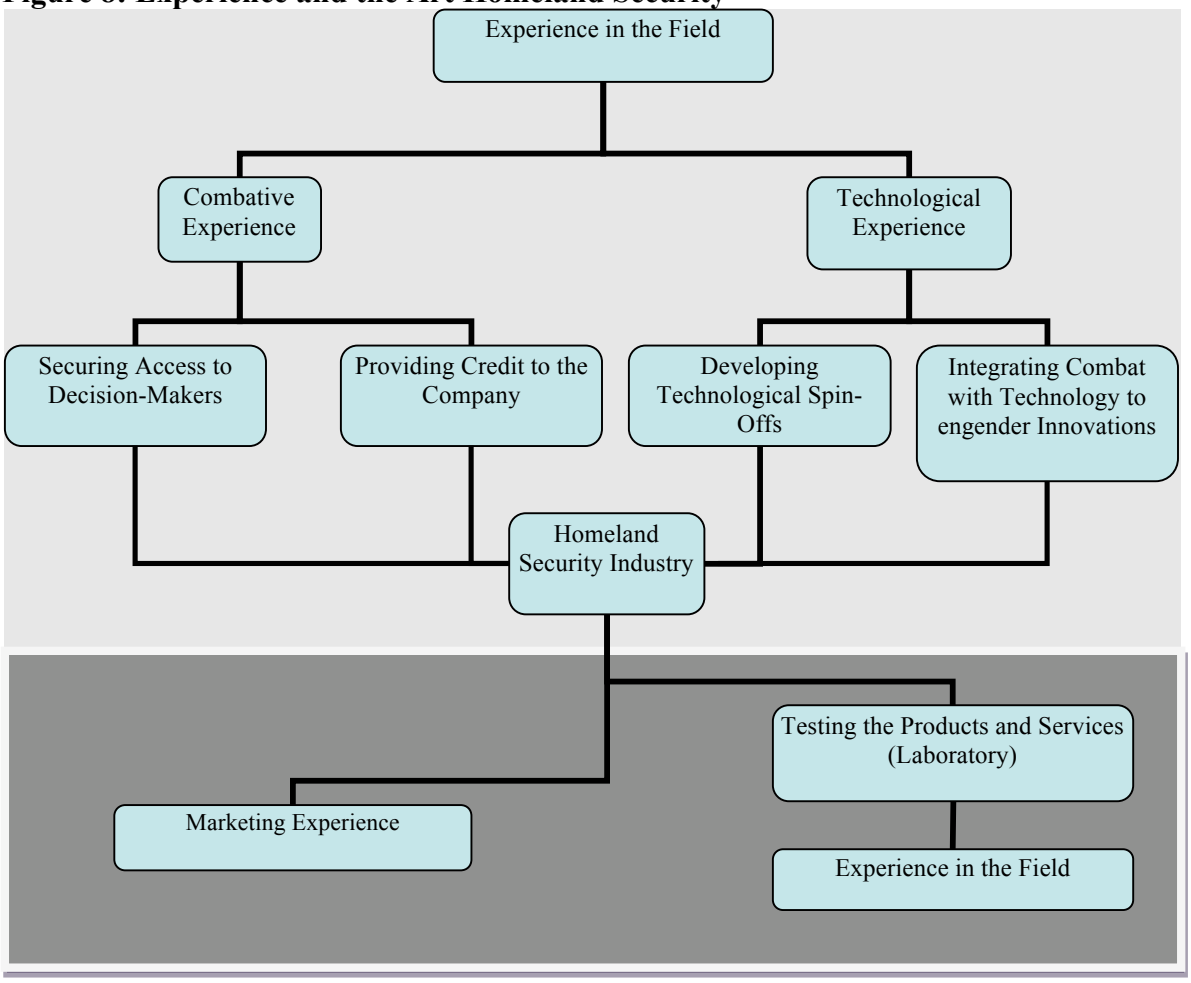
4.1 The Art Homeland Security

As Figure 2 illustrates, each type of experience operates differently. I have already discussed the eight top frames (from "experience in the field" down to "homeland security industry") in order to show how "experience" in its various significations has helped form Israel's homeland security industry and has provided it with a comparative advantage. The three bottom frames shed new light on how experience functions and, as I will claim, urge us to reassess some of our earlier claims about experience's role.

The second to bottom right-hand frame entitled "Testing the Products and Services" is briefly described by Ran Galli, Corporate Vice President of Major Campaigns for Elbit Systems. Galli maintains that, "No other country has Israel's extensive hands-on experience in fighting terror, including the development of new systems, testing them in real-time and adapting and fine-tuning following feedback from performance in the field." Zuri from the Israel Export Institute adds that the "military can say it has used the technologies on the ground, it has not just put them in storage. Israel is a laboratory and we have people who have experience." [168] The notion of

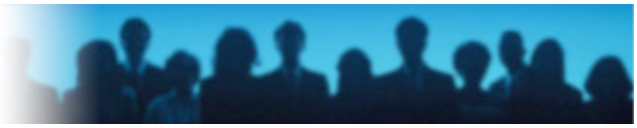
testing products in real-time and fine-tuning is a manifestation of yet another kind of experience, which coincides with the OED's definition of "proof by actual trial; practical demonstration," or "To make trial or experiment of; to put to the test; to test."

Figure 8: Experience and the Art Homeland Security



Yossi Pinkas vice president of Nemesysco, a company that produces technology whose goal is to detect and measure the emotional content of human speech, reinforces the importance of this kind of experience, maintaining that one of Israel's advantages is that,

We check the products on the ground to see if they resolve the issue – solutions means technology, doctrine, and system. After 9/11 everybody began buying technologies… We have already made the mistakes and through our mistakes we learned to produce a general solution, one that unites the different systems. When one is confronted with a terrorist attack or a natural disaster like Katrina one needs holistic solutions that take into account the different systems and determines how to get them to operate together in order to generate the desired results… We learn from our own experience in the West Bank and Gaza as well as Lebanon and employ it in order to improve the products and services; which, ultimately, provide better solutions.[169]

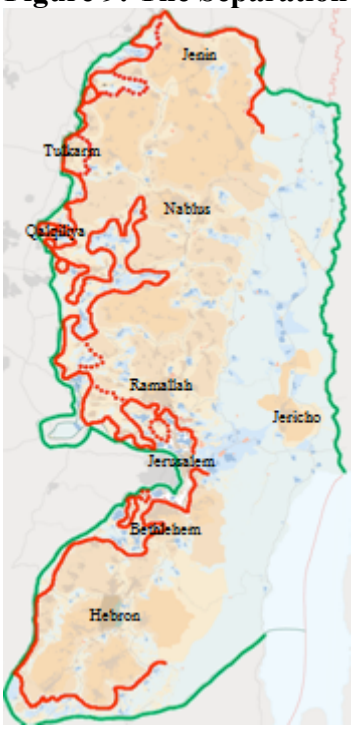


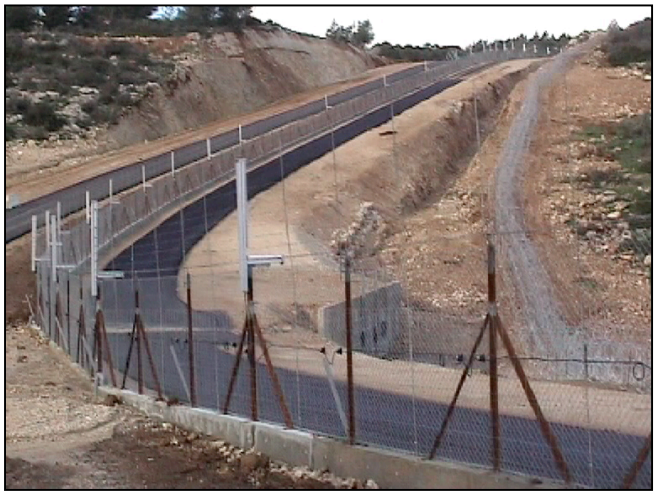
Deputy CEO of the Orad Group, Yossi Goffer, provides a concrete example of this kind of experience when discussing the 360i, one of the products Orad has developed.[170] According to a company brochure, 360i combines a number of advanced targeted technologies, including different types of sensors, a radar detection system, video cameras for varying ranges, top-of-the-line, long-range night vision, a central control system, a wired and wireless communications system, and a "brain," by which they mean advanced "algorithms that utilize pattern and shape recognition, hypothesis testing existing statistical information and more." The 360i was developed "for use along international boundaries and at border crossings, in areas that require special protection, army camps, at installations of strategic importance, air and sea ports and other sensitive sites."[171] Its objective is not only to detect penetration attempts and to alert appropriate intervention units, but to provide ongoing live video images directly to the central command station, to the units in the field and to the defined chain of command. As Goffer puts it, "The idea is that when there is an attempt to infiltrate… and a force is sent to stop the infiltrators, they arrive at the scene with a considerable amount of knowledge including images of the place, the perpetrators, etc. Previously, the military force would arrive blind with no prior knowledge." The improvement of the 360i over other systems is that the forces arrive prepared to confront the perpetrators, its advantage, according to the company brochure, is that it has "undergone extensive testing in extreme weather and changing light conditions and has been approved by the Israel Defense Forces";[172] Goffer adds that it is now being tested along the West Bank separation barrier.[173]

The separation barrier has become an important testing site for several Israeli homeland security firms. Magal Security Systems is a veteran Nasdaq-listed Israeli company in the field of computerized perimeter security systems, which automatically detect, locate and identify the nature of outdoor intrusions. The company's offerings range from taut wire detection to active infrared photoelectric detection and it has been among the major firms responsible for installing the barrier, constructing all together a *few hundred kilometers* of fences and trenches in the occupied West Bank. The company has, no doubt, benefitted from the Israeli experience, since it has been contracted to install over *ten thousand kilometers* of perimeter intrusion detection systems in all five continents and in dozens of countries and currently enjoys forty percent of the global share of this market. Among these is the fence on the US/Mexico border. Its systems are deployed at borders, airports, industrial complexes, nuclear and conventional power stations, as well as public utilities facilities.[174] In an interview for *Fortune Magazine*, Magal CEO Jacob Even-Ezra explains that "People believe we are the only ones who have experience testing this equipment in real life," which helps clarify why Magal is now providing "security for the most sensitive nuclear power and weapons storage facilities in the United States."[175]

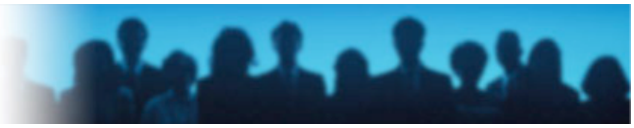
The ability to test the products and services apparently serves three important goals. First, it allows the companies to improve their goods through trial and error. Second, it enables the companies to establish or demonstrate some "truth" about their products and services, which both "certifies" them and provides them with credit. Finally, this process facilitates sales. But if one takes into account the bottom right-hand frame, "Experience in the Field," which is identical to the top frame, it becomes apparent that by testing the products and services the whole process

Figure 9: The Separation Barrier





The width ranges from 60 to100 meters. Made of patrol road, trace road, service road, armored vehicle road, trench, barbed wire and electronic fence. Source: B'Tselem: The Israeli Information Center for Human Rights in the Occupied Territories.



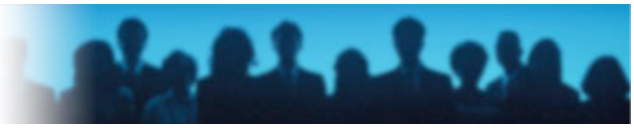
described in the Figure is reactivated.[176] As we will see momentarily, matters are even more complex than this, yet here it is important to stress that the experience generated both from the act of testing the products and from the whole process described on the top of Figure 8 is highlighted in the company brochures and websites and deployed to market Israeli-made homeland security (bottom left-hand frame). The decision to accentuate the Israeli experience is highly significant and provides a clue about the intricate ways experience operates in the service of Israel's homeland security industry.

4.2 Theorizing Israeli Experience

The Israeli experience described in Figure 8 can be understood in several ways. I would like to suggest that it constitutes a vital part of the labor process responsible for the production of the homeland security products and services. The experience of the high-tech professionals alongside the experience of the combat personnel is integral to the production process, not unlike the practice of testing the products in the field. On the one hand, one cannot fully understand the production process of Israeli homeland security commodities without taking these elements into account. On the other hand, they are distinct from the other parts of the labor process – such as the actual construction of the fence, the assembling of cameras, sensors, and the like – in that they are incessantly invoked and attention is drawn to them.

Marx tells us that labor is "put out of sight."[177] The labor of the eight-year old boy who picks coffee beans, the twelve year-old girl who sows apparel in a sweatshop, or even the GM worker who manufactures cars is hidden from the person purchasing the commodity. Similarly, the labor process responsible for producing the homeland security products, including the Israeli experience qua labor, in its different manifestations, cannot be identified in the products themselves. And yet, in sharp contrast to the other elements of the labor process responsible for the production of homeland security products, or for that matter the labor underlying the production of most commodities, the Israeli homeland security firms continuously and incessantly invoke the Israeli experience, thus intentionally rendering an element of what usually remains invisible visible.

With the support of the Israeli government, these companies draw attention to this part of the labor process because the different forms of experience provide an additional element to the product which does not necessarily exist in homeland security commodities that are produced elsewhere. Companies in many European countries cannot test their products in real life situations and need to use simulation to check them. Along similar lines, people working in European homeland security companies do not necessarily have security related background like their Israeli counterparts and therefore do not confer on the products the same kind of credit. These Israeli experiences both add an additional element to the labor process and, simultaneously, raise the labor's qualitative standard (i.e., more experienced labor). Thus, the reason this part of the labor process is made visible for all to see, instead of being hidden as is usually the case, is because it ostensibly improves the commodities and in this way increases their exchange value.

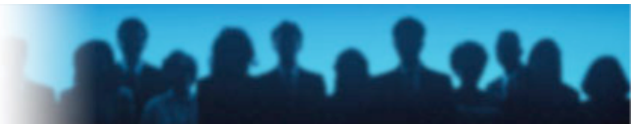


By center staging experience in this way at least three important processes are set in motion. First, the relation towards the commodity is altered. Marx shows that the origin of commodities emerges from the peculiar social character of the labor that produces them. He argues that while the social relations among individuals who are part of the labor process are concealed the "material relations between persons and social relations between things" are accentuated.[178] Thus, it is not only that the eight-year old boy who picks coffee beans and the twelve year-old girl who sows apparel in a sweatshop are hidden, but that the exploitative relation between them and their co-workers, supervisor, and the owner of the means of production are kept out of sight, while the exchangeability of labor and the exchange value of commodities are underscored. The accentuation of these latter elements is necessary, Marx tells us, because it "is only by being exchanged that the products of labor acquire, as values, one uniform social status, distinct from their varied forms of existence as objects of utility."[179] Covering up the social relations is also necessary since it helps mask the exploitation of workers and reduces the possibility of resistance and political crisis.

Insofar as experience is part of the labor process, the decision to accentuate it has the potential to become a double edged sword. The Israeli homeland security sector boasts about its experience in order to increase the exchange value of the commodity, but by doing so it draws attention to the social relations in the labor process, because experience like all other elements of the labor process is constituted not only by and through "material relations between persons and social relations between things" but also by social relationships between people. In other words, the additional labor that is put in the product (and which increases its exchange value) as a result of the experience gained by testing the different electronic fences, sensors, radar detection systems, and video cameras along the West Bank's separation barrier also includes in it the oppressive relations between Israeli security forces and Palestinians. To be sure, one does not find any mention of Palestinians in the brochures, only the terms terrorists and terrorism, but the trace of the Palestinian subject cannot be totally excised and the intelligent observer understands that the experience that increases the exchange value of Israel's homeland security products is gained due to certain concrete repressive social relations between the security forces and Palestinians.

Second, since experience increases the exchange value of the products, it is only logical to sustain and even augment and diversify the processes and structures that create the experience. The diversification of the Israeli experience, one should note, is crucial, since it can potentially open totally new spheres for the industrial production process. The multifaceted experiences that provides Israeli homeland security with a comparative advantage as well as the credit and stamp of approval all seem to indicate that there is a clear economic motivation to continuously maintain, increase and diversify the experiences, since their termination would compromise the competitiveness of Israel's homeland security commodities and decrease their exchange value.

To be sure, the laboratory model is of relevance here, yet it does not capture as broad a spectrum of phenomena as the experience model. The laboratory model suggests that the Occupied Palestinian Territories and other battlefields in which Israeli forces are active

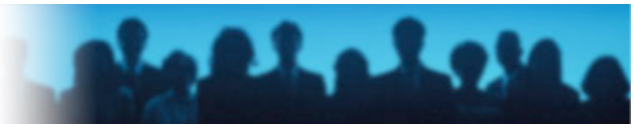


serve as a laboratory to test the performance of certain products. The experience model incorporates the notion of testing performance, but adds both the production process of the products as well as social networking, reputational and ideological dimensions which are deployed in order to market homeland security products. Moreover, the notion of experience helps explain how the field of homeland security reproduces itself.

I have provided a concrete example of one of the ways that Israel intentionally reproduces its own experiences; namely, the whole practice of testing the products manufactured by the homeland security industry in the West Bank, Gaza Strip, Lebanon and Israel itself. Putting the product to the test is carried out in order to check if it works, to fine-tune it, and provide it with some kind of operational certificate that confers credit upon it. But since such product trials are carried out in real life situations they are always overdetermined; the trial itself not only checks the product, but activates a whole series of processes that engender new experiences. The military unit that tests the 360i product when it patrols the separation barrier also undergoes an experience that may, in turn, trigger a succession of new experiences. Moreover, the use of the 360i helps construct an experience that otherwise would not have taken place or would have taken place differently, thus corroborating Michel Foucault's claim that experience is constructed and "exists only after it has been made, not before."[180]

As I understand it, Foucault's claim has two dimensions: ontological and epistemological. Ontologically, experiences do not have a reality before they take place; they do not exist out there in the world and therefore they are always something people construct through their choices, actions and behavior. Epistemologically, we can make sense of an experience only after it has occurred, and the act of making sense is intricately tied to the construction of the experience since experience does not exist before its signification as an experience. This is also how I understand Joan Scott's claim about the ideological assumptions that always inform our experiences.

Such an understanding of experience suggests that the nature of the intentionally created experiences, which appear at the bottom of Figure 2 and are obviously constructed, is not different from the nature of the experiences which appear at the very top of the Figure and instigate the whole process described in this paper's previous sections.[181] There is no essential difference between a military unit that tests the 360i when it patrols the separation barrier and another unit that patrols the separation barrier but does not test the 360i. In both cases the experience is constructed by and through the act of patrolling the barrier alongside the subsequent interpretation given to this act. To be sure, the soldiers in each patrol undergo different experiences, but the differences between them are unrelated to the nature of the experience which in both cases is constructed. Rather, the actual difference involves only the epistemological dimension of the constructive act, and has to do with the justification or the rationale ascribed to the experience. In the case where the military unit tested the 360i as it patrolled the barrier, it is clear that the motivation to produce the experience also came from external economic interests; namely, the interests of the Orad Group which invented and manufactures the product. In the case where the military unit patrols the barrier as part of a daily routine, the experience is generally interpreted as devoid of any external economic motivations, and conceived as

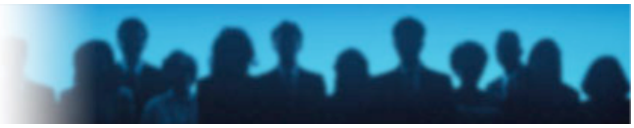


foundationally given, that is, as something that just "is" or exists without any kind of mediation.

My claim is that the acts by and through which the Israeli experiences are constructed – ranging from the experiences of high-tech personal to the experiences of combat soldier – are all propelled by a variety of political, economic, social and cultural forces, while the way the experience is "experienced" is always mediated though one's place in social space. The major difference then between the two military patrols is that in the former case an economic force is, at least partially, acknowledged, while in the latter all motivations that are unrelated to securing the fence are concealed so that the act is naturalized, lacking any obvious external political, economic, social or cultural incentive. Thus, the difference between the "Experience in the Field" frame located at the bottom of Figure 2 and the one at the top is not that the latter is produced by acts that are propelled solely by reasons relating strictly to security, but rather that non-security motivations to carry out the acts that produce the experiences are concealed and therefore more difficult to demonstrate. There is, in general, a reductive move with respect to all the experiences relating to Israeli security.

In sum, an analysis of the political economy of Israel's homeland security industry reveals that there is an economic motivation to both increase the so-called security related experiences and to diversify them. The achievements of this Israeli industrial sector are, in other words, not the result of foundationally given prior experiences -- experiences that are in some sense natural -- but rather all the experiences are constructed and some of them are even produced by the sector itself in order to sustain its own comparative advantage. The ability to demonstrate that experiences are intentionally created so as to support the industrial process and provide it with a comparative advantage is, however, limited to those experiences where the act that produces the experience can be shown to be motivated by economic incentives (e.g., military units that test new products). An analysis based on Scott suggests that the way we construct the experience is informed by the dominant ideological forces, and that the reasons we seldom see the economic motivation behind the military experiences is because the military ideology manages to mask them. It is highly likely that some of the military experiences take place in order to satisfy economic needs and interests, but it is not always so easy to demonstrate such motivations since they are concealed. In other words, the reasoning through which the experience is constructed is a security one and elides the economic, political, social and cultural forces that may have led to the act that produced the experience. Our role, therefore, is to deconstruct the experience so as to trace the motivations and forces that led to its production.

By way of conclusion, I would like to gesture towards two other ways in which the discussion about the Israeli experience can be broadened.

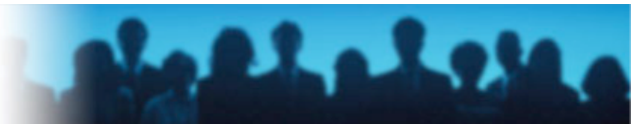


4.3 The Experience of Fighting Terrorism

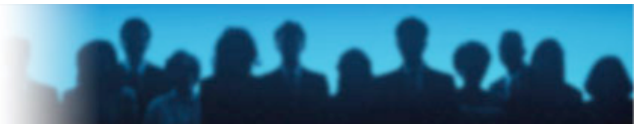
Experience is, as Foucault cogently observed, "something that you come out of changed."[182] Experience changes our relationship with things, people and the world, thus indicating that even as experience itself is constructed, it also, simultaneously, is a constructive force that helps manufacture our reality (i.e., the relations among things, people and the world). And while each individual experience has a personal dimension (the experience of two soldiers on the same patrol is, after all, different), all experiences have a strong social component, both because they are constructed by and through ideological forces and because others "cross paths with [our experiences] or retrace [them]."[183] Thus, the reality that the experience constructs is not confined to the personal, but is ultimately a social reality. Therefore, I understand Foucault's claim that experience is something that you come out of changed, not merely as an observation about the production of individuals as subjects and the construction of their reality, but also about societies. Societies emerge from experience changed and this change helps shape their reality.

For many years now critical sociologists have examined and analyzed the way the military experience has shaped the character, institutions and political, economic, social and cultural relations within Israel and have commented on some of its detrimental effects on Israel.[184] The question I would like to end with is why, following 9/11, the Israeli militaristic experience, which has been known to generate a series of damaging effects, has suddenly became attractive to politicians and political groups in numerous liberal democracies, like the United States and England. Obviously, Israel's experience in fighting terrorism has been center-staged and lauded because its security apparatuses are perceived to be successful in developing strategies to confront what many believe to be one of central threats confronting liberal democracies – namely, terrorism. Hence, one of the attractions is a certain kind of militaristic worldview, which shapes our understanding of reality (e.g., as a continuous conflict between warring sides, a clash of civilizations, etc.) and offers strategies and tactics that provide a solution to this reality, or at least mitigate it.

This paper, however, suggests that the attraction towards the Israeli experience of fighting terrorism is driven by other forces as well, and that the attraction towards the militaristic worldview is merely one of three nodes that operate together, the other two being a neoliberal economic agenda and democracy. Keep in mind that my general claims so far were that Israel's militaristic experiences, like all others, are constructed; that they help explain the development and success of the homeland security industry; and that consequently there is an economic incentive to reproduce these kinds of experiences. More specifically, I maintained that the experience of fighting terrorism is highlighted because it increases the exchange value of the homeland security products and services. Note also that the brochures and corporate executives that boast about the Israeli experience are doing so in order to sell products and services and not to share security strategies.

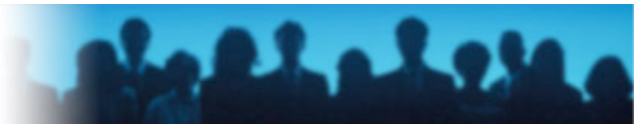


My first claim, then, is that the Israeli experience in fighting terror is attractive not only because Israelis manage to kill "terrorists" (the militaristic worldview), but also because killing terrorists is not necessarily adverse to neoliberal economic objectives, and actually advances them. My second claim has to do with the fact that this is taking place in Israel and not in Saudi Arabia or Egypt, for example. This is crucial, because the former is considered to be a democracy, while the latter two are not. This attraction stems from the sense (real or perceived) that fighting terrorism through methods of homeland security, that include suspending due process in many areas of the criminal justice system, including torture, the right to a speedy trial, the freedom from arbitrary police searches, and the prohibition against indefinite incarceration and incognito detentions (to mention a few methods) does not conflict with democratic values. Thus, the ultimate attractiveness towards the Israeli experience in fighting terrorism is to its ability to link a militaristic worldview with a neoliberal economic agenda and a democratic political regime. The Israeli experience, in other words, purports to show that a democratic political system, a neoliberal economic agenda, and hyped-security strategies can be connected together, without one harming the other. This, to be sure, is a constructed experience.

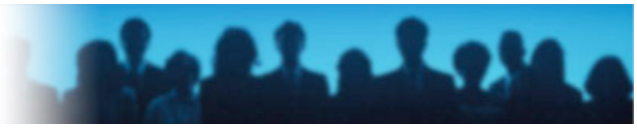


Appendix 1: Websites

Company Name	Website
3DVU	http://www.3dvu.com
4DM Tech	http://www.4dm-tech.com
Accubeat	http://www.accubeat.com
Acrosec	http://acrosec.com/
Aeronautics	http://www.aeronautics-sys.com/
AGS Encryptions	http://www.agsencryptions.com
Alladin Knowledge Systems	http://www.aladdin.com
Allot Communication	http://www.allot.com/
Alvarion	http://www.alvarion.com/
Arcnet	http://www.arcnet.ws/
ARX - Algorithmic Research	http://www.arx.com
Algosec	http://www.algosec.com
Aliroo	http://www.aliroo.com
Applicure	http://www.applicure.com
Artivision	http://www.artivision.com.sg
Asero	http://www.asero.com/
Audiocodes	http://www.audiocodes.com/
Athena	http://www.athenaiss.com/
Avnet	http://www.avnet.co.il/
Azimuth	http://www.azimuth.co.il/
BA Microwaves	http://www.bamicrowaves.co.il
Bar-Kal	http://www.bar-kal.com/
Baran Group (of which Baran Raviv is a subsidiary)	http://www.barangroup.com/
BeepCard	http://www.beepcard.com
Beit Alfa Technologies	http://www.bat.co.il/
Ben Security	http://www.ben-security.co.il
Bental	http://www.bental.co.il/
BeyondSecurity	http://www.beyondsecurity.com/
Bio Guard	http://www.bio-guard.net/
Bio Sense	http://www.bio-sense.com/
Biological Alarm Systems (B.A.S)	http://www.basdetect.com/
BOS Better Online Solutions	http://www.boscorporate.com/index.asp
Bsafe	http://www.bsafesolutions.com
Bsecure	http://www.bsecuregroup.com/
Camero	http://www.camero-tech.com
Cellocator also known as Pointer Tel	http://www.cellocator.com/
Check Point	http://www.checkpoint.com
CipherActive	http://www.cipheractive.com
CNOGA	http://www.cnoga.com
CodeRed	http://www.code-red.biz
Commtouch	http://www.commtouch.com
Comsec	http://www.comsec.co.il/
Comverse	http://www.comverse.com/index.aspx
Control Guard	http://www.controlguard.com/
Controp	http://www.controp.com/
CornerShot	http://cornershot.com/
Cortex	http://www.cortex.co.il
Cyber Ark	http://www.cyber-ark.com
D-Fence	http://www.d-fence.com/
DDS	http://www.dds-security.com/
Defensoft (Form. 3D Act)	http://www.defensoft.com/
Demco	http://www.demco.co.il
Demoman	http://www.demoman.co.il/
Discretix	http://www.discretix.com

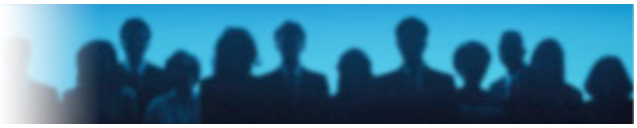


Company Name	Website
Dmatek	http://www.dmatek.com/
Diverse Security Technologies (Formerly Safecard)	http://www.dstid.com/
Dr. Frucht Systems	http://www.smartsecsystems.com/
DSIT Technologies	http://www.dsit.co.il
Dynamtech	http://www.dynamtech.com/
Dynasec	http://www.dynasec.org
ECI	http://www.ecitele.com/Pages/default.aspx
Ectel	http://www.ectel.com/
E.M.G	http://www.emg.co.il
Ephod Magen Security (HawkEye)	http://www.hawkeye.co.il
Encotone	http://www.encotone.com
El - Go Team	http://www.elgoteam.com
El - Op	http://www.el-op.com/
El Far	http://www.elfar.co.il
Elbex	http://www.elbex.com/
Elbit Systems	http://www.elbitsystems.com/
Electronics Line 3000	http://www.electronics-line.com
Elisra	http://www.elisra.com/
Elmotech	http://www.elmotech.com
Elpam Electronics	http://www.elpam.com
Elta (Israel Air Industry)	http://www.iai.co.il
Eltel Technologies (Elul Group)	http://www.elul.com/category/Eltel
Emit	http://www.emituav.com/home.asp
EMZA	http://www.emza-vs.com/
Esc Baz	http://www.escbaz.com/
Essence Security	http://www.essencesecurity.com/
Eurekify	http://www.eurekify.com
Evidence Med	http://www.edvice-med.com/
Excalibur	http://www.mil-1553.com/
Exsys	www.exsys.co.il
Finjan	http://www.finjan.com
ForeScout	http://www.forescout.com
Galdor	http://www.galdor.com/
Galteam	http://www.galteam.com/
G.M.Fencing	http://www.gmsecurity.com/
Gita Technologies	http://www.gita.co.il
Global Security S. Group	http://www.global-security-sgr.co.il
Goldtec Technologies	http://goldtech.pionet.com/
Gordon	http://www.gordonengineers.com/
Goshen	http://www.goshen-security.co.il/
Guardium	http://www.guardium.com
Hashmira	http://www.hashmira.com/
Hi - G - Tek	http://www.higtek.com
Hi - Tech Soulutions	http://www.htsol.com
HomeNet	http://www.homenetip.com
Hydromechanical Engineering	http://www.hec-eng.com/
Idesia	http://www.idesia-biometrics.com/
IDSST	http://www.idsst.com
ImageID	http://www.imageid.com/
Imperva	http://www.imperva.com/
InexZamir	http://www.inexzamir.com
InkSure	http://www.inksure.com/
Innocon	http://www.innoconltd.com
InterVox	http://www.inter-vox.com/
IQS	http://www.biometric-center.com
ISC Security	http://www.isc-security.com/
ISDS	http://www.isds.co.il/
Isorad	http://www.isorad.co.il/
ISR (Integrated System Research)	http://www.isrfleettrack.com/

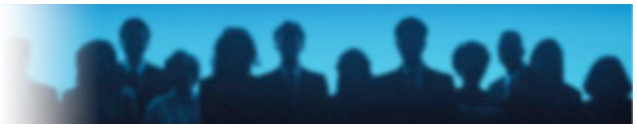


Company Name	Website
Israel Military Industries	http://www.imi-israel.com/
IsraTeam	http://www.israteam.com/
Itcon	http://www.itcon-ltd.com
ITL	http://www.itlasers.com/
ITRR	http://www.terrorresponse.org
ITS Telecom	http://www.its-tel.com
Iturn Group	http://web.sadna.co.il/ituran/website/home/index.html
K-9	http://www.k-9-solutions.com/eng/aboutus_eng.html
Kavit	http://www.kavit.com/
Kidaro	http://www.kidaro.com
Kidumit	http://www.kidumit.com/
KP Electronic Systems	http://www.kpsystems.com
Lamda	http://www.lamda-sys.co.il
LIT	http://www.miragelit.com
Location Net	http://www.locationet.com
Lumio	http://www.lumio.com/
Magal	http://www.magal-ssl.com
Mayan Ventures	http://www.myv.co.il/HTMLs/article.aspx?C2004=12575&BSP=12556
Mango Dsp	http://www.mangodsp.com
Mate	http://www.mate.co.il/
Maximum Security	http://www.maximum.co.il/
Mavix	http://www.mavix.com
mConfirm	http://www.mconfirm.com/
Megason	http://www.megason.co.il
MeproLight	http://www.meprolight.com/
Mer Group	http://www.mer-group.com/
Metalink	http://www.mtlk.com/Management.asp
Mi5	http://www.mi5networks.com
MicroTag Temed	http://www.microtag-temed.com

Company Name	Website
Mifram	http://www.miframsecurity.com/e/Miframm_Company_Profile_ENG.asp
Mipha	http://www.mipha.co.il
Mistral Group	http://www.mistralgroup.com
M.L.M.	http://www.mlm-protection.com/
NDS	http://www.nds.com
Nemesysco	http://www.nemesysco.com/
Ness	http://www.ness.com
Netline	http://www.netline.co.il/
New Noga Light	http://www.nogalight.com/
Nice Systems	http://www.nice.com
Nirtal	http://www.nirtal.com/
ODF Optronics	http://www.odfopt.com
Ofek	http://www.ofek-air.com/
Ofil	http://www.ofilsystems.com/
Opgal Optronics	http://www.opgal.com
Ophir Optronics	http://www.ophiropt.com
Optibase	http://www.optibase.com/
Optisec	www.optisec-systems.com
Orad Group	http://www.orad.cc
Orbit	http://www.orbit-techgroup.com/
Orsus	http://www.orsus.com/
Ortek	
OTI	http://www.otiglobal.com/
OzVision	http://www.ozvision.com
Patus	http://www.odorscreen.com/
Persay	http://www.persay.com
PineApp	http://www.pineapp.com
Praxell	http://www.praxell.com
Protrack	http://protrack.co.il/
Rad Data	http://www.rad.com/
Rafael	http://www.rafael.co.il/



Rada	http://www.rada.com	Synel Systems	http://www.synel.com
Radware	http://www.radware.com/	Tadlys	http://www.tadlys.com/
RBTech	http://www.rbtec.com/	Tandu	http://www.tandu.co.il/
Recognix	http://www.recognix.com/	Tar Ideal	http://www.tarideal.com/
Reflex Security	http://www.reflexsecurity.com/	Team 3	http://www.team3.co.il/
Risco Group	http://www.riscogroup.com/	Telefire	http://www.telefire.co.il
Rontal	http://www.rontal.co.il/	Telematics Wireless	http://www.tlmw.com
Rotan	http://www.rotan.co.il/index.swf	Teletron	http://www.teletron.co.il
Rotem Industries	http://www.rotemi.co.il/	The Israeli College for Security and Investigation	http://www.code.co.il/
Safend	http://www.safend.com/	Tidex	http://www.tidexsystems.com/
Sam Zonensein	http://www.z007.co.il/	TimCon	http://www.timcon.co.il/
Scent Detection Technology (SDT)	http://www.scent-tech.com	Top I Vision	http://www.topivision.com/
Scsquare	http://www.scsquare.com	Top Image Systems, Ltd.	http://www.topimagesystems.com/
Sdema	http://www.sdemagroup.com/	TraceGuard	http://www.traceguard.com
SecureOL	http://www.secureol.com/	TraceSpan	http://www.tracespan.com
SecuSystem	http://www.secu-system.co.il	TransTech	http://www.transtech-solutions.com/
Septier	http://www.septier.com	Trellidor	http://www.trellidor.co.il/
Seraphim Optronika	http://www.seraphim.co.il/	Urban Aeronautics	http://www.urbanaero.com/
Servision	http://www.servision.net/	V-Secure Technologies	http://www.varonis.com
SESP	http://www.sesp.com/	Verint	http://verint.com/corporate/
Shafran	http://www.shafran.biz/	Video Domain	http://www.vdomain.com
Simlat	http://www.simlat.com/	Vidisco	http://www.vidisco.com
SkyBox	http://www.skyboxsecurity.com	Vigilant Technologies	http://www.vigilanttechnology.com
Snapshield	http://www.snapshield.com/	Visonic	http://www.visonic.com
SofaWare	http://www.sofaware.com	Voicesense	http://www.voicesense.com/
SoSecure	http://www.so-secure.com	VsAccess	**http://www.visonictech.com**
SpaceLogic	http://www.space-logic.com	Vuance	http://www.supercom-inc.com/
Spectronix	http://www.spectrex-inc.com/	Vumii	http://www.vumii.com/
Spetrotec	http://www.spetrotec.co.il/	White Cell	http://www.white-cell.com
SpiderTech	http://www.spidertech-security.com/	WonderNet	http://www.penflow.com/
Spike	http://www.spikesecurity.com/	Xsights Sysytems	http://www.xsightsys.com/
Steadicopter	http://www.steadicopter.com/	Zamir	http://www.zamir.co.il



Endnotes

[1] Ministry of Industry, Trade and Labor, *Israel Homeland Security: Opportunities for Industrial Cooperation*, Tel-Aviv, 2005.

[2] Ministry of Industry, Trade and Labor, *Israel Homeland Security*, p. 24 italics added.

[3] See, for example, Pine, B.J. II and Gilmore, J.H., *The Experience Economy: Work Is Theatre and Every Business a Stage*, (Harvard Business School Press, Boston, MA, 1999). Jeremy Rifkin, *The Age of Access: The New Culture of Hypercapitalism, Where all of Life is a Paid-For Experience*, (Los Angles: Tarcher, 2001).

[4] Rifkin, *The Age of Access*.

[5] Martin Jay, The Limits of Limit-Experience: Bataille and Foucault, *Constellations,* Vol. 2 (2), April 1995: 155-174. Martin Jay, *Songs of Experience: Modern American and European Variations on a Universal Theme*, University of California Press, 2005.

[6] Ministry of Industry, Trade and Labor, *Israel Homeland Security*, p. 14 italics added.

[7] Press Release, "Beijing Metro Selects NICE's Next Generation Security Solutions to Enhance Safety and Security at More than 20 Stations," April 17, 2006 online http://www.nice.com/news/show_pr.php?id=584.

[8] See DDS website http://www.dds-security.com/site/news-motorola3.html.

[9] See Clicksoftware website http://www.clicksoftware.com/index.asp.

[10] It also reflects the contacts the Israeli military has with China.

[11] See Invest in Israel online at http://www.investinisrael.gov.il/NR/exeres/7C2F6937-A259-4A4A-9C29-DE351032B87A.htm.

[12] This is not altogether surprising considering that Israeli high-tech companies are among the pioneers of biometric technologies for ID verification, radio frequency identification (RFID) technologies, computer security and electro-optical night vision systems. See Invest in Israel online at http://www.investinisrael.gov.il/NR/exeres/7C2F6937-A259-4A4A-9C29-DE351032B87A.htm. and Industrial Cooperation Authority, "Learning from Israel's Experience," Tel-Aviv, 2005 also online at http://www.israexport.co.il/hls/art.asp?Id=208.

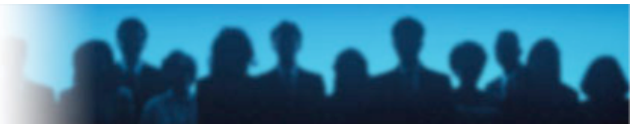
[13] For more information about Nice Systems consult http://www.nice.com.

[14] David Lyon, ed. Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination, London: Routledge, 2003, pg. 11.

[15] David Lyon, "Surveillance Technologies: Trends and Social Implications," in Barrier Stevens, ed. *The Security Economy*, Organization of Economic Co-Operation and Development, 2004.

[16] Lyon, *Surveillance as Social Sorting*.

[17] Lyon, *Surveillance as Social Sorting*.



[18] Lyon, *Surveillance as Social Sorting*.

[19] Barrier Stevens, "The Emerging Security Economy: An Introduction" in *The Security Economy*, Organization of Economic Co-Operation and Development, 2004.

[20] The Israeli Defense, Aerospace and Security Industries, "The Battlefield is a Hotel Lobby," Newsletter # 4 online at http://www.tradingmarkets.com/.site/news/Stock%20News/930927/.

[21] Stevens, "The Emerging Security Economy," p. 18.

[22] Robert Mandel, *Armies Without States: The Privatization of Security*, Boulder, CO: Lynne Reinner, 2002.

[23] David Lyon, Surveillance Studies: An Overview, Cambridge: Polity, 2007, p.14

[24] See online at http://www.israeljobsites.co.il/companies/security_companies.asp.

[25] Therefore it is difficult if not impossible to assess the size of a surveillance industry in these countries. For information on India's high-tech industry consult NASSCOM at http://www.nasscom.in/Default.aspx. For information on Ireland's high-tech industry consult ICT Ireland http://www.ictireland.ie/Sectors/ICT/webict.nsf/wHome?OpenForm and the national software directorate http://www.nsd.ie. For information on Taiwan's high-tech industry consult the Industrial Technology Research Institute http://www.itri.org.tw/eng/index.jsp.

[26] See http://www.export.gov.il/Eng.

[27] Israel Export and International Cooperation Institute, "Israel: Security and HLS Industries," Tel-Aviv, 2007.

[28] Israel Export and International Cooperation Institute, "Israel: Security and HLS Industries," Tel-Aviv, 2007.

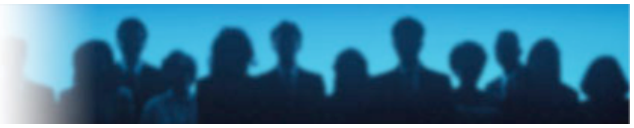
[29] A nearby kindergarten in Ann Arbor Michigan has installed a biometrics system so that parents can enter the premises only after their thumb print has been identified. Israel Export and International Cooperation Institute, "Israel: Security and HLS Industries," Tel-Aviv, 2007.

[30] Cellocator is traded on Nasdaq under the name Pointer Telocation LTD. See http://www.cellocator.com and http://www.e-drivetech.com/fleetLog01.html.

[31] Richard Silberglitt, Philip S. Antón, David R. Howell, Anny Wong, et al., The Global Technology Revolution 2020, In-Depth Analyses: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Social Implications, (Santa Monica, CA.: RAND Corporation, 2006), p. 217.

[32] Nick Denes, Universalising the Unique: Israeli UAV Exports, Border-Security Doctrines and Global War, paper presented at the State of Exception Workshop to be held in Larnaca, Cyprus on 6-8 December, 2008.

[33] See http://www.export.gov.il/Eng/Branch.asp?CategoryID=307.



[34] Even before 9/11 Israeli air-traffic controllers carefully scrutinized all movements of aircraft in the region. Planes are tracked by transceivers in the pilot's cockpit, which send a digital signal to air traffic controllers. Interestingly, the aircraft hijacked on September 11th were all fitted with transceivers. The problem was that the air traffic controllers and other security agencies did not take matters seriously when the hijackers turned off the transceivers. In Israel, even before 9/11, the disappearance of a transceiver signal has always resulted in the scrambling of fighter jets to protect the country's skies and high-rise buildings. These transceivers are backed up by conventional radar systems operated by the Israel Air Force. Over the years there have been incidents of unidentified civil aircraft encroaching on Israel's air space from both Libya and Lebanon, which have been shot down when approaching the country's population centers. Industrial Cooperation Authority, "Securing the Skies," Tel-Aviv, 2005. This brochure can also be accessed online at http://www.israexport.co.il/hls/art.asp?Id=202.

[35] See "Securing the Skies" at http://www.israexport.co.il/hls/art.asp?Id=202.

[36] Magal Security Systems, we are told, has not only designed such fences but also an innovative jet lock product to detect and prevent unauthorized movement of airplanes on the ground. See "Securing the Skies" at http://www.israexport.co.il/hls/art.asp?Id=202.

[37] The fact that Israel has acquired an international reputation vis-à-vis such issues helps explain why the first annual International Security Forum of Ministers of Interior and Public Security convened in Jerusalem for a conference called "Challenges to Homeland Security." According to an official press release, ministers from nine countries congregated in May 2008 – including Canada, England, France, Germany, Israel, Italy, Poland, Spain, and the United States – in order to strengthen homeland security cooperation. Israel, the press release added, "will demonstrate some of its expertise, including understanding the psychology of suicide bombers and how to foil airplane hijackings."The Associated Press, "U.S., Israel, Canada and European countries co-operate on anti-terror efforts," May 28, 2008.

[38] The hurdle in implementing a substantive behavior detection program in the US is overcoming critics that it is racist profiling. Transportation Security Administration (TSA) Secretary Kip Hawley has argued that behavior detection is not profiling.

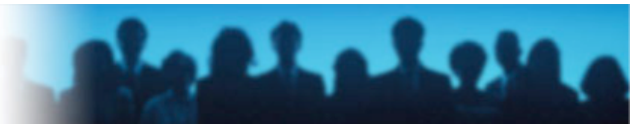
[39] According to *Homeland Security Today*, Ben Gurion airport does not impose US security screening policies, like having passengers remove laptops from their carrying cases and take off shoes, jackets, belts, etc." The need for this kind of screening, Nahum Liss, head of the Planning, Control and Projects Department of the Ben Gurion Security Division explained, "had already been eliminated many security steps back, beginning even before passengers stepped foot through the doors of the airport." Anthony L. Kimery, DHS Looks to Adopt Israeli Airport Security Methods, *Homeland Security Today*, May 30, 2008.

[40] "IDO Security Announces First Sale of MagShoe in US," July 23, 2008. http://www.idosecurityinc.com/press_First_US_Sale.html

[41] See http://www.lightspeedanalyst.com

[42] For K-9 Solutions see online http://www.k-9-solutions.com/eng/aboutus_eng.html and for Mifram Group see online http://www.miframsecurity.com/e/observation_towers.html.

[43] The different components of ICT are defined in the following way: Electronic components: manufacture of electronic chips, semiconductors, microelectronic components, printed circuits, etc.; Electronic communication equipment: manufacture of telecommunications equipment, computer communications equipment, and electronic equipment such as transmitters, facsimiles, etc.; Equipment for control and



supervision: manufacture of electronic equipment for quality control, systems for security control, equipment for control towers, etc.; Telecommunications services: sound, video, data, or other information by telephone, cable, broadcasting or satellite, data communications, etc.; Computer and related services: hardware and software consultancy, programming and system planning, data processing, preparation of database and data storage activities, etc.; Research and Development (R&D) services include systematic and original activity intended to generate new scientific or technological knowledge, or to develop new applications of existing scientific or technological knowledge; Start-up companies are small enterprises established for the purpose of developing a new product or technology, mainly in the fields of software, Internet and telecommunications. Galia Yohay and Nurit Yaffe, Information and Communication Technologies in Israel: 1990-2002, Central Bureau of Statistics, 2003, Statistilite No. 36.

[44] Since diamonds are initially imported to Israel at great cost and then cut in Israel and exported at a profit, the inclusion of this industry in the export figure provides a blinkered perspective since it does not take into account import costs.

[45] Central Bureau of Statistics, "ICT sector estimate for 2006: growth in GDP, Exports and Employment," Press release May 14th, 2007. (in Hebrew). Central Bureau of Statistics, "Imports and exports, by the standard international Trade classification – SITC (revised III)," 16.4 Statistical Abstract Of Israel 2007: 657-658.

[46] Central Bureau of Statistics, "Israel's Balance of Manufacturing Exports and Imports, by Technological Intensity, 2006," Press release, July 23, 2007. According to The Israel Export and International Cooperation Institute. twenty-six percent of high-tech exports are equipment for control and supervision, totaling $3.7 billion, an increase of 17 percent compared with 2005. See The Israel Export and International Cooperation Institute, "Trade Overview: Summary 2006," on the web at http://www.export.gov.il/_Uploads/15362israel.pdf.

[47] Central Bureau of Statistics, "Imports and Exports, by the Standard International Trade Classification - Sitc (Revised Iii)," 2007, No. 16.4.

[48] InfiniBand is a switched fabric communications link primarily used in high-performance computing, while Orthogonal frequency-division multiplexing is a frequency-division multiplexing scheme utilized as a digital multi-carrier modulation method.

[49] See http://www.nasdaq.com. The data was accessed in June 2008.

[50] Guy Griml, Three Israeli firms top the Fast-500 ranking," Ha'aretz, November 27, 2007. See also A Technology, Media & Telecommunications industry group report "Stellar Performers: Technology Fast 500 EMEA Ranking and CEO Survey 2007," Deloitte Touche Tohmatsu, November 2007.

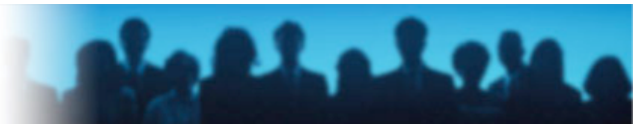
[51] The Israel Export and International Cooperation Institute, "Israel Security and HLS Industries," January 2007. For a list of the six big military producers, their revenues and number of employees see online http://duns100.dundb.co.il/ts.cgi?tsscript=/2007e/e59a1_sector&sec_name=Producers%20of%20Electronic%20Security%20Sys.%20%26%20Equip

[52] See http://www.agentvi.com/.

[53] See online at http://www.optisec-systems.com.

[54] See http://www.agentvi.com/.

[55] For a list of the major companies and their sales consult Dun and Bradstreet Israel under the category Producers of Electronic Security Systems and Equipment on the web http://duns100.dundb.co.il.



[56] Ash Amin, ed. Post-Fordism: A Reader, Oxford UK: Blackwell 1994. See in particular the chapters by Charles Sabel, John Tomaney and Bob Jessop.

[57] Dov Dvir and Asher Tishler, "The Changing Role of the Defense Industry in Israel's Industrial and Technological Development," in Judith Reppy, ed., *The Place of the Defense Industry in National Systems of Innovation,* Cornell University Peace Studies Program, Occasional Paper #25, 2000.

[58] SIPRI Yearbook 2008.

[59] Its researchers were considered academics and were granted all the educational benefits of full time academic staff, including a sabbatical every seven years, which most of them spent outside Israel at leading academic universities or IT companies. Breznitz, *Innovation and the State*, 48.

[60] The Weizmann Institute of Sciences began the development of a computer in the early 1950s.

[61] Daniel Vekstein and Abraham Mehrez, "Technology Policy and Defense Conversion in Israel, 1967-1995," *Journal of Technology Transfer*, Vol. 22 (1), 1997: 47-56.

[62] D. Dvir, and A. Tishler, 'The Changing Role of the Defense Industry in Israel's Industrial and Technological Development', *Defense & Security Analysis*, Vol. 16, No. 1, 2000: 33-51. Central Bureau of Statistics, *Statistical Abstract of Israel 2007*, "Labor force Surveys," 12.1, 2007: 502 on the web at www.cbs.gov.il.

[63] Dvir and Tishler, "The Changing Role of the Defense Industry in Israel's Industrial and Technological Development," p. 198.

[64] Israel Azulay, Miri Lerner and Asher Tishler, "Converting military technology through corporate entrepreneurship," *Research Policy*, Vol. 31, No. 3, 2002: 419-435.

[65]Moshe Justman, "Structural Change and the Emergence of the Israeli High-Tech Sector," in Avi Ben-Bassat, *The Israeli Economy 1985-1998: From Government Intervention to Market Economics*, Cambridge MA: MIT Press 2002, 445-483.

[66] Justman, "Structural Change and the Emergence of the Israeli High-Tech Sector," 445-483.

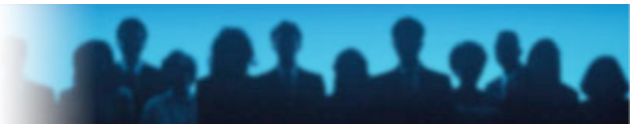
[67] Azulay, Lerner and Tishler, "Converting military technology through corporate entrepreneurship," 419-435.

[68] John Rossant and Neal Sandler, "Out of the Desert," *Business Week*, August 21, 1995.

[69] Local defense expenditure was reduced as the government tried to rein in hyperinflation through a series of deep cuts in domestic expenditure. Consequently, the IDF bought far less from the local industry, opting for American products paid through US military aid to Israel. See Sadeh, "Israel's Defense Industry in the 21st Century."

[70] Gil Avnimelech, and Morris Teubal, "Venture capital start-up co-evolution and the emergence & development of Israel's new high tech cluster," *Economics of Innovation and New Technology*, Vol. 13, No. 1, 2004: 33-60.

[71] Halperin, A. *The Dependence of the Israeli Defense Industry on American Foreign Aid.* (In Hebrew). Tel Aviv: The Israeli International Institute for Applied Economic Policy Review, 1992.



[72] Azulay, Lerner and Tishler, "Converting military technology through corporate entrepreneurship," 419–435.

[73] Local defense expenditure was reduced as the government tried to rein in hyperinflation through a series of deep cuts in domestic expenditure. Consequently, the IDF bought far less from the local industry, opting for American products paid through US military aid to Israel. Sharon Sadeh, "Israel's Defense Industry in the 21st Century: Challenges and Opportunities," *Strategic Assessment,* Vol. 7. No. 1, 2004.

[74] Daniel Vekstein and Abraham Mehrez, "Technology Policy and Defense Conversion in Israel, 1967-1995," *Journal of Technology Transfer*, Vol. 22 (1), 1997: 51.

[75] Breznitz, "Collaborative Public Space in a National Innovation System: A Case Study of the Israeli Military's Impact on the Software Industry," *Industry and Innovation*, Vol. 12, No. 1, 2005: 31–64.; G. Ariav and S. E. Goodman, "Israel: of swords and software plowshares," *Communications of the ACM*, 37(6), 1994: 17–21.

[76] Ariav and Goodman, "Israel: of swords and software plowshares," p. 18.

[77] Breznitz, "Collaborative Public Space in a National Innovation System,"; Ariav and Goodman, "Israel: of swords and software plowshares."

[78] Cited in Breznitz, "Collaborative Public Space in a National Innovation System," p. 47.

[79] Breznitz, "Collaborative Public Space in a National Innovation System," p. 47.

[80] Breznitz, "Collaborative Public Space in a National Innovation System," p. 48.

[81] Breznitz, "Collaborative Public Space in a National Innovation System," p. 48.

[82] Cited in Dan Breznitz, "Collaborative Public Space in a National Innovation System," p. 48.

[83] Christopher Rhoads, "Secret Weapon: How an Elite Military School Feeds Israel's Tech Industry," *Wall Street Journal*, July 6, 2007.

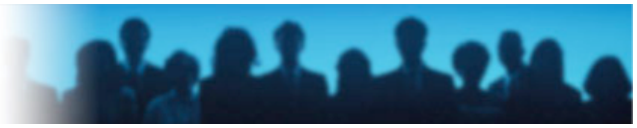
[84] Cited in Dvir, and Tishler, "The Changing Role of the Defense Industry," p. 38.

[85] Ayala Malach-Pines , Dov Dvir, Arik Sadeh , "The Making of Israeli High-technology Entrepreneurs: An Exploratory Study" *Journal of Entrepreneurship*, Vol. 13, No. 1, 2004: 29-52.

[86] Avnimelech and Teubal, "Venture capital start-up co-evolution," pp. 33-60. While the Office of the Chief Scientist invested about $2.5million in R&D in the late sixties, government R&D distributions to the business sector reached close to $300 million in 1996.

[87] Avnimelech and Teubal, "Venture capital start-up co-evolution," p. 40.

[88] Dan Breznitz, "Diffusion of Academic R&D Capabilities as an Industrial Innovation Policy? The Development of Israel's IT Industry," Cambridge, MA: MIT Industrial Performance Center (IPC), May 2004, p. 10, online at web.mit.edu/ipc/publications/papers.html.



[89] The expenditure on R&D as percentage of GDP (Gross Domestic Product) in 1999 was 3.6 percent, tiie highest rate in the OECD (Organization for Economic Cooperation and Development) countries. In comparison, the expenditure in Japan was 3 percent and in the USA, 2.3 percent.

[90] Avnimelech and Teubal, "Venture capital start-up co-evolution," 33-60. See also Ayala Malach-Pines, Dov Dvir and Arik Sadeh The Making of Israeli High-technology Entrepreneurs." Op. cit.

[91] Schwartz, "Prosperity without Peace," *Fortune Magazine*, June 13, 2005.

[92] Israel Export and International Cooperation Institute, "Israel: Telecommunications Industry," Tel-Aviv, 2007.

[93] Avnimelech and Teubal, "Venture capital start-up co-evolution," p. 41. Breznitz, "Diffusion of Academic R&D Capabilities," p. 21.

[94] Avnimelech and Teubal, "Venture capital start-up co-evolution," p. 41. The two authors trace the growth of the high-tech industry to a series of government investments in venture capital funds, the most important of which was Yozma (initiative in Hebrew); a $100M Government owned Venture Capital company, which invested in 10 privately owned Funds which operated in Israel. Yozma, they claimed, triggered the emergence of Israel's venture capital industry.

[95] Breznitz, "Diffusion of Academic R&D Capabilities," p. 23.

[96] Central Bureau of Statistics, "Israel's Balance of Manufacturing Exports and Imports, by Technological Intensity, 2006," Press release, July 23, 2007.

[97] Israeli Venture Capital Research Center, "2007 Summary of Israeli High-Tech Company Capital Raising" online at http://www.iva.co.il/data/uploads_EN/pdfs/IVC_Q4-07_Survey.pdf.

[98] According to *Globes*, Israel's most important business newspaper, "NASDAQ is the US 'home' for Israeli firms."Asaf Homossany, Developments at Nasdaq, Globes Online, December 7, 2007. The numbers of non-US companies traded was downloaded from NASDAQ's website on June 20, 2008.

[99] See the Israeli High-tech Knowledge Portal at http://www.lightspeedanalyst.com/israel_hitech/Template1/Pages/StartSearchPage.aspx.

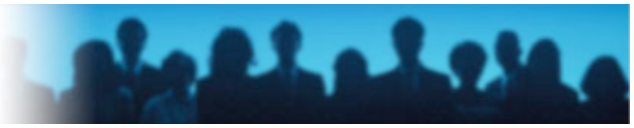
[100] Therefore it is difficult if not impossible to assess the size of a surveillance industry in these countries. For information on India's high-tech industry consult NASSCOM at http://www.nasscom.in/Default.aspx. For information on Ireland's high-tech industry consult ICT Ireland http://www.ictireland.ie/Sectors/ICT/webict.nsf/wHome?OpenForm and the national software directorate http://www.nsd.ie. For information on Taiwan's high-tech industry consult the Industrial Technology Research Institute http://www.itri.org.tw/eng/index.jsp.

[101] Breznitz, "Collaborative Public Space in a National Innovation System," p. 40.

[102] Dan Breznitz, *Innovation and the State: Political Choice and Strategies for Growth in Israel, Taiwan and Ireland*, New Haven CT: Yale University Press, 2007, pp. 72-73.

[103] See online http://www.magicsoftware.com/18-en/home.aspx.

[104] See online at http://www.export.gov.il/Eng/_Articles/Article.asp?CategoryID=909&ArticleID=7460



[105] F. Chesnais cited in Daniel Vekstein and Abraham Mehrez, "Technology Policy and Defense Conversion in Israel, 1967-1995," *Journal of Technology Transfer*, Vol. 22 (1), 1997: 50.

[106] Smith, R. M., *Military Enterprise and Technological Change: Perspectives on the American Experience*, Cambridge, MA: MIT Press, 1985.

[107] The two authors underscore that a number of governmental committees that have stressed the potential of conversion, but that their recommendations were never introduced. Vekstein and Mehrez, "Technology Policy and Defense Conversion in Israel, 1967-1995," p. 57.

[108] Dvir, and Tishler, "The Changing Role of the Defense Industry in Israel's Industrial and Technological Development," 33-51.

[109] Schwartz, "Prosperity without Peace," *Fortune Magazine*, June 13, 2005.

[110] See Given Imaging at http://www.givenimaging.com/en-us/Pages/GivenWelcomePage.aspx.

[111] Schwartz, "Prosperity without Peace," *Fortune Magazine*, June 13, 2005.

[112] Joel Greenberg, "Israelis turn military skills into Software Export Boom," *New York Times,* August 18, 1997 online at http://www.nytimes.com/library/cyber/week/081897ware.html#1. Geotek no longer exists.

[113] See online http://www.enigma.com/e.

[114] Dvir, and Tishler, "The Changing Role of the Defense Industry in Israel's Industrial and Technological Development," 33-51.

[115] Malach-Pines , Dvir, Sadeh , "The Making of Israeli High-technology Entrepreneurs."

[116] Breznitz, "Collaborative Public Space in a National Innovation System."

[117] I am grateful to Elia Zureik for alerting me to this dimension of Breznitz notion of collaborative public space.

[118] Breznitz, "Collaborative Public Space in a National Innovation System."

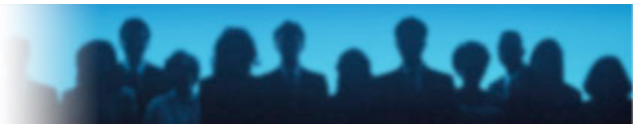
[119] Every Israeli citizen who has served in the military is required to serve for up to 30–40 days a year as part of the reserve duty. Men, in non-combat units, usually serve until the age of 50–56. Women are usually exempt, except for those who have specific skills and training who are usually called to reserve duty until the age of 26.Vekstein and Mehrez, "Technology Policy and Defense Conversion in Israel, 1967-1995," p. 54. Dvir, and Tishler, "The Changing Role of the Defense Industry in Israel's Industrial and Technological Development," 33-51.

[120] Breznitz, "Collaborative Public Space in a National Innovation System."

[121] Breznitz, "Collaborative Public Space in a National Innovation System."

[122] Breznitz, "Collaborative Public Space in a National Innovation System."

[123] See online at http://www.4dm-tech.com.



[124] See online at http://www.arx.com.

[125] See online at http://www.camero-tech.com.

[126] See online at http://www.idsst.com/idse/index.asp.

[127] See online at http://www.athenaiss.com/default.asp

[128] See online at http://www.team3.co.il. Since 1994 Nir Gilboa, the son of Mr. Yoram Gilboa, is acting as CEO of "Team 3 Ltd." Team 3 is the fastest growing security company in Israel. It is classified by Dun & Bradstreet among the 10 leading security companies in Israel. The company has several subsidiaries in various fields related to security, protection and safely and is currently employing 2,200 employees.

[129] Pierre Bourdieu, *In Other Words, Essays,*

Towards a Reflexive Sociology, Stanford: Stanford University Press 1994, p. 135.

[130] It also helps corroborate Barak and Sheffer's claim that in contrast to traditional and critical approaches which speak of "fragmented boundaries" between purportedly autonomous security and civil spheres, or of a "partnership" between them, Israel's security network works against systemic differentiation, creating a high level of continuous mutual penetration and interdependency among the different spheres of Israeli society. The two authors trace this tendency to Israel's establishment, maintaining that the boundaries between the security and civilian spheres of the nascent state were deliberately kept porous, and ultimately allowed security officials to penetrate civilian realms and forge alliances and networks with influential actors within them.

[131] Two types of actors that make up Israel's Security Network: first, prominent members of the state's large and varied defense establishment; second, influential actors within its various civilian spheres, particularly in its "political society" and "civil society." The first category of actors includes "security officials" in active service, that is, senior army officers and their equals in the state's other security apparatuses. The second category includes retired security officials (including officers in the army's reserves) who have been integrated into various political, socioeconomic, and cultural spheres, as well as a host of civilian politicians, bureaucrats, private entrepreneurs, and journalists on the national and local levels. Oren Barak and Gabriel Sheffer, "Israel's Security Network," *International Journal of Middle East Studies,* 38 2006: 235–261.

[132] Barak and Sheffer, "Israel's Security Network," p. X.

[133] Bourdieu, *In Other Words,* p. 135.

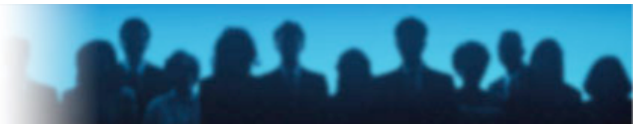
[134] Bourdieu, *In Other Words,* p. 137-138.

[135] Bourdieu, *In Other Words,* p. 138.

[136] Israel Export and International Cooperation Institute, "Israel: Security and HLS Industries," Tel-Aviv, 2007.

[137] Denes, Universalising the Unique, p. 32.

[138] See online at http://www.higtek.com. For more on RFID technology consult Steve Hodges and Duncan McFarlane, "RFID: The Concept and the Impact," in Barrier Stevens, ed., *The Security Economy*, Organization of Economic Co-Operation and Development, 2004.



[139] For Rotem see online at http://www.rotemi.co.il and for SDT see online http://www.scent-tech.com/index. Also the Industrial Cooperation Authority, "Defending Borders and Sensitive Infrastructure," Tel-Aviv, 2005. This brochure can also be accessed online at http://www.israexport.co.il/hls/art.asp?Id=203.

[140] For more information see online at http://www.biometric-center.com/index.asp.

[141] Wondernet recently changed its name to Penflow and can be accessed at http://www.penflow.com, while BioGuard can be accessed at http://www.bio-guard.net/index.aspx?lang=1.

[142] For information about OTI see online at http://www.otiglobal.com and about Vuance see http://www.supercom-inc.com. Also interesting is the brochure put out by Industrial Cooperation Authority, "Defending Borders and Sensitive Infrastructure," Tel-Aviv, 2005. This brochure can also be accessed online at http://www.israexport.co.il/hls/art.asp?Id=203.

[143] This data is interfaced with over 20 existing databases, including ADIS that stores travelers entry and exit data; SEVIS containing data on all foreign and exchange students in the US; IBIS, a "lookout" watch list interfaced with Interpol and national crime data; CLAIMS3, holding information on foreign nationals claiming benefits. See Louise Amoore, "Biometric Borders: Governing Mobilities in the War on Terror," *Political Geography*, 25, 2006: 336-351.

[144] Amoore, "Biometric Borders: Governing Mobilities in the War on Terror," p. 338. Amoore also cogently maintains that the allure of biometric derives from the human body being seen as an indisputable anchor to which data can be safely secured. The intertwinement of individual physical characteristics with information systems has served to deepen faith in data as a means of management and the body as a source of absolute identification (p. 341).

[145] See IDSST at http://www.idsst.com/idse/index.asp.

[146] See Controp at http://www.controp.com; Opgal Optronics at http://www.opgal.com; and also http://www.israexport.co.il/hls/art.asp?Id=203.

[147] See Orad Group at http://www.orad.cc. Interview with deputy CEO Yossi Gofer, May 1, 2008.

[148] Industrial Cooperation Authority, "Transforming Night into Day ," Tel-Aviv, 2005. This brochure can also be accessed online at http://www.israexport.co.il/hls/art.asp?Id=207.

[149] See Elop at http://www.el-op.com/default.asp. Other the companies that are leaders in this field are Electro-Optics Industries and Ortek, two subsidiaries of Elbit Systems, International Technologies Lasers Ltd. (ITL), Rafael Armament Development Authority and its subsidiary Opgal, and ISORAD, the commercial arm of the Soreq Nuclear Research Center.

[150] Industrial Cooperation Authority, "IT Solutions Enhance Safety and Security," Tel-Aviv, 2005. This brochure can also be accessed online at http://www.israexport.co.il/hls/art.asp?Id=201.

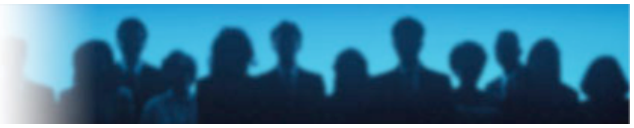
[151] See Verint at http://verint.com/corporate/home.cfm.

[152] See Top Image Systems online at http://www.topimagesystems.com.

[153] See Synel Industries at http://www.synel.com/about.

[154] See Ectel at http://www.ectel.com/default.aspx and Aladdin at http://www.aladdin.com. The latter was recently hired by MedStart Health, a $2.7 billion non-profit, community-based healthcare organization to deploy a strong authentication device that will provide powerful security for doctors and nurses remotely accessing vital hospital applications.

[155] Industrial Cooperation Authority, "Defending Borders and Sensitive Infrastructure," Tel-Aviv, 2005. This brochure can also be accessed online at http://www.israexport.co.il/hls/art.asp?Id=203.



[156] Industrial Cooperation Authority, "IT Solutions Enhance Safety and Security," Tel-Aviv, 2005. This brochure can also be accessed online at http://www.israexport.co.il/hls/art.asp?Id=201.

[157] See online http://www.dmatek.com/ and http://www.elmotech.com/.

[158] See online at http://www.ptm.com/default.asp.

[159] See online at http://www.dmatek.com.

[160] François Ewald, "Insurance and Risk" in Burchell, Graham, Colin Gordon, and Peter Miller, eds., *The Foucault Effect: Studies in Governmentality* (London: Harvester Wheatsheaf, 1991): 197–210.

[161] François Ewald, "Insurance and Risk."

[162] The Israeli Defense, Aerospace and Security Industries, "The Battlefield is a Hotel Lobby," Newsletter # 4 online at http://www.tradingmarkets.com/.site/news/Stock%20News/930927/.

[163] Joan W. Scott, "The Evidence of Experience," *Critical Inquiry*, Vol. 17, No. 4 (Summer, 1991): 773-797.

[164] F. Chesnais cited in Daniel Vekstein and Abraham Mehrez, "Technology Policy and Defense Conversion in Israel, 1967-1995," *Journal of Technology Transfer*, Vol. 22 (1), 1997: 50.

[165] Breznitz, "Collaborative Public Space in a National Innovation System."

[166] Interview with Rami Bar Eyal, February 28, 2008. The CEO of O.D.F. Optronics, which manufactures innovative vision-based systems for military, homeland security and consumer electronics markets, claims that the industry's success is dependent on the ability to predict future needs, while this ability develops through experience. He adds that though his different positions in the Israeli military, the last of which was the deputy chief scientist, he attained this kind of experience. Interview with Ehud Gal, November 27, 2008.

[167] Interview with Guy Zuri, November 29, 2008.

[168] Interview with Guy Zuri, November 29, 2008.

[169] Interview with Yossi Pinkas February 11, 2008.

[170] Interview with Yossi Goffer, May 1, 2008.

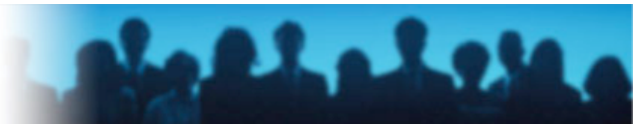
[171] *Looking Forward*, The Orad Quarterly, Issue 26, Autumn 2006, p. 4.

[172] *Looking Forward*, The Orad Quarterly, Issue 26, Autumn 2006, p. 4.

[173] Interview with Yossi Goffer, May 1, 2008. In 2002, Israel began building the separation barrier, which, according to the International Court of Justice, is illegal because it is being built on occupied Palestinian territory and is infringing basic Palestinian rights, from the right to livelihood and movement to the right to education and health care. See Neve Gordon, "The Barrier," in Cheryl Rubenberg, *Encyclopedia of the Israeli-Palestinian Conflict,* Lynne Reinner Publishers, 2009.

[174] See Magal at http://www.magal-ssl.com/profile/.

[175] See Schwartz, "Prosperity without Peace." See "U.S. Nuclear Weapons Being 'Guarded' by Israel," September 26, 2007. On the web at http://www.kavkazcenter.com/eng/.



[176] The act of testing the product and the experience in the field are represented in two distinct frames for methodological reasons, but in many ways are one and the same.

[177] Marx, Karl. 1992. *Capital: Volume 1: A Critique of Political Economy*, New York: Penguin Classic.

[178] Marx, *Capital: Volume 1*.

[179] Marx, *Capital: Volume 1*.

[180] Michel Foucault, *Remarks on Marx: Conversations with Duccio Trombadori*, Translated R. James Goldstein and James Cascaito, New York: Semiotext(E), 1991, p. 36.

[181] This relates to the whole claim about Israel being a laboratory (Klein 2008) – a site where experiments are carried out intentionally in order to discover something unknown, to test a hypothesis, or establish or illustrate some known truth by putting to the test – for homeland security products. We now see that the laboratory is not necessarily limited to the bottom frames in the Figure, but also to the top one.

[182] Foucault, *Remarks on Marx*, p. 27.

[183] Foucault, *Remarks on Marx*, p. 40.

[184] See Uri Ben-Eliezer, *The Making of Israeli Militarism* (Bloomington and Indianapolis: Indiana University Press, 1998); Yagil Levy, *Israel's Materialist Militarism* (Madison, MD: Rowman & Littlefield/ Lexington Books, 2007). Baruch Kimmerling, "Patterns of Militarism in Israel," *European Journal of Sociology*, 2, pp. 1993, 1-28.