HAARETZ.com

Revealed: Israel's cyber-spy industry helps world dictators hunt dissidents and gays

Haaretz investigation spanning 100 sources in 15 countries reveals Israel has become a leading exporter of tools for spying on civilians. Dictators around the world – even in countries with no formal ties to Israel – use them eavesdrop on human rights activists, monitor emails, hack into apps and record conversations

Hagar Shezaf, Jonathan Jacobson | Oct. 19, 2018 | 1:33 PM | 5

During the summer of 2016, Santiago Aguirre divided his time between part-time university lecturing and working for an organization that helps locate missing people. Mexico was then in the news internationally because of presidential candidate Donald Trump’s promise to build a wall on the American border with its southern neighbor. However, for Aguirre, a Mexican human rights activist, the problems of the present were far more pressing than any future wall. At the time, he was in the midst of a lengthy investigation to solve the mystery of the disappearance and presumed murder of 43 students in the city of Iguala two years before. It was becoming increasingly clear that his findings were incompatible with the results of the investigation conducted by the government.

Aguirre wasn’t concerned when he received a series of text messages containing broken links. “Please help me with my brother, the police took him only because he is a teacher,” one message read. And another: “Professor, I encountered a problem. I am sending back my thesis, which is based on your dissertation, so that you can give me your comments.” The messages looked no different from many of the legitimate messages he received every day as part of his work. And therein lay the secret of their power. When Aguirre clicked on the links, however, he was inadvertently turning his smartphone into a surveillance device in the hands of the government.

“Those text messages had information that was personal,” Aguirre notes, “the kind of information that could make the message interesting for me so I would click. It wasn't until later that I actually thought – well, it is actually pretty weird that I received three messages with broken links."

The discovery had a brutally chilling effect on the work of his organization. For the first time, he says, speaking with Haaretz by phone, he really and truly feared that every step he took was being watched, and that perhaps his family too was under surveillance.

"Over the past 10 years, we have a figure of around 30,000 people who disappeared" in Mexico, Aguirre explains. "Many places in Mexico are controlled by organized crime. It has under its influence and power the authorities of some regions of the country, so they use the police to detain and then disappear people that they think are the enemy. I can tell you of many examples in which the Mexican military, for example, has presented the work human rights defenders as [benefiting] the drug cartels and organized crime. So there's a pattern of thinking about the human rights sector in Mexico as a sector that needs to be surveilled."

The public revelation of the fact that Aguirre was under surveillance was made possible by cooperation between Mexican organizations and the Canadian research institute Citizen Lab. It turned out that Aguirre was one of a group of 22 journalists, lawyers, politicians, researchers and activists who were being tracked by local authorities. An examination of Aguirre's telephone revealed that the links in the text messages were related to Pegasus spyware, which the authorities were using.

But how did Pegasus get to Mexico? The trail of the malware led to Herzliya Pituah, the prosperous Tel Aviv suburb that is one of the major hubs of Israel's high-tech industry. It's there, in a narrow stretch of land between Israel's coastal highway and the Mediterranean Sea, that NSO Group, the company that developed this Trojan-horse program, has its headquarters. Pegasus, which Forbes magazine called "the world's most invasive mobile spy kit" in 2016, allows almost unlimited monitoring, even commandeering, of cellphones: to discover the phone's location, eavesdrop on it, record nearby conversations, photograph those in the vicinity of the phone, read and write text messages and emails, download apps and penetrate apps already in the phone, and access photographs, clips, calendar reminders and the contacts list. And all in total secrecy.

Pegasus' invasive capability was rapidly transformed into dazzling economic success. In 2014, less than five years after entering the world from a space in a chicken coop in Bnei Zion, a moshav in the country's center, 70 percent of the company's holdings were purchased for $130 million. The buyer was Francisco Partners, one of the world's largest private equity firms, which specializes in high-tech investments. That deal followed Francisco Partners' earlier purchases of Israeli firms Ex Libris and Dmatek, According to Reuters, a year after the NSO takeover, Francisco Partners enjoyed a profit of $75 million.

But the big money of NSO is only a small part of the big picture. Within a few years, the Israeli espionage industry has become the spearhead of the global commerce in surveillance tools and communications interception. Today, every self-respecting governmental agency that has no respect for the privacy of its citizens, is equipped with spy capabilities created in Herzliya Pituah.

Supreme secrecy

The reports about Pegasus prompted Meretz MK Tamar Zandberg and human rights lawyer Itay Mack to go to court in 2016 with a request to suspend NSO's export permit. At the state's request, however, the deliberations were held in camera and a gag order was issued on the judgment. Supreme Court President Justice Esther Hayut summed up the matter by noting, "Our economy, as it happens, rests not a little on that export."

The Defense Ministry benefits from the news blackout. Supervision takes place far from the public eye – not even the Knesset's Foreign Affairs and Defense Committee is privy to basic details of the lion's share of Israel's defense exports. Contrary to the norms that exist in other democracies, the ministry refuses to disclose the list of countries to which military exports are prohibited, or the criteria and standards that underlie its decisions.

A comprehensive investigation carried out by Haaretz, based on about 100 sources in 15 countries, had as its aim lifting the veil of secrecy from commerce based on means of espionage. The findings show that Israeli industry have not hesitated to sell offensive capabilities to many countries that lack a strong democratic tradition, even when they have no way to ascertain whether the items sold were being used to violate the rights of civilians. The testimonies show that the Israeli equipment has been used to locate and detain human rights activists, persecute members of the LGBT community, silence citizens who were critical of their government and even to fabricate cases of heresy against Islam in Muslim countries that don't maintain formal relations with Israel. The Haaretz investigation also found that Israeli firms continued to sell espionage products even when it was revealed publicly that the equipment was used for malicious purposes.

Private Israeli companies, the investigation discovered, have sold espionage and intelligence-gathering software to Bahrain, Indonesia, Angola, Mozambique, the Dominican Republic, Azerbaijan, Swaziland, Botswana, Bangladesh, El Salvador, Panama and Nicaragua. In addition, the investigation corroborated earlier reports over the years about sales to Malaysia, Vietnam, Mexico, Uzbekistan, Kazakhstan, Ethiopia, South Sudan, Honduras, Trinidad and Tobago, Peru, Colombia, Uganda, Nigeria, Ecuador and United Arab Emirates.

The great majority of employees with whom we spoke declined to have their detailed testimonies appear in this investigative report, because of the draconian secrecy contracts they signed. Other personnel, who agreed to tell about their part in the industry, appear under false names. While some CEOs spoke to us, others preferred to toe the secrecy line and spout the usual response: Israeli systems help thwart terrorism and fight crime; the sales were authorized by the Defense Ministry; the exports are carried out lawfully.

And the truth is that all of the above claims are correct. The law does not prohibit the sale of surveillance and interception equipment to foreign governments and law-enforcement agencies, the exports are approved by the Defense Exports Control Agency (a unit in the Defense Ministry), and the items in question are used to thwart terrorism and crime. For example, systems of the Verint company assisted in the effort to stop abductions in Mozambique and in a campaign against poaching in Botswana. In Nigeria, Israeli systems assisted in the battle against the terrorist organization Boko Haram. However, senior officials in the Israeli firms admit that once the systems are sold, there is no way to prevent their abuse.

"I can't constrict my client's capabilities," says Roy, who is experienced in cyberware. "You can't sell someone a Mercedes and tell him not to drive faster than 100 kilometers an hour. The truth is that the Israeli companies don't know what use will be made of the systems they sell."

"It's hard to supervise," adds Yaniv (a pseudonym, like all the other names cited here), who is employed in the industry and served in the Israel Defense Forces' vaunted Unit 8200 in the Intelligence Corps. "Even when limitations are placed over the capabilities of the computer programs, the companies don't know who they will be used against. Everyone in this field knows that we are manufacturing systems that invade people's lives and violate their most basic rights. It's a weapon – like selling a pistol. The thing is that in this industry people think about the technological challenges, not about the implications. I want to believe that the Defense Ministry supervises exports in the right way."

However, even the supervisors in the ministry have no way of knowing who's being spied on with the Israeli products. Israelis who train the buyers in the use of the systems sometimes learn about the purposes for which they have been acquired. "I happened to see a super-wrong use of the systems," says Tomer, who has trained intelligence bodies all over the world. "I'm telling foreign trainees about the system's capabilities, and they pounce on it and start to place people under surveillance for negligible reasons, right before my eyes. Someone was critical of the president's move to raise prices, someone else shared a hashtag identified with the opposition – and in an instant they're both on the surveillance list."

Guy Mizrahi, co-founder of Cyberia, a cyber solutions company, divides the industry into two types of firms. "There are companies that know how to do only one thing, but really well," he notes, "while other companies have a range of products. Some of them control the databases of internet providers and cellular operators, some are capable of getting to the [targeted] device itself, by all kinds of means."

NSO, the developer of Pegasus, is probably the best-known example of the first category, which consists of one exceptional ability. Verint Systems, one of the multifaceted giants of the industry, is an example of the second type, with diverse products. Verint started as the intelligence unit of Comverse Technology, which was established by Jacob "Kobi" Alexander, an American-Israeli businessman who was recently released from prison in the wake of fraud charges brought against him by the U.S. Securities and Exchange Commission. Verint subsequently went its own way and is now headed by CEO Dan Bodner. The company has 5,200 employees in a number of countries, of whom 1,000 work at its Herzliya Pituah headquarters.

Though sources who worked with Verint products in Mozambique and

Botswana encountered only legitimate projects, instructors of agencies in Azerbaijan and Indonesia related that the firm's products were used maliciously. "I was an instructor in Azerbaijan. One day the trainees came over to me during a break," Tal recalls. "They wanted to know how to check sexual inclinations via Facebook. Afterward, when I read up on the subject, I discovered that they're known for persecuting the [gay] community there. Suddenly things were connected."

An example of what he meant is a 2017 report on the arrest and torture by Azeri police of 45 gay men and transgender women. That took place a few years after Verint's systems began being used in the country. Tal says he now regrets having worked there, adding that incidents of the Azerbaijan type hastened his decision to leave the profession.

Indonesia is no haven for the LGBT community, either: Same-sex relations are classified as a criminal offense there. Reports by human rights organizations have noted the tough policy against the community, as well as against religious minorities, under legislation that bans "blasphemy." Three sources who spoke to Haaretz talked about wrongful use of Verint products in Indonesia.

In one case, the systems were used to create a database of LGBT rights activists who had been targeted for surveillance. In another, the victims of the spyware were religious minorities. "As soon as I arrived in the country, the client told me that my help was needed with an investigation that was bogged down," Netanel, who worked with the Indonesians to activate the systems, relates. "Very quickly the investigation turned out to be a case against a non-Muslim public figure who was accused of heresy, an offense that carries the death penalty."

Leave no traces

Back to NSO. The Israeli cyber giant was founded in 2010 by three friends: Omri Lavie, Shalev Hulio and Niv Carmi (the latter left early on). Lavie and Hulio, who are today in their late 30s, knew each other from high school in Haifa. They embarked on their path in business a few years after Hulio completed his army service in a classified intelligence unit.

What is their business path? "We are a ghost," Lavie was once quoted as saying. "We are completely transparent to our goal and we leave no traces."

Some years later, the traces of the ghosts from Haifa could be detected in every corner of the world.

As befits ghosts, Lavie and Hulio are not prone to making public statements. In 2015, Hulio gave a rare interview to the podcast “Hashavua” (This Week). “From the outset, we thought of creating a system that would allow all the intelligence and law enforcement bodies to be in control of telephones remotely, or to extract information from them, with or without the user’s knowledge,” Hulio related. “We thought it would be simple, but it was extremely complex. That’s actually what NSO is doing to this day. We have iPhones and Androids, and everything is very secure, but in the end we see that everyone is listening to everyone,” he said, chuckling. “The phone goes with you everywhere. The amount of information about a person that can be extracted from his telephone is amazing, and there is no phone that is secure today.”

The most blatant case in which NSO apparently left traces is that of Ahmed Mansoor, a human rights activist from the United Arab Emirates. In August 2016, Mansoor received a text message on his iPhone, promising secret information about the use of torture in the country, if he clicked on an attached link. Behind the link, however, was Pegasus spyware, which was then identified by the organization Citizen Lab. Its exposure generated worldwide panic. Experts at the time suggested that it was the most sophisticated and comprehensive breach of Apple’s exacting security systems. Embarrassed, the corporation had to issue an urgent software update for all its clients’ devices.

Mansoor is currently serving a 10-year prison sentence for publishing posts critical of the regime on social networks. His story appears in two lawsuits that were filed against NSO and another firm, Circles Technologies, which was also founded by Israelis. One of the plaintiffs is the Mexican activist Santiago Aguirre, together with a Qatari citizen. Documents appended to the suit allege that NSO and Circles systems in the UAE kept tabs on 159 members of the Qatari royal family, senior government officials and various citizens of that country.

According to the suit, filed in August 2014 in Israel and Cyprus, Eric Banoun, an Israeli who was a senior executive at Circles, received an email from Ahmad Ali al-Habsi, an official of the UAE’s Supreme Council for National Security. The message noted that the council’s directorate would soon make a decision, apparently referring to the purchase of the company's products. In the meantime, he asked Banoun to demonstrate the company's capabilities, "even though I know that this is not included in our license," and is also prohibited under the rules of the [Israeli] Defense Ministry. In this connection, Circles was asked to intercept the conversations of the editor of the Al Arab newspaper, of Qatar, over a 48-hour period. And indeed, within two days al-Habsi received an email with recordings of the editor's conversations.

Ben, who serves as a consultant to surveillance firms in the Emirates, spoke with Haaretz from his residence in the Persian Gulf. Israeli companies are known in the region as suppliers of espionage equipment, he said. "Dubai [referring to the UAE] is a big client of surveillance technologies," he maintains, "and they know that the best technologies come from Israel." During the call he started to laugh nervously and remarked, "For sure the conversation now is being recorded." Voice calls via encrypted apps such as WhatsApp, Single and Telegram are blocked in the country, leaving only the monitored phone network.

The UAE is not alone. Earlier this month, Citizen Lab announced with "high confidence" that Pegasus spyware was used to track Omar Abdulaziz, a Saudi dissident living in Canada under political asylum. According to the organization's report, agents of the regime in Riyadh used NSO technology in Montreal against Abdulaziz. NSO did not deny the report.

Haaretz now adds another piece to the Israeli spyware puzzle in the Gulf. Our investigation reveals that Verint systems were sold to Bahrain, a small, undemocratic kingdom in the Gulf, where a Shi'ite majority is ruled by a Sunni royal house. During the Arab Spring, the rulers brutally suppressed demonstrations in the country with the aid of reinforcements brought in from Saudi Arabia. Last February, Nabeel Rajab, Bahrain's most prominent human rights activist, was sentenced to five years in prison in the wake of a series of tweets critical of the regime.

According to two sources who have been to Bahrain, Verint supplied the kingdom with systems that are typically used by monitoring centers, and with another system used for collecting information from social networks. One of the two sources, Arnon, related that Israelis travel to the country to train regime officials in the use of the systems or to carry out maintenance work. The Israelis arrive with foreign passports and are usually forbidden to move about in the country, he adds. The ban on free movement was a recurring theme in conversations with several sources who act as instructors in countries that want to play down the Israeli presence. In many cases, the Israelis are confined to their hotel room when they're not working.

"I have been to many countries," Arnon relates. "There were places where I trained soldiers and members of enforcement agencies, and places where we trained confidants – people who seem to be members of the ruler's extended family. In Bahrain all the members of the team were Indians, and alongside them were the personnel of Bahraini intelligence – including women, by the way. The truth is that I hated that country, because we were simply bored there. It's not scary, but we're not allowed to go anywhere. If I had to speculate on what use they make of the systems, I would guess that it has to do with anti-regime protest."

From Elbit to Ethiopia

Besides the Persian Gulf, Africa is also a flourishing arena for Israeli espionage equipment. Two sources who were involved in Verint projects confirmed to Haaretz that systems relating to communications interception were sold to Swaziland, which has gained the dubious distinction of being "the last absolutist monarchy in Africa." Our investigation found that Israeli companies sold espionage and intelligence capabilities to eight countries on the continent, as mentioned above. In addition to Swaziland, transactions were concluded with Angola, Mozambique, Ethiopia, South Sudan, Botswana, Nigeria and Uganda.

The most disturbing case is South Sudan, the young country founded in 2011. Two years after it gained independence, a vicious civil war erupted in the country, in which war crimes, including massacres and systematic rape were perpetrated by all the parties involved. As early as 2016 the United Nations stated that Israeli companies were selling equipment to South Sudan that was used for eavesdropping on opponents of the regime. Now, three sources confirmed that Verint supplied espionage means to the country, and two of them were able to say that the equipment was used in a monitoring center.

From the distance of time, Tomer, who used to train security personnel in use of surveillance systems, looks back at South Sudan and is overcome with disgust. "There were Israelis there from the moment they started to talk about the peace agreement that led to the country's establishment," he says.

“Two weeks after the signing we already started to talk about projects there. The spirit of things was ‘What fun, we have a new opportunity.’ It’s simply revolting.”

Abuse of Israeli-manufactured capabilities apparently occurred in Nigeria, too. A comprehensive report published in that country asserted that products of Circles Technologies were sold in 2012 to the governors of Delta and Bayelsa, states in the Nigerian federation. The investigation found that, ahead of the 2015 election, the governor of Bayelsa used the capabilities to monitor his chief rival and his wife and aides, and in one case to locate and arrest a well-known critic of the regime.

In 2013, it was revealed that the Israeli firm Elbit Systems had also been awarded a contract in the country, worth $40 million. At the time, Yehuda Vered, general manager of one of the company’s divisions, said the deal was for the supply of “systems for cyber analysis and protection.” But then came a report saying that, in addition to devices for “analysis and protection,” Elbit had supplied the Nigerians with an espionage program as well. In the wake of the revelation, the Nigerian National Assembly suspended the transaction pending the outcome of an investigation. However, it wasn’t long before the Israeli systems were installed in the headquarters of the National Intelligence Agency in Abuja.

Last December, Citizen Lab reported that the spyware PC 360 was used inside Ethiopia against dissidents living in the United States and Britain. The targets received an email supposedly leading to a link proving that the war between Ethiopia and Eritrea was expected to continue. In this connection, the recipients were asked to download an Adobe update, in which the malware was concealed. By this means, passwords, email exchanges and screenshots were stolen from them.

The investigation by Citizen Lab led to the servers of Cyberbit, formerly the intelligence division of Nice Systems, which was subsequently acquired by Elbit Systems. The laptops used by company personnel to illustrate the products’ capabilities helped the investigators of Citizen Lab trace their visits to potential clients in the Philippines, Thailand, Uzbekistan and Zambia.

To this day, no one in either Israel or Ethiopia has admitted that the deal was consummated, but two sources who were employed by Cyberbit confirmed to Haaretz that it was. The two, Gal and Roy, decided to leave the surveillance field because of moral qualms and the secrecy their work entailed.

“There’s a difference between selling to countries such as Germany or Denmark, and to clients from Ethiopia or Kazakhstan,” notes Gal. “That no longer suited my values. Whoever takes part in this industry knows what he is doing. There’s no way that technology of this sort will not be wrongfully abused – the only question is in what way. I don’t want to be part of that agonizing.”

Adds Gal, “Along with that, it’s a good industry. The army supplies very young but experienced talents, with specific knowledge. Why don’t we [Israelis] develop social networks like Snapchat, in which a message that’s sent immediately fades? Because we don’t have a relative advantage [in that]. The relative advantage there lies with an American college student, who knows that people send each other nude photos.”

And we’re good at extracting those nude photos from phones?

Gal: “Precisely! That’s the relative advantage. There are other industries like this – the drones, for example. The reason that the industry in Israel is flourishing so well is the ecosystem that was created here. It’s not that we’re so special.”

Scene of the crime

No few traces of Israeli activity can be found in Latin America, too. Documents uncovered by the AP news agency show that in 2015 Verint set up a military monitoring base in Peru, at a cost of $22 million. The system is capable of tracking satellite, wireless and landline communications of 5,000 targets, and of recording conversations of 300 individuals simultaneously.

The deal with Peru also included a product called SkyLock. The cover page of the commercial brochure for the surveillance system, which was leaked to The Washington Post, states: “Locate. Track. Manipulate.” The brochure goes on to describe in detail how the system can pinpoint the location of telephones throughout Peru, and in most other countries.

However, the deal was delayed due to unforeseen difficulties, when Peru’s chief intelligence agency became involved in an espionage scandal. The prime minister at the time, Ana Jara, had used the agency to place legislators, journalists and leading businesspeople under surveillance. Jara was forced to resign, but Verint apparently did not back out of the deal. According to a source who was involved in the details, personnel from the agency that got into trouble are now operating the system within the framework of the police force.

Another source who spoke to Haaretz confirms that Israeli firms are continuing to sell offensive cyber capabilities to Mexico as well, even after it became known that they were being used against civilians. “One of the things that always scared me in Mexico is that you never know whom you’re actually talking to, and who’s behind him,” the source says. “Everything there is utterly corrupt, but they are very careful not to reveal their purposes to the Israelis.”

Another example of a decision to go on doing business with those who abuse the surveillance capabilities is Colombia. In 2015, the British nonprofit Privacy International revealed that Verint and Nice had supplied the Bogota police with systems to intercept phone conversations, and that the technology was used to surveil opponents of the regime. A source involved in Verint’s deals in Latin America maintains that despite this, the company is continuing to sell its products in Colombia.

An instructor who trained local agencies in Latin America in the use of Verint systems, relates that he personally witnessed the abuse of the products. “There was one time that I was teaching people how to collect information from the social networks,” he recalls. “I’m working with the trainees and explaining things to them, when suddenly they ask me to run a check on [political] demonstrators. Just like that, in the middle of the training session.”

Rolling in billions

“Since the birth of communications, there have been attempts, and new means, of trying to intercept and decrypt these communications. Most recently, since the rise of the internet, this took on a whole new perspective, as more and more civilians have access to digital technology,” says Edin Omanovic, a Privacy International investigator whose field of expertise is espionage and intelligence means produced by private companies. “That, alongside the end of the Cold War and the beginning of the ‘war on terror,’ has led governments around the world to invest more and more capital in surveillance technologies […] Today's equipment enables mass surveillance over the internet and other means of electronic communications."

Privacy International has been publishing research studies about international trade in surveillance technology since 1995. A PI report issued two years ago noted the tremendous growth of the industry. Whereas in 2012 it encompassed 246 companies globally, by 2016 the number of firms had more than doubled, to 528. There are 27 Israeli firms on the list, making Israel the country with the highest per capita ratio of surveillance companies. Local and international data indicate that Israel accounts for between 10 and 20 percent of the global cyber market. In 2016, investments in Israeli startups in the industry accounted for 20 percent of the world total.

The dizzying success of the Israeli interception and surveillance industry is not a chance development that was generated by a spontaneous eruption of Jewish genius. When the high-tech bubble burst, in 2000, the Israeli economy went into a tailspin, which was countered by the intervention of Finance Minister Silvan Shalom and his successor, Benjamin Netanyahu. The government increased security expenditures by more than 10 percent and encouraged the local startup industry to enter the fields of security and surveillance.

The Israel Defense Forces, for its part, played the role of a business hothouse, as its technological intelligence units swelled and their graduates channeled the knowledge they'd acquired into a host of startups. The timing certainly played into the hands of the industry. After the attacks of September 11, 2001, countries around the world started to intensively acquire devices to monitor individuals suspected of terrorism or radicalization. The rich experience of recently discharged IDF soldiers met that need precisely.

Since then, the IDF and the local startup industry have continued to nourish each other. Only recently Haaretz reported that at the end of 2015, the army issued a call for bids for the establishment of a system to track targets on the net, which a year later was already being operated by an external firm. Concurrently, when the wave of stabbing attacks erupted, in 2015, the defense establishment made wide use of early-warning systems based in part on information gleaned from the social networks.

Another example is Fifth Dimension, a local firm that provides predictive systems for Israeli security agencies. These products join the ramified eavesdropping system that the IDF has employed for years against the Palestinians in the territories.

Indeed, a recently published study found that the 700 local cyber companies were established by a small group of 2,300 Israelis, 80 percent of whom belong to the exclusive club created in the IDF's intelligence units, notably Unit 8200.

If at the beginning of the last decade the government of Ariel Sharon sought to exploit the know-how of former intelligence-unit personnel, at the beginning of the current decade, the Netanyahu government was bent on exploiting the potential latent in academia. The reasons derive from security and economic aims alike. During the past year the internet information-security market had a turnover of $31 billion, and estimates project that within eight years the turnover will soar to $76 billion annually worldwide. Or, in Netanyahu's words, "Cyber is a serious threat and a very lucrative business."

After returning to power in 2009, Netanyahu set out to push the industry ahead. To that end, he called on Maj. Gen. (res.) Isaac Ben-Israel to draw up a multiyear plan. Prof. Ben-Israel now heads the Interdisciplinary Cyber Studies Center at Tel Aviv University. The national cyber program with whose development he was entrusted engendered four additional cyber research centers around the country. Ben-Israel believed that the focus should be on education and research. "Before this, it was impossible to take cyber studies in the universities, only computer sciences," he says. "There were no research institutes, the industry did not have a mechanism to encourage cyber development, and the defense system, which in Israel is a huge component in high-tech, wasn't connected to it in the least."

What about the exponential increase in the exports of Israeli-made espionage capabilities to every corner of the world? According to Ben-Israel, offensive cyber constitutes a small part of the industry, which is for the most part geared to defense.

But is it really a negligible component? Gil Reider, director of the homeland security and aerospace division of the Israel Export Institute, admits that it's difficult to gauge the proportion of the espionage capabilities within the overall cyber market.

“These days, everyone who served in 8200 comes out of the army with some cool idea, embarks on a career change, and before you know it there’s a startup and a new product,” Reider says, referring to the difficulty of quantifying the export volume, adding, “Governmental regulation in the cyber world is in its very early stages. Where the institute’s work is concerned, in order to track the export of a product, we are aided by organizations connected to customs duties and the business world. But it’s very difficult to measure the cyber market. After all, you don’t export a container of cyber the way you do a container of security equipment.”

Relocating abroad

The secrecy of the Defense Ministry, feeble regulations and the Export Institute’s monitoring difficulties all help the industry to move ahead and grow under the radar. We contacted the Central Bureau of Statistics, too, and were told, “It is not possible to provide information about security companies, and we are unable to distinguish between security exports and civilian exports.”

Attempts to track Israeli exports of espionage devices are also hampered by the fact that in many cases the systems are not actually exported from Israel. Many companies prefer to be registered abroad, or to operate physically overseas, for a variety of reasons: cheap labor, a beneficent taxation policy, greater secrecy, laxer governmental regulation and a desire to camouflage the systems’ Israeli origins, in order to penetrate markets in hostile countries.

NSO is an example of a particularly complex interlinking of companies. After its purchase by the American equity fund Francisco Partners, it was rebranded as Q Cyber Technologies and became the subsidiary of a company called OSY Technologies, which is registered in Luxembourg. From there the corporate babushka encompasses another pair of companies in Luxembourg, goes on to a firm in the British Virgin Islands and finally to the Cayman Islands.

Nevertheless, NSO’s center remains in Herzliya Pituah. Other companies have moved their center of activity abroad. “You will come across many firms that have research and development centers in Moldova and in Ukraine,” says Roy, an industry veteran. “As I understand it, the reason is, above all, cheap labor. To pay a Ukrainian or Moldovan $2,000 a month to investigate weaknesses in security mechanisms nonstop, is not a lot of money.”

Some of the cyber firms have remained in Israel but maintain subsidiaries or branches overseas. Two prominent countries on the Israeli cyber map are Cyprus and Bulgaria. The choice of those countries, says a particularly experienced source, derives from low costs, the fact that both are members of the European Union, and also because, despite the European cachet, they are still undeveloped in a way that ensures toothless regulation.

According to Cyberia's Guy Mizrahi, "Cyprus is definitely one of the preferred countries. Some countries are unwilling to work with Israeli companies and insist on working with a European firm, so you need an additional front to win bids. In most cases, when you want to sell in the EU, and very definitely in the Gulf states, you will need a non-Israeli front."

Avi Rosen is CEO of the Israeli cyber-defense firm Kaymera, and former vice president in charge of development at Cyota, the information security firm founded by Education Minister Naftali Bennett. Rosen: "When you sell in the Gulf, with a license of course, they prefer to see a Bulgarian, on top of which Israelis have a problem due to visa issues. One way or another, there are Israeli products in every country in the world, especially in the security market. It makes no difference whether they like us publicly in the media or not."

Cyber expert Yaniv notes another method for disguising the origin of espionage systems, one that is used by Israeli firms at home and abroad. "In many cases products have white names and black names," he says. "White names have no connection with the product. Pegasus, for example, is already saliently connected to the Israeli firm that developed the program, but you might also encounter software you know rebranded under names that you don't know. You can't know how items are presented abroad."

Circles Technologies is one of the leading companies operating out of Europe. It was founded in 2011 by Boaz Goldman and the intelligence expert Tal Dilian, who were later joined by Eric Banoun. "Circles," Guy Mizrahi explains, "created a product that uses the weakness of the cellular network to locate devices. You give me a phone number and I tell you which cellular cell it's currently connected to and approximately where it's located."

According to Ronen, a former employee of Sigmabit, an Elbit intelligence firm, systems like this intercept information that passes between devices as they are being transmitted. The physical mechanism is less complicated than one might think: The Circles system can be installed on drones, surveillance vehicles and even in a suitcase carried by an agent in the field.

“Our phones are engineered to connect with the strongest cellular cell in the area near them,” Kaymera’s Avi Rosen explains. “So I set up a mobile cell close to you, which looks and behaves as though it’s the desired cell, so that you will disconnect from the cellular network and connect to mine.” At the same time, the system will deceive the cell operator into thinking that it is the target’s device, and thus basically becomes a hub through which his incoming and outgoing communication flows.

Another type of system that’s widespread in the Israeli cyber industry focuses on collecting information from the social networks. These are non-invasive systems that are not under Defense Ministry supervision. The systems concentrate open-source information and analyze it in a way that enables conclusions to be drawn from big data and to assist the authorities. Our investigation found that Israeli firms sold systems of this kind to Angola and Malaysia.

But when all is said and done, the most sought-after espionage means is one that breaches the device. Yaniv: “What is a hack? It’s not the black screens you see in movies, where a hacker keys in something and, poof, he’s in another computer. It’s a programmer – or a researcher, in our parlance – who detects a bug, a kind of weakness, in software. It can be in an internet browser, a chat, email or a system in a particular device. When a weakness like that is detected, it’s possible to exploit it in order to change the system’s behavior. For example, I might detect a weakness in a chat program that will allow me to enter the computer of the person who’s talking to me and send his files to me.”

The big cyber firms employ researchers like Yaniv who spend their days looking for cracks in the code lines of cellular infrastructures, internet infrastructures, computers, telephones, operating systems, apps and software programs. “Naturally, the demand is for ‘exploits’ of weaknesses in very widespread platforms, such as Apple devices,” Yaniv observes.

Large firms, he adds, maintain a few weaknesses of these kinds on the shelf, ahead of the day when they will close the breach they are now using. “One of the advantages of NSO is that, according to reports, it has the ability to exploit weaknesses without sending a link to the target. That’s known as zero click. It's the best weakness, because I need zero interaction with you. It's something I send to your phone and, poof, I'm inside."

A case in point, Yaniv says, is the iPhone. "The phone is connected to Apple servers. An espionage program can impersonate an application you've downloaded to your phone that sends push notifications via Apple's servers. If the impersonating program sends a push notification and Apple doesn't know that a weakness was exploited and that it's not the app, it transmits the espionage program to the device. Still, that's rare. Generally you need human engineering, to search for ways to interest you on the social networks. With that information [about our target], I can use a fictitious character and make the target press on a link that's been sent."

How rare is it for a researcher to detect a weakness in one of the systems? According to Yaniv, detecting a weakness that no one is familiar with is valuable. "I once found a thing like that," he says. "It's a discovery that's worth millions of dollars."

Indeed, the prices of intelligence products can be astronomical. That's the background to the high salaries that are paid in the cyber world.

"When I was job hunting, I received an offer from one of the Israeli offensive cyber firms located in Cyprus," Yaniv relates. "They were talking wild amounts, like tens of thousands of dollars a month. A weakness researcher in Israel can make 50,000 shekels [$13,775] a month. I make 36,000. The Cyprus offer was almost four times as much. I passed it up, because I wanted to stay close to family and friends. The most generous offer I rejected was to teach cyber in Singapore. They offered absolutely crazy amounts – hundreds of thousands of shekels a month. You don't find salaries like this in any field until you come to offensive cyber."

Hacker and antivirus

"Everyone needs defense, everyone wants offense," says Avi Rosen from Kaymera. "It's a matter of timing, of long-term experience. This is a relatively young industry, and it takes time for these things to spread."

The demand for both defense and offense has led to a widespread phenomenon in the Israeli cyber industry: the sale of espionage capabilities alongside security products. The phenomenon can be likened to a group of hackers who develop malware and afterward sell the antivirus, or to physicians who spread epidemics and then sell the vaccination. Though in some fields this is prohibited practice, in the security world it's common and widely accepted.

"Today people want a comprehensive solution, not a product," says Roy, speaking from experience. "On the one hand, the clients are told, 'Come and see the offensive systems we have and you'll understand what we can do with them.' On the other hand, they sell the clients systems to defend against those very attacks."

The example of Kaymera, the cyber defense firm whose genesis lies in the offense-oriented NSO, isn't the only example of this duality. Still, there are probably not many experts who can testify to the phenomenon better than Rosen. Asked in the past about Kaymera's origins, he replied, "NSO started to sell its products, and suddenly a strong need for defensive tools emerged. Everyone who saw what NSO can do said, 'Hold on, this is an interesting story, but how do I protect myself against similar things?'"

Rosen relates that "NSO initially thought about how to create a product like this, because the need arose from the clients, but they quickly realized that it would need to be something separate. So they drew me in and we built this thing from scratch. We raised money and set up a separate company. I am not privy to what goes on in NSO."

Although NSO founders Lavie and Hulio don't invest in Kaymera, they are on its board of directors, as Rosen himself attests. Asked about the connection between the firms, he admits that indeed, "It's of great value. The proximity is important to us – thanks to it, we are exposed to all kinds of things in the offensive world."

"The argument that NSO's success nourishes Kaymera's success is correct and logical," said Guy Mizrahi, from Cyberia. "The truth is that defending and attacking call for very similar capabilities."

Kaymera is not the only example. Elbit, too, maintains an offensive cyber company that disseminates intrusive espionage means, and along with it a security company that provides cyber defense. Thus, within the same ecosystem that enjoys Israeli government patronage, a two-headed industry has sprung up: One wreaks havoc, the other provides immunization.

Supervising the supervisor

Attorney Itay Mack is devoting his life to uncovering information about Israel's security exports. Commerce in weapons is inherently not fully transparent, but according to Mack the level of secrecy in Israel and the absence of a public debate are exceptional. "In the United States relatively open discussions are held by Congress about decisions to arm all kinds of juntas and dictatorships," Mack notes. "There is nothing like that here."

According to Mack, "Documents in the State Archives show that from the very day of its establishment, Israel grasped the diplomatic clout of weapons as a means to forge alliances. You can see that in connection with countries on the Mideast periphery, such as Ethiopia and Turkey. The thing is that, under Netanyahu, security exports have become a cynical tool. You see many transactions that have no security-strategic value. We have moved from Ben-Gurion's 'alliance of the periphery' to Netanyahu's Micronesia alliance" – referring to security exports to small countries whose sole purpose is to gain votes for Israel at the United Nations."

Edin Omanovic, from Privacy International, doesn't rely on governmental supervision. "Every country can buy a certain technological tool and pass it on to some government agency. So every country that buys this equipment needs an end-user certificate, stating that the buyer won't pass it to somebody else and that they'll only use it for specific purposes, but enforcing that is really difficult. It's basically relying on their word. In Britain, public campaigns at least made them publicize the export permits."

Mack is concerned about the absence of supervision over the supervision. "How many people make the decisions about security exports? Very few," he says. "If you ask members of the Foreign Affairs and Defense Committee, they say that they have never discussed exports to specific countries [in their deliberations], only regulations. So who takes part in the discussions about specific exports? Personnel from the [Defense Ministry's] supervisory unit, a few other senior people, and in sensitive cases the decision is apparently simply made by Netanyahu."

A discussion that took place in June 2017 provides a clear example of the impotence of the Foreign Affairs and Defense Committee. The participants were the committee chairman, MK Avi Dichter (Likud), Foreign Ministry and Defense Ministry officials, representatives of the military industries, and a pair of guests, MKs Yehuda Glick (Likud) and Tamar Zandberg (Meretz). The subject was exemptions from marketing permits, which would benefit the cyber industry in particular. In 2016, 1,200 marketing and export permits were issued for 73 cyber products that are subject to supervision, though only 16 of them are in the classified category.

The following excerpt from the transcription of the deliberations exemplifies the Knesset's weakness in supervising the Defense Ministry:

Zandberg: "Is there a policy by which you transmit an opinion not to export because [the product] is used in crimes against civilians, but your recommendation is not accepted?"

Director of the department for export supervision in the Foreign Ministry, Eliaz Luf: "No, that can't happen."

Zandberg: "In other words, the Foreign Ministry of Israel authorized exports to Burma and South Sudan?"

Luf: "I can't answer that question."

Glick: "Why not?"

Zandberg: "I prefer to think that you recommended against [doing so], and perhaps the Defense Ministry gave the authorization due to other considerations."

Rachel Chen, director of the Defense Export Control Agency in the Defense Ministry: "I want to reply that even if the Foreign Ministry does not pass on a recommendation to the Defense Ministry, I will still not authorize products that are liable to harm human rights, period."

Glick: "But there is something here that we aren't able to understand. If at the moment and in practice these countries have weapons, does that mean that you authorized it?"

Chen: "I do not intend to give answers here about specific countries."

The rest of the meeting was unfruitful. Some months later, MK Zandberg told Haaretz that the most urgent issue for her was to uncover the list of countries to which Israel sells its security products. Data supplied to the Knesset's State

Control Committee in 2014 indicate that the list comprises 130 countries.

MK Glick also says that he was unable to get a copy of the list, despite his efforts. “In Israel, everything is placed under the security rubric and you automatically get an impenetrable protective barrier,” he says. “Instead of being a light unto the nations, the Jewish state is circulating weapons that are used in crimes against humanity, and it makes no difference whether it’s a rifle by the force of which a woman was raped by soldiers, or a digital system used for surveillance.”

Yaniv, the industry person who was of great help in the investigation, changed his tone in his last conversation with Haaretz. “Until last week I was certain that the Defense Exports Control Agency is doing its job properly, and I had no second thoughts about it,” he said. “After checking it out with colleagues, I discovered that supervision is awful. I had no idea that things were conducted like this, that there’s such a gap. I thought that they were in the guts of things, that they restrict usage and sales. It really jolted me.”

Tomer, the instructor for Verint products, mocks the supervision efforts and laughs when asked if there’s a protocol in the event that they encounter a violation of the terms of use. “Most of the people who worked with me in the company and carried out the training didn’t talk about this subject. It feels like guys who came back from a war. Everyone knows what it means to go to those countries, but no one says what they do when they see problematic things.”

Roy, who held key positions in Cyberbit and other companies, says that nothing surprises him any longer. He remembers reports revealing abuse of Israeli cyber products in countries of the former Soviet Union, but where the sales continued afterward as though nothing had happened. He himself served as an emissary in Uzbekistan and Turkmenistan, when it was already clear what use the authorities there were making of the systems. “To say that I relied on our clients?” he asks, and immediately answers, “I don’t trust anyone. That’s why I’m no longer in that field.”

Responses: ‘International standards’

From the Defense Ministry: “The Defense Exports Control Agency operates under the aegis of the Supervision Law to safeguard Israel’s strategic interests. The supervision is carried out according to [international] conventions and is applied in the light of international standards. The supervision policy is examined frequently in accordance with diverse considerations, including considerations of upholding human rights. The Foreign Ministry, which also attaches great importance to human rights, takes part in the decision-making process."

From NSO: "The company develops products that are sold solely to officially authorized government bodies, for the exclusive purpose of investigation and prevention of crime and terrorism, and all subject to the law. The company's products have helped save thousands of lives, including [by] the prevention of suicide attacks, the arrest and conviction of heads of drug cartels, the investigation of complicated crimes and the return of kidnapped children to their parents. The company's ethics committee is an independent body that includes external experts who have the power to annul contracts in case of improper usage.

"We investigate every allegation about improper use of the system, but in light of contractual restrictions we cannot refer to specific clients. A 2014 case that is being heard in a suit against us has nothing to do with the company. We do not operate the systems for the clients, but only develop the products. In the case of a contract violation, the company acts accordingly vis-à-vis its clients, including cancellation of contracts. Any attempt to present training as involvement in the system's operation is groundless."

Elbit: "The company operates according to the law and in accordance with the rules of the defense establishment."

Nice: "The company sold its security business a few years ago. Nice today has no activity, products or personnel dealing with these spheres."

Verint did not respond. Every attempt to get a response to findings about the firm went unanswered, as did a request to the company's CEO.

Circles Technologies also did not provide a response.

Contact the authors at surveillance@haaretz.co.il