Photo: Ohad Zwigenberg

How Israel Became a Hub for Surveillance Technology



Alex Kane

October 17 2016, 10:33 p.m.

Photo: Ohad Zwigenberg

In 1948, the year Israel was founded, the Mer Group was established as a metal workshop.

Today it's a much different company. It operates a dozen subsidiaries and employs 1,200 people in over 40 countries, selling wireless infrastructure, software for public transit ticketing systems, wastewater treatment, and more. But at the ISDEF Expo, an event held last June to show off Israeli technology to potential buyers from foreign security forces, the Mer Group's representatives were only promoting one thing: surveillance products sold by the company's security division.

The Mer Group's evolution from cutting metal to electronic snooping reflects a larger shift in the Israeli economy. Technology is one of the main sectors in Israeli industry. And Israeli firms with ties to intelligence, like the Mer Group, are using their expertise to market themselves internationally. The company's CEO, Nir Lempert, is a 22-year veteran of Unit 8200, the Israeli intelligence unit often compared to the National Security Agency, and is chairman of the unit's alumni association. The Mer Group's ties to Unit 8200 are hardly unique in Israel, where the cyber sector has become an integral aspect of the Israeli economy, exporting $6 billion worth of products and services in 2014.

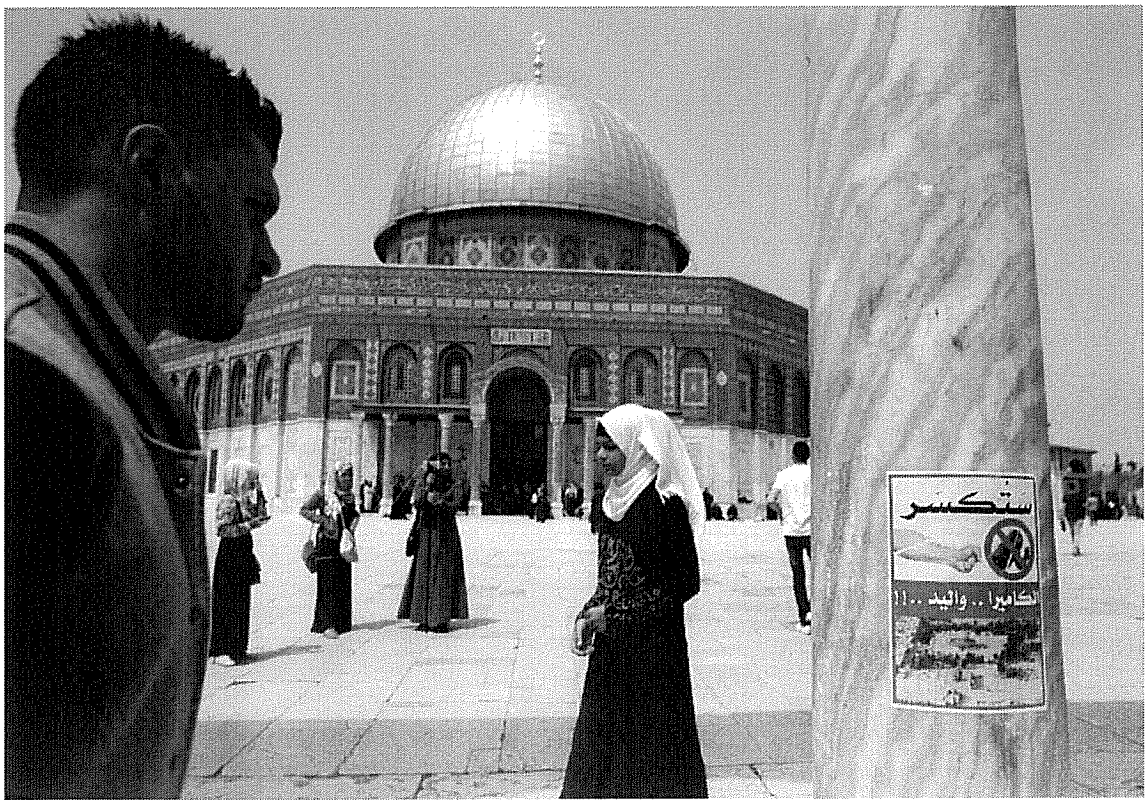
When drafted into the army, Israel's smartest youth are steered toward the intelligence unit and taught how to spy, hack, and create offensive cyberweapons. Unit 8200 and the National Security Agency reportedly developed the cyberweapon that attacked Iranian computers running the country's nuclear program, and Unit 8200 engages in mass surveillance in the occupied Palestinian territories, according to veterans of the military intelligence branch.

Increasingly, the skills developed by spying and waging cyberwarfare don't stay in the military. Unit 8200 is a feeder school to the private surveillance industry in Israel, the self-proclaimed "startup nation" — and the products those intelligence veterans create are sold to governments around the

world to spy on people. While the companies that Unit 8200 veterans run say their technologies are essential to keeping people safe, privacy advocates warn their products undermine civil liberties.

In August, Privacy International, a watchdog group that investigates government surveillance, released a report on the global surveillance industry. The group identified 27 Israeli surveillance companies — the highest number per capita of any country in the world. (The United States leads the world in sheer number of surveillance companies: 122.) Unit 8200 veterans either founded or occupy high-level positions in at least eight of the Israeli surveillance companies named by Privacy International, according to publicly available information. And that list doesn't include companies like Narus, which was founded by Israeli veterans of Unit 8200 but is now owned by Boeing, the American defense contractor. (Privacy International categorized Narus as an American company because it's headquartered in California.) Narus technology helped AT&T collect internet traffic and billions of emails and forward that information to the National Security Agency, according to reporting in Wired magazine and documents from the Snowden archive.

"It is alarming that surveillance capabilities developed in some of the world's most advanced spying agencies are being packaged and exported around the world for profit," said Edin Omanovic, a research officer at Privacy International. "The proliferation of such intrusive surveillance capabilities is extremely dangerous and poses a real and fundamental threat to human rights and democratization."



A poster calling for the destruction of CCTV cameras is posted on a column at the Al-Aqsa Mosque compound in Jerusalem in front of the Dome of the Rock, April 8, 2016.

Photo: Ahmad Gharabli/AFP/Getty Images

Today, Amit Meyer is a journalist, an unusual career path for a veteran of Unit 8200. Many of his colleagues have taken the skills in intelligence collection and hacking they learned in the military and

monetized them in the private sector. Unit 8200 is a "brand name" in Israel, a celebrated institution that allows members easy access to tech companies after their service, said Meyer. Sometimes technology companies approach alumni of the unit; other times alumni recommend one another. There's a secret Facebook group for alumni filled with job offers at tech companies, Meyer said. "In many cases you just put Unit 8200 in your CV, and magic happens," he told The Intercept.

Neve Gordon, an Israeli scholar who has studied the country's homeland security industry, explained that Israel's prominence in the surveillance industry stems from the close links between the Israel Defense Forces and the technology sector. In 1960, the Israeli military was developing computer software — nine years before the Israeli software industry and university computer science programs even existed. Israeli military units that work with computers, including Unit 8200, have become a "conveyor belt" toward Israel's military and homeland security industry, said Gordon.

Gordon said there are two other reasons why Israel plays such an outsize role in the global surveillance industry. One is that there are "hardly any" legal limits on veterans "taking certain research ideas they worked on in the military and developing them" in the private sector. In addition, said Gordon, Israel's decadeslong occupation of the West Bank, Gaza, and East Jerusalem, along with its periodic wars, "provides a laboratory for testing and fine tuning different commodities that are created, or different technologies."

Those technologies are then exported around the world.

Mer Security is one of the companies exporting spy products. It is well-known in the country's security circles; it won an Israeli police contract in 1999 to establish "Mabat 2000," which set up hundreds of cameras in Jerusalem's Old City, a flashpoint of tensions in the occupied area. In an interview with the Israel Gateway magazine, a trade publication, Haim Mer, chairman of the company's board and also a Unit 8200 veteran, explained that "the police needed a system in which 'Big Brother' would control and would allow for an overall view of events in the Old City area."

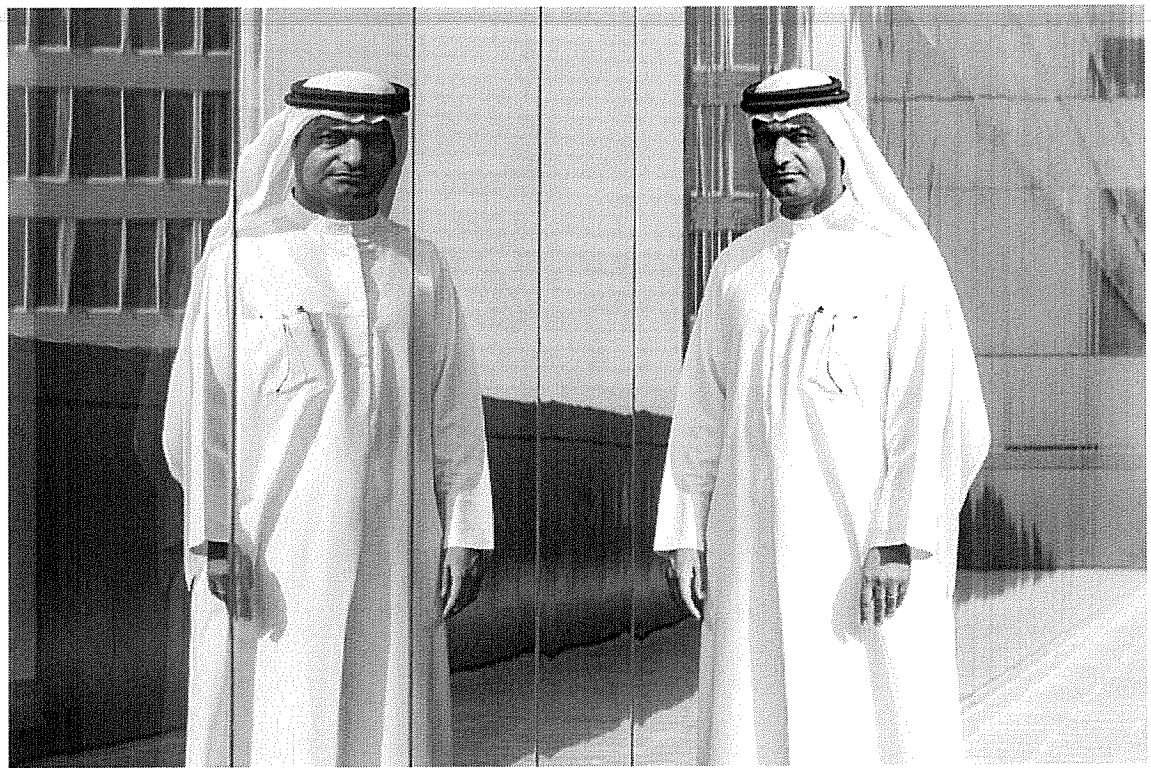
At the ISDEF Expo, Eyal Raz, the product director for Mer Security, told The Intercept about what "Israel's greatest security minds," as a company brochure puts it, have created. Raz was showcasing Open Source Collection Analysis and Response, known as OSCAR, which trawls through the internet and social media platforms and promises to uncover hidden connections from the data OSCAR collects and monitors.

Another product, called Strategic Actionable Intelligence Platform, or SAIP, takes that data in and groups it together. To pinpoint "actionable intelligence," SAIP uses technology that can highlight words, sentences, and information that might interest intelligence officers. These types of language analysis tools are increasingly popular with intelligence services around the world as a tool for pinpointing the next threat. These products claim to "understand what it's reading," as Raz said. For instance, a list of chemicals included in a paragraph may seem innocuous to the layperson, but the language analysis machine can recognize that the person is talking about making an explosive device, Raz said.

Raz explained another feature of SAIP: Users can create an avatar "in order to get the credentials to closed forums and to gather information from closed forums. This is also one way you can counterfeit your activities." Facebook does not allow people to create fake profiles, but the technology Raz and others are selling promises to blend into social networks so that profiles operated by law enforcement look authentic. Multiple news outlets this year have reported that the Israeli Police use similar tactics by creating fake Facebook profiles to befriend targets of investigations and monitor Palestinians. Though Israeli Police spokesperson Micky Rosenfeld was

quoted in one report as confirming the police use this tactic, he denied this claim when contacted by The Intercept.

Mer Group's clients are in Israel and abroad. The company does "joint development" work with Unit 8200, according to Raz, and they recruit veterans from the unit to work for the company. Other clients are scattered around the world, including in Europe, though Raz refused to divulge specifics. But publicly available information shows, for instance, that in 2011 Mer inked a $42 million contract with Buenos Aires to set up a "Safe City" system, complete with 1,200 surveillance cameras, including license plate recognition technology.



Ahmed Mansoor, a Dubai-based blogger and activist, poses for a portrait in Dubai, in the United Arab Emirates, on Sept. 25, 2012.

Photo: Bloomberg/Getty Images

Unit 8200's ties to the Israeli surveillance industry attracted widespread attention in late August, when digital security researchers at the University of Toronto-based Citizen Lab released a report detailing the provenance of a specific type of malware. They said it was likely that the United Arab Emirates had targeted Ahmed Mansoor, a prominent human rights activist, with sophisticated spyware that had the ability to turn his iPhone into a mobile surveillance device that could track his movement, record his phone calls, and control his phone camera and microphone.

Mansoor says he's been targeted since 2011, the year he signed a petition demanding democratic reforms in the Emirates. "The state security authorities are basically very obsessed with the monitoring and spying on people, activists," he said. "They are totally possessed with this kind of thinking."

Citizen Lab analyzed the spyware after Mansoor received a text message with a link promising "new secrets about torture of Emiratis in state prison." Rather than clicking, Mansoor sent the texts to the

digital security group, which had also, in 2012, analyzed spyware created by Italian surveillance company Hacking Team that had infected Mansoor's computer.

"We've never seen any exploits like this for a mobile device which operates on the very latest version," said Bill Marczak, a senior research fellow at Citizen Lab who co-authored the report.

The culprit behind the spyware, Citizen Lab's report concluded, was the NSO Group, a secretive Israeli surveillance company.

Details about the NSO Group are hard to come by. Their founders rarely talk to the press. They have no website. Israeli and foreign news media have reported that Omri Lavie and Shalev Hulio, the founders of the company, are veterans of Unit 8200. However, some Israeli outlets have reported that they served in other units. Still, at least three of NSO Group's current employees served in the intelligence unit, according to their LinkedIn pages. And Unit 8200 veterans provided the company with $1.6 million in seed money to develop Pegasus, the name for the spyware, according to Defense News, a trade publication.

Zamir Dahbash, the spokesperson for the company, did not answer specific questions about the NSO Group, which was bought in 2014 for $120 million by a U.S. private equity fund. He told The Intercept in a statement that "the company sells only to authorized governmental agencies, and fully complies with strict export control laws and regulations. ... The agreements signed with the company's customers require that the company's products only be used in a lawful manner."

On its face, an Israeli surveillance company selling spyware to an Arab nation is striking. The United Arab Emirates and Israel do not have official diplomatic relations, and like in other parts of the Arab world, many Emiratis detest Israel's decadeslong occupation of Arab lands. But NSO Group's sale to the UAE is an indication of the growing ties between Israel and the Gulf state, which has a growing appetite for surveillance gear.

"These regimes are unstable in the sense that most of the people living in these regimes do not have basic rights," said Gordon, the Israeli scholar, "and they constantly need to monitor and surveil their populations."

In February 2015, the Middle East Eye writer Rori Donaghy reported that the UAE had signed a contract with Asia Global Technologies, a Swiss-registered company owned by an Israeli and reportedly staffed by former Israeli intelligence agents, to set up a surveillance system featuring thousands of cameras.

Donaghy, who is also the founder of the Emirates Centre for Human Rights, said the UAE has quietly bought hundreds of millions of dollars worth of security products from Israel in recent years. The UAE turns to Israel, he said, because it believes Israelis are "simply the best in this market, the most intrusive, the most secretive."

Top photo: People observe surveillance cameras on screens inside the Jerusalem Police's Mabat 2000 unit on Nov. 17, 2015, in Jerusalem.