Inside Israel's lucrative — and secretive — cybersurveillance industry

By Michelle Anindya ⋮ 25-32 minutes ⋮ 3/9/2021

At age 18, K., like almost all Israelis, began his mandatory army service. "This was my way to give back to society and defend my country," he says. "I was one of them. I was one of the radical ones." From violent policing in the occupied West Bank to obscure, mundane office work, assignments in the Israeli Defense Forces vary wildly. K. remembers thinking, "Whatever job I'm given, I'll do it."

He also knew: "My head is stronger than my body. So, I thought, intelligence."

After his initial assessment, K. was offered a chance to enter Unit 8200, an elite intelligence unit in the IDF. (K. spoke to *Rest of World* on condition of anonymity). Akin to the NSA, 8200 has attained an almost mythical cachet in the global tech industry. Graduates of 8200 go on to launch successful startups and land coveted jobs. Officially, an 8200 soldier's status is classified both during and after service. Publicly, 8200 graduates happily boast of their experience in cover letters. In the many industries that touch their work, Unit 8200 is a brand name.

Post-8200 success comes at a cost: conscription to the unit requires five years of IDF service for many members. (The standard conscription period is currently 24 months for women, around 32 months for men). As for the incentives — what a post-8200 life might mean — K. says, "Other people around me did think about it. How it opened up doors afterwards. It's there." But for eighteen-year-old K., "being successful later in life and earning money and having a family and a house and whatever" wasn't top of mind.

Most Popular

As K. recalls, the recruitment pitch directed toward him was more about the "caressing of ego." He was told: "You're the best. We chose you. You're one in a million. Most people can't handle this job. You're a genius." So he said yes.

K.'s family belongs to Israel's old-school elite, made up of the children and grandchildren of the country's founding generation. They are an economically privileged, majority Ashkenazi social class that, in years past, has made up a large percentage of IDF's elite combat units. Within modern-day Israel, where there is no strong left-wing opposition remaining, this class's political leanings are

classified as liberal. “They are Zionist, but they think of themselves as peaceful,” K. explains, “as longing for peace.”

As in everywhere else in the world, the privileges of this elite come with proscriptions. “It was clear that, for someone like me, there are routes in life,” K. says. One example: “You don’t go to the Border Police,” in the occupied territories, where IDF soldiers physically control Palestinians’ movements. “It’s not ‘our kind of people’ that do that kind of thing.”

But fulfilling your IDF service with honor is paramount to fulfilling your elite’s obligations. Serving in 8200, then, “is a way of achieving the goal, of being part of the one side but [without] doing the ugly stuff of the occupation.” For K., “intelligence was a moral choice.”

Many Israelis find ways to use their IDF skills in the private market. Israeli journalists often get their start at the IDF’s popular radio station, Galatz. For graduates of 8200, though, the post-army opportunities come in cybersurveillance.

A 2018 study cited by *Haaretz* estimated that 80% of the 2,300 people who founded Israel’s 700 cybersecurity companies had come through IDF intelligence. Private Israeli companies have sold surveillance technology to Malaysia, Botswana, Azerbaijan, Angola, Honduras, Peru, Nigeria, Ecuador, Mexico, Ethiopia, Kazakhstan, Trinidad and Tobago, Colombia, Uganda, and the United Arab Emirates. The industry’s collective sales are near $1 billion annually.

Israel’s cyberintelligence community is met with global prestige. But international human rights organizations and lone activists are pushing against the ease and secrecy with which homegrown companies export their cyberweaponry all around the world.

Meanwhile, a generation of brilliant young people is being funneled from a resource-rich government spy agency into an unchecked cyber-surveillance industry. Can anything stop this pipeline?

Within the Israeli cyberweapons industry, the totemic name is NSO Group. Its Pegasus technology can purportedly hack a phone without the target even clicking a link. It's been used to track dissidents, activists, and journalists from Mexico to Morocco. Most infamously, according to a 2018 lawsuit, the Saudi government is alleged to have used Pegasus to hack the phone of a friend of Jamal Khashoggi's in order to monitor the journalist before his murder.

Behind NSO Group, there are many more. Cellebrite offers services to reconstruct data deleted from devices. The company gained renown after it was suggested that they cracked the iPhone of the 2015 San Bernardino shooters for the FBI. NSO's sister company Circles sells the ability to locate a person's physical location using only their phone number. Candiru goes after servers; it's named after the Amazonian fish famed for "parasitizing the human urethra."

Many of these companies are marketed globally on the prestige of their *former Israeli intelligence* founders and employees. Some observers of the industry argue that these companies exaggerate the scope of their dark arts. Subsequent reporting indicated Cellebrite did not actually crack the iPhone in the San Bernardino case. More recently, Cellebrite had to walk back claims that it can hack the encrypted messaging app Signal. Said Signal of Cellebrite, in a dismissive statement, "They don't do live surveillance of any kind."

Similarly, K. says much of the work he did inside Unit 8200 is far from the sophisticated spyware that's so often trumpeted. "Most Israelis think that intelligence is pure and slick," he says. He came to see IDF intelligence as blunt, dirty work. "Old school things," he says. Like blackmailing gay Palestinians, he

explains. Or threatening to cut off medical care from people with health problems. Or threatening the families of people with health problems. But when it comes to criticism of 8200, K. is an anomaly among his peers. Many are more like Raphael Ouzan — true believers.

George Etheredge for Rest of World

Ouzan, stubbled, bespectacled, is a paragon of Israel's 8200-to-tech pipeline. He is foregrounded while we speak on Zoom, his lovely downtown Manhattan apartment behind him. His camera is so sharp that I'm ashamed of my own; his input audio is so crisp, it's as if he is whispering into my ear. He drinks a coffee out of a tiny clear glass cup. For dramatic pauses, he alternates between sips

and the hands-in-prayer-to-lips motion. He is polite, thoughtful, and at pains to not intimidate.

He grew up in France's Champagne region, obsessed with computers. He says, "It was an escape from my narrow world." As soon as he was physically able, he started tinkering with old junk desktops. He didn't have access to expensive "gadgets" or "peripherals." He had a dial-up connection and books on C++, which he was figuring out on his own. By 11, he was the neighborhood computer kid. He built websites for family friends from the synagogue. They'd pay him through his bar mitzvah cash gift registry.

He started dreaming bigger. His beautiful hometown felt bleak. "I was born in a place that was very small, very non-ambitious, very content," he says. "I had to move." He'd been to Israel on family vacations: "There was this energetic, creative chaos that felt really relevant. So I gave it a shot."

At 16, he left his family and his country and enrolled in a boarding school in Jerusalem. "In France, we were studying PowerPoint and Microsoft Office," he scoffs. "In Israel, we were studying robotics and computer science convergence." He started competing in contests; in 2006, he won the Israel-Intel Young Scientists Competition. "In Israel, everyone cares about tech. Everybody. I was super happy. Maybe I didn't know Hebrew so well. But I was doing computer stuff."

Startups in the U.S. picked up the French-Israeli whiz kid. Before he turned 17, he went to Boston to work for a communications company, eDial. It was there in Massachusetts, not Israel, where Ouzan first learned about tech work in the army: "There were a bunch of Israelis there, and I heard about this cool stuff you can do. In the tech unit, in the army."

The specifics of Ouzan's path are unique. But his precocity is common. In Israel, tech education can begin as early as middle school. Promising teenagers are then funneled into a variety of elite feeder programs before landing in 8200.

> "You get trained super hard. From morning to night. And everything is pragmatic. It's not theories. It's about going on missions."

Ouzan's initial IDF evaluation assigned him the "profile of a fighter," which should have meant a place in a combat unit. Leaning on his rarefied background, he pushed his way into 8200. First came basic training, which he found appealing in a funny kind of way. "It has nothing intellectual about it," he says with a smile. "Maybe you learn perspective." Then came the specialized intelligence course for 8200. The months-long course is intense and multifaceted.

The first day of that classified course, he says, everything changed. “I knew nothing about it, but I could tell I was sitting across from some of the smartest people I’ve ever met,” he says. You get trained super hard. From morning to night. And everything is pragmatic. It’s not theories. It’s about going on missions.” In pristine resolution, he looks, plaintively, to his side: “And at this point, that’s it — you’re no longer a kid.”

After the specialized course, Ouzan was hand-picked to build a small team within 8200. “I was 20, and I was given people that were older than me and had more education than me,” he says. “I could give it a brand name and give it a mission. And my life became amazing.” Like most graduates of 8200, Ouzan will not go into details on his actual work. He does allude that he didn’t do surveillance in the occupied Palestinian territories, which means his team within 8200 likely focused on perceived threats to Israel from abroad.

After his five years in 8200, Ouzan built a financial security app called BillGuard. Five years later, it was acquired for $30 million. Next, he created his own elite feeder program, which promises to train participants “in an intensive program inspired by the IDF’s 8200 Intelligence Unit” and provide “incredible placement opportunities in the top hi-tech companies in Israel.” Currently, he’s working on a new startup, A.Team, an invite-only tech-talent incubator. He says that, even during the pandemic, “it’s been growing like crazy.”

Throughout his ascendant career, Ouzan has relied heavily on his 8200 network. He hired 8200 graduates and worked with ex-8200 investors. Even his former banker in New York City was 8200. And the network spans decades — one of

Ouzan's board members at BillGuard was in the same 8200 building as he was, 20 years back.

Plus, 8200 has its own accelerator, 8200 for Startups by EISP, and an official alumni association. But Ouzan says, "The alumni network is so strong that it doesn't have to be formal. You can reach out to anyone from 8200, and they'll talk to you," or vouch for you or give you information on a potential employee. "Compare that to the Ivy League in the U.S.," he says. "I can ask about someone you went to college with. What you gonna tell me? That they're a good guy? Went to class on time? This network is absolutely global, very powerful, and likes to come together to do good."

When trying to explain the specifics of what made it so special to him, Ouzan points to the audacity of the unit. During that initial rigorous intelligence course, Ouzan would constantly stare at a poster on the wall. It read "*hakol efshari*" — "everything is possible."

"For the first five minutes, I found it cheesy," Ouzan says. Quickly, it became like a mantra. "You just do it. You don't ask questions. You don't ask, Why not? It's foolishness — it's foolishness that is integral. You can do anything, if you are foolish enough to believe."

When we speak in late 2020, Eitay Mack has just filed a petition to stop the shipment of Israeli-made Negev machine guns to São Paulo's military police. For years, the activist attorney fought the international export of traditional Israeli

weapons. But the last few years, he explains, have brought “a change in my perspective.”

These days an oppressive regime “doesn’t have to shoot protestors,” he says. “With Israeli technologies, they manage to prevent protests before they happen. The Israeli surveillance system is the new Uzi.”

To that end, increasingly, his petitions are focused on Israeli cyberweapons sales. Mack, dry and quiet, is a one-man shop: he investigates and discovers weapons sales, then files the legislation to stop them.

> “With Israeli technologies, they manage to prevent protests before they happen. The Israeli surveillance system is the new Uzi.”

All Israeli weapons exports have to be approved by Israel’s Ministry of Defense. But the details of the sales are classified. In an annual briefing, the Ministry reports only the total monetary amount of sales and the total number of countries sold to.

Israel has strict military censorship. That means it’s actually illegal for Mack, as an Israeli citizen, to obtain classified Israeli military information. Mack, then, does all his work based on information acquired from activists and open sources. “A lot of information is already online,” he explains, bemusedly. “These kinds of regimes are proud of gaining Israeli technology.”

In 2015, he discovered a sale to the Myanmar military after the head of the military posted photos of Myanmar soldiers with Israeli weapons on Facebook. (As of a February coup, Myanmar is again under military control.) He found a Ukrainian neo-Nazi group, the Azov Battalion, was using Israeli Tavor rifles via the group’s Instagram account. He learned Cellebrite was selling to the Venezeulan government by reading the internal magazine of an elite Venezeulean investigation unit.

Mack has also found evidence that Cellebrite has sold its technology to Indonesia, where LGBTQI communities have suffered arrests, and to Belarus, where free-election activists have endured crackdowns. In Hong Kong, Cellebrite tech was allegedly used to crack phones confiscated from pro-democracy activists, including Joshua Wong, who is serving a year-long jail sentence for his involvement in the protests. In Russia, Cellebrite has been used at least 26,000 times by Putin’s pet spy unit, the Investigative Committee, which has targeted opposition leader Alexey Navalny and hundreds of human-rights groups. Cellebrite is also selling briskly in the U.S. According to Gizmodo, eight school districts, including the 600,000-student-strong Los Angeles Unified School District, have bought Cellebrite tech to unlock student cell phones. One 8200 graduate who previously worked at Cellebrite told *Rest of World* that she found

her job through former army intelligence friends, a “community that 8200 creates.”

Through a spokesperson, Cellebrite declined to comment on specific sales, saying only “We do not sell to countries sanctioned by the U.S., EU, U.K., or Israeli governments. Furthermore, we carefully vet and verify that the end users of our solutions are registered with Cellebrite to ensure their compliance with our guidelines.”

In Mack’s view, the sale of cyberweapons is, first, a continuation of Israel’s decades of exports of traditional weapons: in the 1960s, to the military dictatorship in Brazil; in the 1990s, to the conflicts in Rwanda and the Balkans; in recent years, to the civil war in South Sudan.

It’s not just Israeli weaponry that moves around the world — it’s Israeli people too. DarkMatter is a private Abu Dhabi intelligence firm that, according to Reuters reporting, is widely believed to be a contractor for the UAE government. DarkMatter is also known for, according to Yedioth Ahronoth, recruiting 8200 graduates by offering massive $100,000-a-month contracts and foofy beachfront rentals on beautiful Cyprus beaches. A few years back, according to the *New York Times*, DarkMatter even managed to poach some 8200 graduates away from NSO Group.

After years of sending software and talent to the small but influential Gulf state, it’s no coincidence, says Mack, that the UAE and Israel reached a Trump-brokered normalization agreement in the summer of 2020.

In the Israeli cyberweapon sector, he argues, “the companies are implementing government policy.” Mack says Israeli companies are not truly private, like their European or American counterparts. “Israel has so much military sensitivity” that, in effect, many of these cyberweapon sales are “military agreements between governments.”

But when NSO is covered in international media, the role of the Ministry of Defense is rarely mentioned. “The policy of the Ministry of Defense is not to deny — it’s not to say anything,” Mack explains. “Everyone is talking about this private company. But it is working according to the policy of the Ministry of Defense.”

> Israel’s export sales are either about shoring up relationships or about destabilizing its enemies — or about anything else that can be seen as a net good for Israel’s place in the global order.

In response to questions from *Rest of World*, a spokesperson said that the Ministry of Defense "does not comment on the export licenses of specific companies or to specific countries."

Primarily, Mack sees cyber sales as tied to "the other problem of Israeli security": the cold war with Iran and its proxies across the Middle East. From this point of view, Israel's export sales are either about shoring up relationships or about destabilizing its enemies — or about anything else that can be seen as a net good for Israel's place in the global order. Israeli tech reporter Amitai Ziv has argued that "when Israel sells weapons to Morocco or to Saudi Arabia, it obtains diplomatic quiet and weakens international criticism of the occupation. Thus, one crime justifies another."

Mack is part of a loose, tiny, unofficial network of forces pushing against Israeli cyberweapon exports. That network includes Eli Yosef, a settler and activist who first made his name in the 1970s, protesting in support of the Prisoners of Zion, a group of Russian Jews unable to leave the Soviet Union for Israel. At a performance of Moscow's Bolshoi Ballet in his native London, he crashed the stage and let loose mice.

When we speak on the phone in late 2020, Yosef is indignant: "We believe, very much, in the sanctity of life!"

Yosef is, quite possibly, always indignant. A religious Jew who immigrated to Israel in 1975, Yosef still carries his native North London accent. He became an activist to fight for freedom for Jews. But in recent years, Yosef's focus has been Israel's arms sales. He holds hunger strikes in protests of sales. He has a small group of fellow protesters that he mobilizes through a WhatsApp group. "I'll be honest with you," he says. "It's not a big group."

His primary tactic remains public spectacle. As Yosef explains, "I go to different meetings of members of Parliament and get myself bashed up." Online, you can find footage of Yosef in action: while politicians speak, he stands and accuses them of facilitating the murder of children, until he's literally picked up and dragged, still screaming, out of the premises.

"Whether you're using conventional weapons or whether you're using cyber," Yosef says, "they're all part of the system. You start hunting down human rights activists, things can go much, much worse."

In 2018, Amnesty International discovered evidence that NSO Group's technology had been used in an attempt to monitor an Amnesty employee. (The employee's identity and location remain undisclosed.) For Amnesty's Israel office,

this was a clear opportunity for action; they filed a lawsuit asking the Ministry of Defense to revoke NSO Group's export license.

While the case was pending, Amnesty Israel employees attended a technology conference, Mind The Tech. There, they ran into Shalev Hulio, the CEO of NSO Group.

Hulio, who is actually not a graduate of 8200, has a peculiar backstory. He says that, in its original iteration, NSO Group was a service to help consumers purchase products they spotted on TV. Last year, an intelligence official suggested to national security reporter Ronen Bergman that the provenance of NSO Group's technology could be the state of Israel.

Hulio hung around the Amnesty reps, trying to charm them. Amnesty Israel spokesperson Gil Naveh says one of the Amnesty reps finally told Hulio, "Listen, you're a billionaire, and you think you're fighting criminals — but you're not Bruce Wayne. Get over it." Hulio laughed it off.

A few months later, the Tel Aviv District Court dismissed Amnesty Israel's case: they ruled that Amnesty had failed to prove a connection between NSO and the targeted Amnesty staffer. Under the green light of the Ministry of Defense, NSO Group was allowed to continue exporting internationally.

Israel's small anti-weapons coalition continues to push for new legislation that would prevent exports to governments with histories of human rights violations and create increased oversight of homegrown defense companies. But public support for their cause has limited support inside the country of 9 million. Most regular Israelis, says human rights activist and former Amnesty International employee Chen Bril Egri, have "literally zero tolerance for fights that we want to promote." If there is a general consensus from Israeli society toward the cyberweapons industry, it is perhaps one of puzzled respect.

One month after Jamal Khashoggi's murder in 2018, during an appearance at a Tel Aviv tech conference, Edward Snowden publicly accused NSO Group of helping the Saudis monitor Khashoggi before his death. That same week, a popular Israeli late talk show, "Good Evening with Guy Pines," ran a short, peculiar segment about the spyware firm.

By piecing together a few social media posts, the talk show had figured out that NSO Group had recently flown hundreds of its employees out for a secret company retreat at a luxury resort in Thailand. There were massages, poolside parties, NDAs, and exclusive performances from the singer Netta (she won Eurovision Song Contest 2018) and the mentalist Lior Suchard (he performed at Kanye West's 41st birthday).

In the segment, Pines and his co-host, Shalmor Shtruzman, talk about NSO Group with a smirking remove. At one point, Shtruzman says that NSO could "invade the privacy of every human being in the world." Adds Pines, sarcastically, "but on a beach in Thailand, who has the energy to deal with privacy?"

Yes, this is a strange business, they seem to be suggesting, *but what a lovely place to work.*

K. himself now works in the Israeli tech industry as a data analyst. "For sure, it has to do with my service," he says. "It opened up the possibility. The experience, the connections." It wasn't always the plan to build a career on the back of his 8200 experience. He studied humanities in university. He spent many years after 8200 not doing any kind of tech work at all. "Then you need to make a living. Now I'm back in the industry. It's a good job."

It wasn't until after his five years of 8200 service that K. made his decision to disavow his work. "It's rarely the case in the army," he says, that something happens "that is so immoral that you go out of the room and say, 'I cannot participate.' You don't really see it in its entirety. You don't really understand your actions. Because you're a cog in the machine." Instead, "it's a lot of little things that add up."

After his service, he toured the West Bank. He attended discussion groups with Palestinian activists. He spoke with Arab friends from his university. Eventually, he learned that some fellow 8200 graduates were thinking in the same way. A friend approached him about this idea that had been manifesting: this idea to write a public letter. That first time, that first conversation, he remembers thinking, "I'm not sure it's for the best." He thought maybe he could do more from the inside. It's a big thing, "to tear your connection to society." The impulse to "not be an outsider" is strong.

In 2014, K. and 42 other 8200 graduates released an open letter addressed to the chief of staff at the IDF, refusing on moral grounds to fulfill their IDF reserve duties. (K. spoke to *Rest of World* in a personal capacity, not as a representative of this larger group.)

When I mention the 2014 refusenik letter to Ouzan during another Zoom, he asks me to jog his memory. I explain the gist: a group of former 8200 soldiers contended that the unit's pervading surveillance of Palestinians has only exacerbated the conflict. "I don't know about that particular letter and that particular thing with Palestinians," he says. "I have no idea; it's not what I worked on. But there's one thing I believe: people have to be safe. Without [safety], we are doomed."

> In the tech industry, the brilliant young men and women who fight their way through the IDF's elite intelligence unit are as coveted as ever. Their brand is powerful.

When it was published in 2014, the refusenik letter created a media storm, with much of the coverage coming in the international press. But the fundamental reputation of 8200 was not affected. In the tech industry, the brilliant young men and women who fight their way through the IDF's elite intelligence unit are as coveted as ever. Their brand is powerful.

Eli Yosef is still an active reserve IDF paratrooper. His WhatsApp profile photo shows him pulling an Israeli flag up a flagpole, while in the fatigues of the IDF. He believes in the Jewish people's divine right to the land; he lives in one of the major West Bank settlements deemed illegal by international law. "I'm coming from the position that I love Israel," he says. "I love the people of Israel. I love the state of Israel. I am for Israel in everything. It shouldn't come over as if I'm some kind of leftist." Yosef yearns to believe in Israel's moral righteousness, in a justification for its pervasive militarization. But "something very bad is going on underneath the covers," he says, "in the dark!"

Years before it can ever possibly happen, Yosef worries the Israel tech talent pipeline will ensnare his little granddaughter. He says, "In 18 years time, when she's 22, 23 — after the army — her friends will get phone calls from different cyber and arms companies that offer them a lot of money to train people in these dictatorial countries. And the innocence of heart — they'll try to rob it from her by offering her a nice sum of money," he laments. "I don't want her ever to get approached in that way."