LRB

Vol. 43 No. 21 · 4 November 2021

On Pegasus

Edan Ring

With the Covid infection rate soaring in spring last year, Naftali Bennett – Israel's then defence minister, now its prime minister – came up with an original approach to the crisis. As an emergency measure, the domestic security service, Shin Bet, had already been tasked with reporting the movements of mobile phone users for the purposes of contact tracing, making Israel one of the most privacy-disregarding countries in the world when it came to the battle against coronavirus. But Bennett now sought to bypass the civil and medical authorities completely. A former elite commando officer turned tech startup millionaire before he went into politics, he felt the solution lay in Israel's lucrative tech frontrunners – in particular, a boutique cyber-hacking company from Herzliya called NSO.

The company had made its reputation with its Pegasus software, designed to infiltrate mobile phones. Pegasus has 'zero-click' capabilities, meaning you don't even need to press a button or follow a link for it to take over your device, at which point it can intercept text messages, track calls, retrieve passwords and access the microphone and camera. A few reports had been circulating about problematic uses of the software, but Bennett – who wasn't very concerned about privacy and civil rights – wanted NSO to be allowed to analyse the location data of every Israeli citizen, enabling it to predict the likelihood of future outbreaks and cut the chain of infection. This was the magic formula, not only for beating the pandemic, but for fast-tracking his own ascent just as corruption charges against Benjamin Netanyahu were looming.

Bennett's plan was rejected by a Knesset committee, but he did manage to use the pandemic to propel himself to the top of Israel's political system. After losing his government job after the March 2020 elections, he published a book, *How to Beat a Pandemic*, packed with analogies from the world of combat and terror. Israel's leading tabloid, *Yedioth Ahronoth*, printed an 'expert' column by NSO's CEO, Shalev Hulio, calling for 'more surveillance' in order to save lives. This way of thinking wasn't unpopular, and it helped secure Bennett the premiership this June. But, a month after taking office, NSO was the cause of his first diplomatic crisis.

He wasn't the only politician to exploit the opportunities presented by Israel's cyber weaponry. In August 2020 Netanyahu surprised everyone by signing the first of the Abraham Accords, normalising relations between Israel and a number of Arab states. Hawk though he had always been, he now sought to secure his hold on power yet again by presenting himself as the man who could bring peace to the Middle East. But the countries he reached agreements with – the UAE, Morocco, Sudan, Bahrain – had little interest in Israeli-Palestinian relations. One thing they had in common was that they were all customers of Israeli cyber-surveillance firms, including NSO. Later in the year Netanyahu flew out to meet Mohammed bin Salman, the de facto ruler of Saudi Arabia, another state with an NSO contract. Other leading clients included some of Netanyahu's friends and allies over recent years: India's Narendra Modi, Hungary's Viktor Orbán, Rwanda's

Paul Kagame and Azerbaijan's Ilham Aliyev. All of them are leaders of countries with a record of human rights abuses and restrictions on press freedom; all of their countries have been destinations for glad-handing visits by Netanyahu.

It later emerged that some of the signatories to the Abraham Accord started targeting domestic opposition using NSO software only days after Netanyahu had visited. Reports in the *New York Times* and *Haaretz* have suggested that Israeli officials not only 'permitted' the sale of NSO and other cyber weapons to authoritarian states that would put them to questionable uses but 'encouraged' it, using these backroom deals to buy the public support of countries which had been hostile to Israel. For politicians and leaders on both sides it was a win-win situation, for cyber companies it meant a fortune, but for journalists, activists and opposition groups it was very bad news.

On the morning of 19 July, NSO employees woke up to a new reality. The publicity-shy company – known mainly to Israeli intelligence officers looking for lucrative jobs in the private sector, or to journalists investigating cyber surveillance in Mexico or Saudi Arabia – was now a household name. NSO was suddenly at the epicentre of a spying scandal involving some of the world's most oppressive and corrupt regimes. The findings of the Pegasus Project, a long-term journalistic effort led by Amnesty International and the Paris-based organisation Forbidden Stories, appeared in seventeen major international media outlets – including the *Süddeutsche Zeitung*, *Le Monde*, the *Washington Post*, the *Guardian*, Mexico's *Proceso*, Lebanon's *Daraj* – and the hair-raising revelations went on for weeks.

What had undone NSO was a leaked list of 50,000 phone numbers said to have belonged to those targeted by NSO's clients. From Mexico through Morocco and Rwanda to Italy and Hungary, across the Gulf States to Saudi Arabia and all the way to India, Pegasus had been used to monitor, harass, silence and detain. Even family members of government critics had been subject to surveillance. In Mexico, the list included parents of the 43 disappeared students from Ayotzinapa. In Rwanda, the daughter of the jailed activist Paul Rusesabagina was tracked for months. In India, not just the aides but the friends of Modi's main rival, Rahul Gandhi, were on the list, along with Gandhi himself. The biggest shock came from Morocco, which was apparently responsible for installing Pegasus spyware on the phones of five French cabinet ministers and for seeking to target Emmanuel Macron.

A wave of international condemnation followed. Macron called Bennett demanding to know why Israel had approved the sale of NSO cyber tools to countries like Morocco. Ursula von der Leyen described Israel's actions as 'completely unacceptable' and a statement from a number of figures at the UNHCR, including three special rapporteurs, called for 'a global moratorium on the sale and transfer of surveillance technology'. In Israel itself, the Ministry of Defence announced that an inquiry would be launched, but the story didn't keep government officials awake at night. The defence minister, Benny Gantz, claimed that 'Israel gives cyber export licences only to governments and only for combating terror and crime', pretty much the line of NSO's own PR.

The truth is that none of the revelations came as a surprise to Israeli officials. A handful of tech journalists and others had been trying to write about NSO for the last five years – it had been suggested, for instance, that the Saudi government used Pegasus to hunt down Jamal Khashoggi – but no one had shown much interest. Even now, Israel's courts have rejected the claim that the defence ministry was negligent in issuing export licences to NSO (the court also refused to release the details of those licences). Stories appeared in the press pointing out that 'many Israeli families make a living selling these technologies,' and that if Israeli companies didn't supply them then foreign companies would.

NSO has been preparing itself for this moment for some time. It hired expensive PR firms to manage its media campaigns and recruited establishment figures to sit on its board. Some of its senior executives had a background in IDF censorship and were well connected with the military bureaucracy. Only a few weeks before the findings of the Pegasus Project emerged, the company had issued a 'transparency and responsibility report' declaring its 'commitment to respect human rights' and claiming that there were more than 55 countries – it didn't give the names – it would not do business with. Its immediate response to the Pegasus allegations was to question the reliability of the leaked list of phone numbers, claiming it had no direct connection to its systems or its clients. The final line of defence was of course to attack: criticisms of the firm were 'anti-Israeli' and even 'antisemitic'.

But Pegasus is only the tip of the iceberg. NSO is one of a long list of companies to profit from Israel's booming cyber-spying industry. Others include Candiru, which sells spyware to UAE, Saudi Arabia, Uzbekistan and Qatar; Verint, whose software is reported to have been used in the persecution of LGBT and other activists in Indonesia, Azerbaijan and Nigeria; Cellebrite, which has helped the authorities in Botswana to break into journalists' phones and in Russia to harass opposition figures; and Elbit, which has supplied surveillance devices to Ethiopia and Nigeria. Many other companies work hard to keep their names under the radar.

Last year was a bonanza for the industry. Together, the firms raised $2.9 billion in funding through more than a hundred different deals, a 70 per cent rise from 2019. Five Israeli cyber startups reached 'unicorn' status for the first time in 2020, meaning that they achieved a valuation of $1 billion or more. In the first quarter of this year the industry raised a staggering $1.5 billion in funding, setting another record. Although Israel has a population of only nine million and comes 30th in the rankings by GDP, its cyber industry accounted for 31 per cent of global investments in the sector in 2020, second only to the United States.

This spectacular success is largely the result of the industry's connections to Unit 81, the IDF's elite special operations tech centre, described in *Israel Hayom* as 'developing unimaginable capabilities bordering on science fiction'. Veterans of Unit 81 have set up at least fifty private tech companies, which are together now worth around $10 billion, according to the financial newspaper *Calcalist*. 'It would not be an exaggeration to say that the unit's veterans have changed the face of the Israeli tech scene over the past decade,' the paper concluded, 'or at the very least determined the direction it is headed in.'

A peculiar mix of militarisation, patriotism and entrepreneurship has turned Israel – the 'startup nation' that once celebrated its innovations in agriculture and its mathematicians and engineers – into the world's leading exporter of cyber weaponry. It's not an entirely unfamiliar role: the Uzi submachine gun used to be a common sight in many African and Latin American countries, along with Israeli former generals continuing their careers by supplying training and expertise to foreign armies. But the events of recent years have given Israel the impetus to make technological advances as it seeks to find ways to prevent terror threats and missile launches without sending in troops and endangering lives. Gaza and the West Bank are living cyberlabs where new tools can be tested. With the rise of the internet, mobile phone networks and social media, every single move can be monitored and tracked. Old-style bugging devices and listening antennae are redundant now that military supercomputers are looking and listening to everything all the time, compiling data points, correlating activities and identifying faces. In a reality where there is no peace process in sight, the occupation and total control of an entire civilian population has come to seem vital, and vast amounts of money are being poured into perfecting the systems of surveillance.

The IDF is always on the lookout for the hottest young talent, and seeks budding engineers in high schools all over the country, investing in pre-army courses and special education plans. The lucky few who get recruited by the cyber units are rewarded with guaranteed admission to the tech industry and can look forward to a promising career instead of spending three years in the desert on tanks and jeeps or dealing with Palestinian civilians at checkpoints. And the private tech sector, in turn, doesn't have to look far for talent. In 2019 a cybersecurity firm called SentinelOne put up a billboard outside the Glilot army intelligence base with the slogan: 'We normally hunt attackers. NOW WE'RE HUNTING TALENTS.' There is ferocious competition for the best software engineers: a UAE-based company called Dark Matter is reported to have been offering ex-IDF programmers up to a million dollars a year. Dark Matter says its cyber products are intended for 'defensive' use only, but according to researchers at Macquarie University it works closely with UAE intelligence to target journalists and activists in rival countries. Sounds familiar.

This summer a story came to light that reveals something about the place that cultivates some of the best cyber surveillance developers in the world. The IDF censorship unit allowed the press to report news of a 25-year-old who had been found dead in a military prison, presumably after committing suicide. He had been jailed eight months earlier, found guilty of causing 'severe damage to national security'. No further details were provided, but an army spokesman said he had 'acted independently for personal motives and not for ideological, nationalist or economic motives' and had no connections to enemy agents. He was described by his friends and colleagues as a computer genius who got his BA in computer science and a job at a tech company before leaving high school. Even though psychological tests showed he had an 'immature' and sensitive character he was recruited to one of the IDF's elite tech units, where he served for more then five years.

Ronen Bergman, an intelligence reporter for the *New York Times* and *Yedioth Aharonot*, reported that a 'mixture of fury and revenge' against officials in the unit had made him break the rules. Aviv Kochavi, the IDF chief of staff, said 'he was about to compromise a big secret, and he was stopped at the last minute.' A report in *Haaretz* compared the affair to the Edward Snowden story, and included an interview with an officer who had a similar role in the same unit. Programmers have 'unlimited powers and capabilities', he said, but are given few 'rules or limits about the difference between right or wrong'. As for the young man: was this self-destruction, or did the system destroy him? Either way, this is the habitat that produces the great minds behind the some of the world's most sophisticated modern spying weapons. Now imagine how these cyber-geniuses feel when they leave the military and are bought up by the commercial sector. What do you get when you combine a mindset that places the highest value on patriotism with an industry that demands vast profits above all else? One answer is Pegasus.