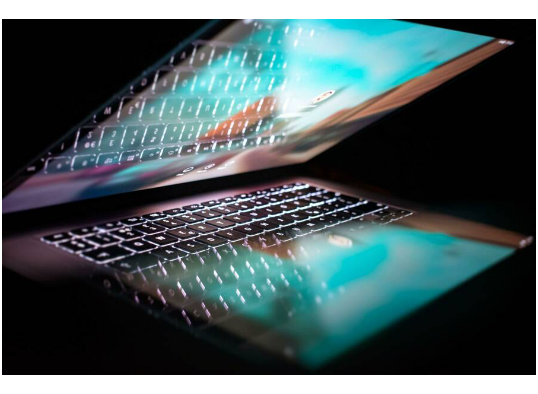
FEATURE

How Israeli Spyware Endangers Activists Across the Globe

Israeli surveillance technology is empowering antidemocratic governments to track journalists and human rights activists. Regulation is virtually nonexistent.

ANTONY LOEWENSTEIN JUNE 13, 2023



FEDERICO ORLANDI

The following is an excerpt from *The Palestine Laboratory: How Israel Exports the Technology of Occupation Around the World* (2023, Verso Books). It has been edited for length and clarity.

Griselda Triana is a Mexican journalist, and human rights activist whose husband, Javier Valdez Cárdenas, was slain by a drug cartel on May 15, 2017, in Culiacán, the capital of Sinaloa state. Valdez was the cofounder of the media outlet *Riodoce*, which investigated corruption and crime, and wrote about the bloody drug war. He paid the ultimate price—a grenade was thrown into his office in 2009. He had received death threats in the months before his murder, but he bravely continued his groundbreaking work despite the threats.

Ten days after his killing, Triana started receiving unexpected text messages on her mobile phone. She had no idea that they were suspicious until almost one year later, when it was discovered that there had been attempts to infiltrate her phone with the Pegasus system, a phone-hacking tool sold by Israeli surveillance company NSO Group, almost certainly by elements within the Mexican state. “Before Javier’s murder I did not know that we were being monitored,” she told me. Javier had never informed her about the possibility of phone hacking, and she presumed that he was taking precautions for his safety. “Javier knew about the risks of reporting criminal activities, but even so he was aware that someone had to document the atrocities of criminal organizations,” she said.

The murder of Valdez devastated Triana. “He was my husband and father of my two children. I was really shocked because Javier didn’t want to leave Sinaloa even though he knew they [the cartels] could kill him.” I asked her why she thought she had been targeted by Pegasus. She said she believed it was because “they thought that by tapping the phones they could get data from various sources of information or listen to calls related to Javier’s crime investigations.” To this day, Triana has never been told by the Mexican state why it spied on her—and there’s been no court case for the man accused of masterminding her husband’s death.

Both the Mexican government and NSO claim that Pegasus is used solely for the purposes of fighting crime and terrorism, but Triana’s case proves that this claim is false. Mexico has been a major testing ground for NSO technology. “The problem is that it has been used to spy on people who do not represent a danger to the country,” Triana said.

After Valdez’s death, Triana moved to Mexico City, where she works as a journalist and activist. The fear has never gone away, however—the feeling of being violated by both her husband’s gruesome death and the state’s intrusion on her communications. “I am afraid every time I visit Culiacán,” she said. “It is something that I have not been able to overcome.”

MAX DEROIN

Israel’s surveillance apparatus is a competitor and ally of Washington’s National Security Agency (NSA), the most powerful eavesdropping network in the world. While outmatched in terms of manpower, Israel has a long history of spying on its closest ally, a fact that does not appear to publicly bother the superpower. Some estimates suggest that around 350 American intelligence officials spend their days spying on Israel. Despite this, the NSA partners with Israel and has passed on data-mining and analytical software. In turn, says a former NSA intelligence official, Bill Binney, Israel transfers this technology to private Israeli companies, which allows them to gather a massive amount of sensitive military, diplomatic, and economic information to be shared with Israeli officials.

This is the frame around which to see the role of NSO Group, the world’s most successful cyber-surveillance company, and other Israeli high-tech outfits. NSO works with the Israeli state to further its foreign policy goals, and is used as an alluring carrot to attract potential new friends. Since its inception, NSO has been funded by a range of global players, including London-based equity firm Novalpina Capital. One of the biggest investors in Novalpina, to the tune of US$233 million in 2017, before NSO was on the company’s books, was the Oregon state employees’ pension fund. In 2019 pension money for the British gas provider Centrica was also invested in Novalpina.

Former *Haaretz* tech reporter Amitai Ziv, who has done some of the most insightful work uncovering NSO, told me that the power of NSO is not in the money that it makes but in diplomacy: “When Israel is selling cyber-surveillance to some African country, they can assure their vote at the United Nations. Since there’s an occupation, we need the votes.”

Whether NSO lives or dies, however, will make little difference to the burgeoning global industry in spying tools and cyber weapons. Entire countries can be brought to their knees, such as Russia’s cyberattack on Ukraine’s entire business and government infrastructure in 2017, or government and private companies inserting “zero-day” hacks, bugs for which there are no known fixes, into virtually every piece of hardware or software on the planet from computers to TVs to fridges. NSO is the tip of the iceberg of this surging industry, which largely operates in the shadows with no public scrutiny. It’s not just the American, Chinese, Russian, Israeli, or Iranian authorities unleashing cyber hell but a litany of private entities, sometimes built in democracies, that often act as proxies for state actors. Regulation is virtually nonexistent.

If NSO collapses, many others will rise to take its place and countless Israeli rivals are already in business. One company, Paragon, promotes similar services and is backed by former Israeli Prime Minister Ehud Barak and Unit 8200 veterans. Even if all private cyber-hacking firms are shut down globally, a highly unlikely proposition, far more powerful state actors, from Israel to the US and China to Britain, are more than willing to occupy the space. At least seventy-three nations have used spyware. NSO is just the most prominent spyware company, but large numbers of competitors are stepping in, making these tools even easier to obtain.

The role of Israeli surveillance globally is empowering antidemocratic and fascist governments, Israeli human rights lawyer Eitay Mack told me, and it’s not just targeting journalists and human rights activists. The Israeli defense sector is evolving and becoming far less public. “In the coming years, I do not see police in Bahrain using Israeli rifles or Israeli drones or missiles being bought by the United Arab Emirates because it could cause another Cuban missile crisis type situation and inflame Iran,” Mack said. “But selling Israeli surveillance equipment is much easier to do and not be detected.” He wants NSO spyware completely banned.

When Mack tried in 2016 to force the Israeli state to stop granting NSO an export license, the government succeeded in making all deliberations private. Supreme Court President Justice Esther Hayut was honest about what was at stake: “Our economy, as it happens, rests not a little on that export.” The Israeli Ministry of Defense admitted selling weapons to about 130 countries in 2021.

The trajectory of NSO is symptomatic of an Israeli tradition in testing, marketing, and proliferating surveillance technology across the globe. The reasons behind this were explained by the former head of Israel’s Defense Export Control Agency, Eli Pinko, who told a private conference in late 2021 that Israel had no choice but to sell weapons and cybertech to anyone who asked. “It’s either the civil rights in some country or Israel’s right to exist,” he said. “I would like to see each of you face this dilemma and say: ‘No, we will champion human rights in the other country.’ Gentlemen, it doesn’t work.”

But it is not just a question of free enterprise. A source with intimate knowledge of Israeli surveillance told me that Israel’s Ministry of Defense had “almost complete control” of NSO Group. “The MOD controls ownership and rights and has a veto on shareholders, owners and operators,” he said. “The tech, patent, and IP [intellectual property] is also controlled and technology has to be protected in a way that it can’t be reverse engineered.”

“I think that it is not well understood by American leaders,” said Eva Galperin, director of cybersecurity at the digital rights group Electronic Frontier Foundation, to journalist Ronan Farrow at the *New Yorker*. “They keep expecting that the Israeli government will crack down on NSO for this, whereas, in fact, they’re doing the Israeli government’s bidding.” The same willful blindness should be directed at much of the international media for its years of viewing NSO as just a rogue corporation, whereas it has always been a crucial tool of the Israeli state.

“The greater the violence and insecurity become, the greater the business opportunities for these companies.”

Mexico was an enthusiastic user of Pegasus, and by 2013 it was installed in at least three Mexican agencies with hardware and software worth US$15 million. During this time, NSO sold for US$77 million a package of services that allowed comprehensive surveillance of individuals whom Mexico under President Felipe Calderon wanted monitored. Calderon called NSO cofounder Shalev Hulio, though ended up speaking to his colleague, and said that “I couldn’t have asked for a better Christmas present. With what you gave us, we can finally eradicate the cartels.”

From a private Mexican company hacking a journalist, despite NSO claiming that it sold only to governments, to advocates of a soda tax that aimed to tackle the huge amount of sugary drinks consumed by Mexicans, it was increasingly clear that the kinds of people being monitored had no connection to crime or terrorism.

Over a decade, Mexico spent over US$160 million on Pegasus, but local authorities said that they could not identify who in the country was behind its use to prosecute anybody. Nonetheless, the profits of NSO’s private security business soared. “The greater the violence and insecurity become, the greater the business opportunities for these companies,” said Dr. Paloma Mendoza Cortes, a Mexican national security investigator, to Haaretz.

The scandals kept on coming in Mexico, where for years NSO had its most profitable work. Drug cartels colluded with corrupt Mexican officials to gain access to Pegasus and use it to eradicate mutual enemies. Criminal networks bribed corrupt officials to target individuals they want removed or monitored. Cybersurveillance is a completely unregulated industry, and despite NSO’s assurances there is no indication that Pegasus is monitored for breaches once installed. Since the 2010s, Mexico’s voting pattern at the United Nations has shifted to a less critical stance toward Israeli policies.

Unknown numbers of journalists, critical of state corruption, had their phones hacked by NSO spyware and ended up dead. They included freelance reporter Cecilio Pineda Birto in 2017. Just hours after hosting a Facebook Live video in which he accused local politicians and state police of working with a renegade thug, he was shot dead in the town of Ciudad Altamirano in southern Mexico. A few weeks before his killing, his mobile phone number had been selected as a possible target of Pegasus surveillance by the Mexican state.

This was just the tip of the iceberg of NSO’s potential victims, for between 2016 and 2017 leaked data (revealed in 2021) showed that over fifteen thousand Mexicans had been listed as potential targets of surveillance. At least fifty people connected to Mexico’s President Andrés Manuel López Obrador, including his close family, were placed on a list of phone numbers revealed by The Pegasus Project, a leak of fifty thousand numbers potentially used globally by NSO clients.

If Mexico was the first major NSO testbed, other states across the world soon followed. Pegasus was quickly purchased by often undemocratic clients, including the United Arab Emirates, Panama, Kenya, and Turkey, and reportedly assisted in the disclosure of terror cells, child abduction rings, and organized crime. Within a few years, NSO was celebrated across Israel, heralded by academic institutions and lavished with funds.

Research agency Forensic Architecture describes the role of NSO and cyber hacking actors as “digital infections” that do not “target civil society actors as individuals, but rather as networks of collaboration.” The group found that in India, Mexico, and Saudi Arabia, one person is initially hacked “before their professional networks are targeted within a similar time period. In each of these examples, the use of Pegasus occurs after or during periods where these civil society networks expose or confront controversial or criminal state policy.”

Pegasus was used by the Moroccan regime to target its critics, including outspoken opponents of the government who ended up in prison on bogus charges. Israel and Morocco normalized ties in late 2020, with the understanding that the US would recognize Morocco’s disputed control of Western Sahara. To sweeten the deal, Israel sold kamikaze drones to Morocco and in the past has sold a missile defense system. When Israel’s Defense Minister Benny Gantz visited Morocco in November 2021, there was no hiding that the two nations were principally interested in arms trading (with diplomatic relations further down the list). “Morocco is no chump in the cyber field,” Israel’s Foreign Minister Yair Lapid said in 2021, conveniently omitting to mention that it was Israeli technology that boosted Morocco’s cyberhacking abilities.

A full rogue’s gallery of dictatorships has bought and deployed Pegasus, nations that either had official relations with Israel or desperately wanted Israeli spyware. Bahraini and Omani activists have been targeted by NSO tech. Rwanda used Pegasus to monitor dissident Paul Rusesabagina, the man who inspired the Hotel Rwanda film, who was tricked and then kidnapped by Rwandan officials in Dubai, put on trial in Rwanda in 2021, and found guilty of terror-related crimes. Morocco used Pegasus to spy on senior French politicians including President Emmanuel Macron. Hungarian Prime Minister Viktor Orbán, a close ally of Netanyahu, bought Pegasus to spy on opposition politicians and critical journalists. When this was exposed in 2021, Orbán’s spokesman defaulted to his government’s usual anti-Semitic refrain when under attack, blaming billionaire Jewish philanthropist George Soros. This was the kind of ally that Israel wanted to foster in Europe.

I asked the NSO PR team questions about how and why it sells its products to undemocratic states and what safeguards are put into place to ensure that its products aren’t abused by the buyer. In response, NSO directed me to its “Transparency and Responsibility Report,” released in 2021. In it, NSO claimed that it had “rejected over US$300 million in sales opportunities as a result of its human rights review processes” and said that Israel’s Ministry of Defense “restricts the licensing of some of our products and it conducts its own analysis of potential customers from a human rights perspective.” The report further claimed that the company is “committed to respecting human rights” by the establishment of a Governance, Risk, and Compliance Committee (GRCC). The GRCC “reviews potential sales, providing recommendations and decisions after an in-depth, risk-based due diligence process including a comprehensive assessment of potential human rights impacts.”

SIGN UP FOR OUR WEEKEND NEWSLETTER
A weekly digest of our best coverage
EMAIL ADDRESS
SUBMIT

It is not only NSO that’s causing harm around the globe. Cellebrite is another Israeli company that works with repressive states and yet it has received far less criticism. It is hard to know exactly why it has escaped NSO’s notoriety, but perhaps it’s because Cellebrite prefers to operate under the radar with its phone hacking capabilities or because NSO’s alliance with despots has uniquely captured the attention of researchers and media outlets that often fail to make the necessary ties to the Israeli state. “Cellebrite sells equipment to hack phones from short distance and NSO Group from long distance, but the effect is the same for activists,” Israeli human rights lawyer Eitay Mack told me.

Founded in the 1990s, Cellebrite started out as a consumer technology firm but by the 2010s was deep into the surveillance business and mobile phone hacking because it saw the potential of huge profits from working with law enforcement officials around the world. In late 2021, Cellebrite launched a large scale PR campaign called “Heroes behind the Heroes,” featuring online ads and physical billboards that promoted the essential work being performed by their “digital intelligence solutions” in police forces around the globe.

Unsurprisingly, the PR blitz was selective about what services Cellebrite offered and who these advertisements were intended to influence. In 2022 Eitay Mack wrote to the company and Israel’s Defense Ministry to remind it where Cellebrite equipment had ended up, including Russia, where journalists are pursued, and the Philippines, where countless reporters have been murdered during the reign of President Rodrigo Duterte. Neither the Israeli government nor Cellebrite could claim ignorance of what might happen to sophisticated surveillance gear in the hands of autocrats. There is a published photograph of Cellebrite employees meeting Duterte in 2018 and admitting that the corporation had trained a range of public bodies, some of whom were directly complicit in the murder of thousands of Filipinos during Duterte’s brutal “war on drugs.” When challenged on its complicity, Cellebrite told Haaretz that it had “strict oversight mechanisms” over its sales. It was a statement that was remarkably similar to NSO’s when pushed on its international relations.

The countries where Cellebrite surveillance tech has been used against critics, journalists, dissidents, or human rights workers include Botswana, Vietnam, Bangladesh, and Uganda. This includes the Universal Forensic Extraction Device (UFED) hacking tool, which allows the extraction of information from mobile phones. In Bangladesh the hardware was used by the Rapid Action Battalion, a notorious paramilitary unit, which has been accused of extrajudicial killings and disappearances. When this connection was exposed in 2021, the company quickly announced that sales to Bangladesh were being suspended, though it was likely Bangladesh could still use the tech that had already been acquired. Furthermore, Cellebrite said it would establish an advisory committee to ensure that “ethical considerations” were prioritized moving forward. Once again, Cellebrite used the same PR-driven tactic employed by NSO. Bangladesh has no formal ties with the Israeli government, but this did not stop Israeli intelligence experts from training Bangladeshi officers during a four-day event on the outskirts of Budapest, Hungary, in 2019. The Ethiopian federal police use Cellebrite products despite the government’s mass detention of minorities and repression of dissidents, journalists and activists.

The disgraced Hollywood producer Harvey Weinstein wanted to hire the most effective private intelligence firm that money could buy to kill any media stories about his sexual assault on countless women. In 2016, he chose Israeli company Black Cube, founded in 2010 by former Israeli intelligence officers and the former head of Mossad, Meir Dagan. The company would get a US$300,000 bonus if a major story about Weinstein did not appear in the New York Times. Former Israeli Prime Minister Ehud Barak admitted introducing Weinstein to the Israeli firm. Nonetheless, Weinstein failed in his mission, and he’s now in a US prison for a string of rapes.

London-based spy, former journalist, stockbroker, and IDF soldier Seth Freedman admitted to working for Black Cube and investigating ninety-one people associated with Weinstein who had some connection to his sexual assaults. They included actress Rose McGowan, who Freedman tricked, along with many others, into an interview for a supposed story in the paper he used to write for, the Guardian. When asked by the BBC if he regretted his work, he said that “my job is to get a piece of information that isn’t freely available, and as long as I stay within the letter of the law, I’m not worried about your ethics when you judge me.”

How to stop these NSO-type companies in their tracks? It will take systematic, global change because the disappearance of NSO itself will not remove the demand for tools like Pegasus by democracies and dictatorships alike. David Kaye, the former United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression between 2014 and 2020, argues that “our attention shouldn’t be focused only on one company [NSO] because if we’re only focused on them then we might think that the solutions are just to restrain Israeli export control processes. Or we need to ensure that NSO alone abides by emerging standards for corporate, human rights responsibility. The problem is global.”

Kaye believes that an international code of conduct for cyber-surveillance firms is an important first step, though he acknowledges it would likely be nonbinding and thus making enforcement close to impossible. Government regulation was the better option, Kaye told me, because then companies would fear stepping out of line. He compared it to the 1997 Anti-Personnel Landmines Convention where most of the world, except the US, Israel, China, Pakistan, India, Egypt, and Russia, came together to outlaw the destructive weapons.

“You could imagine a process where some members of the international community want to ban this stuff [cyber weapons],” Kaye said. “My guess is that most governments would only be willing to regulate the export and use, because give me a reason why states would give up this ridiculously powerful tool?”

During his time as a UN Special Rapporteur, Kaye regularly called out NSO for its transgressions against human rights activists and journalists worldwide. At the end of his term in 2020 he acknowledged that global regulation was in its infancy. “Right now, it’s almost as if there are no shadows because there are no legal constraints,” he told the Committee to Protect Journalists.101 UN human rights experts, including Kaye’s UN successor, Irene Khan, issued a call in 2021 for states to “impose a global moratorium on the sale and transfer of surveillance technology until they have put in place robust regulations that guarantee its use in compliance with international human rights standards.”

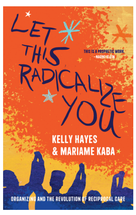
The challenges of regulating this out-of-control industry may be hard to overcome, since it is already so ubiquitous around the globe. But as Shoshana Zuboff, Harvard professor and author of The Age of Surveillance Capitalism, has said, this is the same feeling that many people had before unions started fighting for workers’ rights or the abolition of child labor. A simple, sensible suggestion is to ban all commercial tools in cyber-hacking. “Eliminating the profit motive reduces the risks of proliferation while protecting progress,” Edward Snowden argues, thus “leaving room for publicly minded research and inherently governmental work.”

Not doing so guarantees a proliferation of NSO-type tools where every person on the planet might have their mobile phone or digital devices vulnerable to exposure. But this is not enough. The purveyors of these tools, whether in Israel, the US, or Italy, must be held legally liable. A few major court victories against surveillance corporations could be morally clarifying for those in

the trade.

Hacking of mobile phones is just the beginning of what is possible in the complete surveillance of our lives. Bill Marczak, a senior research fellow at Citizen Lab, fears that the improved security of mobile devices in the future could "make it extremely difficult for NSO and others to target them. It may come to the point where it's not feasible. Maybe they'll hack smart cameras in homes instead, turning on microphones to listen in. Or fridges, toasters, and cars. There's no shortages of domains to surveil."

For a limited time:



Donate $20 or more to support *In These Times* and we'll send you a copy of Mariame Kaba's new book, *Let This Radicalize You*.

Longtime organizers and movement educators Mariame Kaba and Kelly Hayes examine the political lessons of the Covid-19 pandemic, and the convergence of mass protest and mass formations of mutual aid. Featuring insights from a spectrum of experienced organizers, including Sharon Lungo, Carlos Saavedra, Ejeris Dixon, Barbara Ransby, and Ruth Wilson Gilmore and more.

"Kelly Hayes and Mariame Kaba have created a visionary and urgently needed guide to cultivating hope and action in treacherous times." — L.A. Kauffman

GET YOUR COPY

ANTONY LOEWENSTEIN is an independent journalist, best-selling author, filmmaker and co-founder of Declassified Australia. He's written for *The Guardian*, *The New York Times*, *The New York Review of Books* and many others. His books include *Pills, Powder and Smoke*, *Disaster Capitalism* and *My Israel Question*. His documentary films include *Disaster Capitalism* and the Al Jazeera English films *West Africa's Opioid Crisis* and *Under the Cover of Covid*. He was based in East Jerusalem 2016-2020.

Have thoughts or reactions to this or any other piece that you'd like to share? Send us a note with the Letter to the Editor form.

SIMILAR ARTICLES

FEATURE

This Video Appears To Show Bernie Sanders Being Arrested at a 1963 Civil Rights Action in Chicago

It looks like there's proof of the presidential candidate participating in civil disobedience to end segregation

MILES KAMPF-LASSIN

FEATURE

Slavoj Zizek: The Need to Traverse the Fantasy

A call to mobilize Europe's radical-emancipatory tradition, and why we need a solidarity of struggles, not a "dialogue of cultures"

SLAVOJ ŽIŽEK

FEATURE

How Wall Street Is Cashing In on Climate Catastrophe

Come hell or high water, the finance industry will make a killing

KATE ARONOFF

SIGN UP FOR OUR WEEKEND NEWSLETTER

A weekly digest of our best coverage

your@emailaddress.com SUBMIT

GET 10 ISSUES FOR $19.95

Get the whole story: Subscribe to In These Times magazine.

SUBSCRIBE NOW

As a reader-supported 501(c)3 nonprofit, In These Times does not oppose or endorse candidates for political office.
COPYRIGHT © 2023 BY THE INSTITUTE FOR PUBLIC AFFAIRS (EIN: 94-2889692)