F.B.I. Secretly Bought Israeli Spyware and Explored Hacking U.S. Phones

Israel used the NSO Group's software as a tool of diplomacy. The F.B.I. wanted it for domestic surveillance. Then everything soured. Here are highlights of a New York Times Magazine investigation.

By Michael Levenson
Jan. 28, 2022

It is widely regarded as the world's most potent spyware, capable of reliably cracking the encrypted communications of iPhone and Android smartphones.

The software, Pegasus, made by an Israeli company, NSO Group, has been able to track terrorists and drug cartels. It has also been used against human rights activists, journalists and dissidents.

Now, an investigation published Friday by The New York Times Magazine has found that Israel, which controls the export of the spyware, just as it does the export of conventional weapons, has made Pegasus a key component of its national security strategy, using it to advance its interests around the world.

The yearlong investigation, by Ronen Bergman and Mark Mazzetti, also reports that the F.B.I. bought and tested NSO software for years with plans to use it for domestic surveillance until the agency finally decided last year not to deploy the tools.

The Times found that sales of Pegasus played a critical role in securing the support of Arab nations in Israel's campaign against Iran and negotiating the Abraham Accords, the 2020 diplomatic agreements, signed at a Trump White House ceremony, that normalized relations between Israel and some of its longtime Arab adversaries.

The U.S. sought the cyberweapon for domestic use.

The U.S. had also moved to acquire Pegasus, The Times found. The F.B.I., in a deal never previously reported, bought the spyware in 2019, despite multiple reports that it had been used against activists and political opponents in other countries. It also spent two years discussing whether to deploy a newer product, called Phantom, inside the United States.

The discussions at the Justice Department and the F.B.I. continued until last summer, when the F.B.I. ultimately decided not to use NSO weapons.

But Pegasus equipment is still in a New Jersey building used by the F.B.I. And the company also gave the agency a demonstration of Phantom, which could hack American phone numbers.

A brochure for potential customers, obtained by The Times, says that Phantom allows American law enforcement and spy agencies to "turn your target's smartphone into an intelligence gold mine."

The yearlong Times investigation was based on interviews with government officials, leaders of intelligence and law enforcement agencies, cyber experts, business executives and privacy activists in a dozen countries.

It tells the story of NSO's rise from a start-up operating out of a converted chicken coop on an agricultural cooperative to its blacklisting by the Biden administration in November because of its use by foreign governments to "maliciously target" dissidents, journalists and others.

NSO began with two school friends, Shalev Hulio and Omri Lavie, hatching start-ups in Bnai Zion, an agricultural cooperative outside of Tel Aviv, in the mid-2000s.

One of their start-ups, CommuniTake, which offered cellphone tech-support workers the ability to take control of their customers' devices — with permission — caught the attention of a European intelligence agency, Mr. Hulio said.

NSO was born, and the company eventually developed a way to gain access to phones without the user's permission — no need to click on a malicious attachment or link. (That the company's name sounded like the N.S.A. was a mere coincidence).

'You start to believe your every move is watched.'

After NSO began selling Pegasus globally in 2011, Mexican authorities used it to capture Joaquín Guzmán Loera, the drug lord known as El Chapo. And European investigators used it to smash a child-abuse ring with dozens of suspects in more than 40 countries.

But abuses have also been revealed in reports by researchers and news organizations, including The Times.

Mexico used the spyware to target journalists and dissidents. Saudi Arabia used it against women's rights activists and associates of Jamal Khashoggi, the Washington Post columnist who was killed and dismembered by Saudi operatives in 2018.

That year, the C.I.A. bought Pegasus to help Djibouti, an American ally, fight terrorism, despite longstanding concerns about human rights abuses there, including the persecution of journalists and the torture of dissidents.

In the U.A.E., Pegasus was used to hack the phone of an outspoken critic of the government, Ahmed Mansoor.

Mr. Mansoor's email account was breached, his geolocation was monitored, $140,000 was stolen from his bank account, he was fired from his job and strangers beat him on the street.

"You start to believe your every move is watched," he said. In 2018, he was sentenced to 10 years in prison for posts he made on Facebook and Twitter.

Through a series of new deals licensed by the Israeli Ministry of Defense, Pegasus has been provided to the far-right leaders of Poland, Hungary, India and other countries.

Mr. Netanyahu did not order the Pegasus system to be cut off, even when the Polish government enacted laws that many Jews inside and outside of Israel saw as Holocaust denial, or when Prime Minister Mateusz Morawiecki, at a conference attended by Mr. Netanyahu himself, falsely listed "Jewish perpetrators" among those responsible for the Holocaust.

The blacklisting of NSO infuriated Israeli officials.

American companies have been trying to build their own tools that could hack phones with the ease of NSO's "zero click" technology.

One of those companies, Boldend, told Raytheon, the defense-industry giant, in January 2021, that it could hack WhatsApp, the popular messaging service owned by Facebook, but then lost the capability after a WhatsApp update, according to a presentation obtained by The Times.

The claim was especially notable because, according to one of the slides, a major Boldend investor is Founders Fund — a company run by Peter Thiel, the billionaire who was one of Facebook's first investors and remains on its board.

The recent American blacklisting of NSO could suffocate the company by denying it access to the American technology it needs to run its operations, including Dell computers and Amazon cloud servers.

The rebuke has infuriated Israeli officials who have denounced the move as an attack not only on a crown jewel of the country's defense industry but on the country itself.

"The people aiming their arrows against NSO," said Yigal Unna, director general of the Israel National Cyber Directorate until Jan. 5, "are actually aiming at the blue and white flag hanging behind it."