Hacking a Prince, an Emir and a Journalist to Impress a Client

By David D. Kirkpatrick and Azam Ahmed
The New York Times, Aug. 31, 2018

Rulers of the United Arab Emirates have been using Israeli spyware for several years, leaked e-mails show.Rustam Azmi/Getty Images

Rulers of the United Arab Emirates have been using Israeli spyware for several years, leaked e-mails show.Rustam Azmi/Getty Images

The rulers of the United Arab Emirates had been using Israeli spyware for more than a year, secretly turning the smartphones of dissidents at home or rivals abroad into surveillance devices.

So when top Emirati officials were offered a pricey update of the spying technology, they wanted to make sure it worked, according to leaked emails submitted Thursday in two lawsuits against the spyware's maker, the Israel-based NSO Group.

Could the company secretly record the phones of the emir of Qatar, a regional rival, the Emiratis asked? How about the phone of a powerful Saudi prince who directed the kingdom's national guard? Or what about recording the phone of the editor of a London-based Arab newspaper?

"Please find two recordings attached," a company representative wrote back four days later, according to the emails. Appended were two recordings the company had

made of calls by the editor, Abdulaziz Alkhamis, who confirmed this week that he had made the calls and said he did not know he was under surveillance.

The NSO Group's actions are now at the heart of the twin lawsuits accusing the company of actively participating in illegal spying — part of a global effort to confront the growing arms race in the world of spyware.

As private companies develop and sell cutting-edge surveillance technology to governments for tens of millions of dollars, human rights groups say the scant oversight over the practice invites rampant misuse. And no company is more central to the battle than the NSO Group, one of the best-known creators of spyware that invades smartphones.

The two lawsuits, filed in Israel and Cyprus, were brought by a Qatari citizen and by Mexican journalists and activists who were all targeted by the company's spyware.

In Mexico, the NSO Group has sold the surveillance technology to the Mexican government on the explicit condition that it be used only against criminals and terrorists. Yet some of the nation's most prominent human rights lawyers, journalists and anti-corruption activists have been targeted instead. Many are now plaintiffs in the lawsuits.

The government of Panama also purchased the spyware, and the president at the time used it to spy on his political rivals and critics, according to court documents in a case there.

Whenever challenged, the company has said that it merely sells the technology to governments, which agree to deploy it exclusively against criminals but then operate it on their own.

The new lawsuits include leaked documents and emails that directly challenge the company's repeated assertions that it is not responsible for any illegal surveillance conducted by the governments that buy its spyware.

In the case of the U.A.E., the lawsuits argue, an affiliate of the NSO Group attempted to spy on foreign government officials — and successfully recorded the calls of a journalist — at the request of its Emirati customers four years ago.

The technology works by sending text messages to a target's smartphone, hoping to bait the person into clicking on them. If the user does, the spyware, known as Pegasus, is secretly downloaded, enabling governments to monitor phone calls, emails, contacts and potentially even face-to-face conversations conducted nearby.

For the U.A.E., documents show, an affiliate of the NSO Group specifically suggested language for the corrupting text messages. Many were tailored for the

Persian Gulf with seemingly innocuous invitations like “Ramadan is near — incredible discounts” and “keep your car tires from exploding in the heat.”

Leaked technical documents included in the lawsuits also show that the company helped its clients by transmitting the data gained through surveillance through an elaborate computer network.

“We are pushing to make the law catch up with technology” and show that the spyware makers “are complicit in these privacy violations,” said Alaa Mahajna, an Israeli lawyer who filed the lawsuits in cooperation with Mazen Masri, a senior lecturer in law at the City University of London.

The NSO group declined to comment until it could review the lawsuits. The Emirati Embassy in Washington did not respond to a request for comment.

After The New York Times reported last year that prominent Mexican lawyers, journalists and anticorruption campaigners had been targeted by the NSO Group’s spyware, the Mexican government announced a federal investigation.

But more than a year later, the investigation has made little apparent progress, so the Mexican journalists and human rights defenders joined the lawsuits to uncover more about the government’s hacking program.

The lawsuits also shed new light on the political intrigues involving Israel and the Persian Gulf monarchies, which have increasingly turned to hacking as a favorite weapon against one another.

The NSO Group’s actions are now at the heart of the twin lawsuits accusing the company of actively participating in illegal spying.Daniella Cheslow/Associated Press

The NSO Group's actions are now at the heart of the twin lawsuits accusing the company of actively participating in illegal spying.Daniella Cheslow/Associated Press

The U.A.E. does not recognize Israel, but the two appear to have a growing behind-the-scenes alliance. Because Israel deems the spyware a weapon, the lawsuits note, the NSO Group and its affiliates could have sold it to the Emirates only with approval by the Israeli Defense Ministry.

Leaked emails submitted in the lawsuits show that the U.A.E. signed a contract to license the company's surveillance software as early as August 2013.

A year and a half later, a British affiliate of the NSO Group asked its Emirati client to provide a sixth payment of $3 million under the original contract, suggesting a total licensing fee of at least $18 million over that period.

An update the next year was sold through a different affiliate, based in Cyprus, at a cost of $11 million in four installments, according to leaked invoices.

Tensions between the U.A.E. and its neighbor Qatar reached a boil in 2013 over a struggle for power in Egypt. Qatar had allied itself with the Egyptian Islamist movement that won the elections after the Arab Spring. Then the U.A.E. backed a military takeover that cast the Islamists into prison instead.

In the escalating feud, each side accused the other of cyberespionage. Hackers broke into the email accounts of two outspoken opponents of Qatar — the Emirati ambassador to Washington, Yousef al-Otaiba, and an American Republican fund-raiser who does business with the U.A.E., Elliott Broidy. Mr. Broidy has filed a separate lawsuit accusing Qatar and its Washington lobbyists of conspiring to steal and leak his emails.

Other hackers briefly took over the website of the Qatari news service to post a false report of an embarrassing speech by the emir to damage him, and later leaked Qatari emails exposing awkward details of Qatari negotiations over the release of a royal hunting party kidnapped in Iraq. Allies of Qatar blamed the Emiratis.

The leaked emails disclosed in the new lawsuits may also have been stolen through hacking. Lawyers involved said the documents were provided by a Qatari journalist who did not disclose how he had obtained them.

The messages show that the Emiratis were seeking to intercept the phone calls of the emir of Qatar as early as 2014.

But the Emirati target list also included Saudi Arabia. In the email discussions about updating the NSO Group's technology, the Emiratis asked to intercept the phone calls of a Saudi prince, Mutaib bin Abdullah, who was considered at the time to be a possible contender for the throne.

The Emiratis have been active promoters of Prince Mutaib's younger rival, Crown Prince Mohammed bin Salman. Last year, the crown prince removed Prince Mutaib from his role as minister of the national guard and ordered his temporary detention in connection with corruption allegations.

In a telephone interview, Prince Mutaib expressed surprise that the Emiratis had attempted to record his calls.

"They don't need to hack my phone," he said. "I will tell them what I am doing."

According to the emails, the Emiratis also asked to intercept the phone calls of Saad Hariri, who is now prime minister of Lebanon.

Mr. Hariri has sometimes been accused of failing to push back hard enough against Hezbollah, the powerful Lebanese movement backed by Iran. Last year, the U.A.E.'s Saudi ally, Crown Prince Mohammed, temporarily detained Mr. Harari in Riyadh, the Saudi capital, and forced him to announce his resignation as prime minister. (He later rescinded the announcement, and he remains prime minister.)

Mr. Alkhamis, who resigned in 2014 as the editor of the London-based newspaper Al Arab, called the surveillance of his phone calls "very strange" but not unexpected, since he had published "sensitive" articles about Persian Gulf politics.

The U.A.E.'s use of the NSO Group's spyware was first reported in 2016. Ahmed Mansoor, an Emirati human rights advocate, noticed suspicious text messages and exposed an attempt to hack his Apple iPhone. The U.A.E. arrested him on apparently unrelated charges the next year and he remains in jail.

After Mr. Mansoor's disclosures, Apple said it had released an update that patched the vulnerabilities exploited by the NSO Group. The NSO Group pledged to investigate and said in a statement that "the company has no knowledge of and cannot confirm the specific cases."

But other leaked documents filed with the lawsuits indicate that the U.A.E. continued to license and use the Pegasus software well after Apple announced its fix and the NSO Group pledged to investigate.

On June 5, 2017, the U.A.E. and Saudi Arabia began a blockade of Qatar in an effort to isolate it. Ten days later, an internal Emirati email cited in the lawsuits referred to 159 members of the Qatari royal family, officials and others whose phones it had targeted with the NSO spyware, promising a report based on "what we found from the top 13 targets only."

"ur highness based on ur instructions we viewed the collecting from the Q phone targeting," wrote an Emirati official identified in the lawsuits as an assistant to Prince Khalid bin Mohammed, the chairman of the Emirati intelligence agency and the son of the de facto ruler of the U.A.E., Crown Prince Mohammed bin Zayed.

This month, Amnesty International said one of its staff members working in Saudi Arabia had also been targeted by spyware that appeared to be linked to the NSO Group, and the company reiterated that it bears no responsibility for its customers' use of its spyware.

"Our product is intended to be used exclusively for the investigation and prevention of crime and terrorism," the company said in a statement to Amnesty, pledging to "investigate the issue and take appropriate action."

A version of this article appears in print on Aug. 31, 2018, on Page A7 of the New York edition with the headline: How United Arab Emirates Used Israeli Technology to Spy on Rivals. Order Reprints | Today's Paper | Subscribe