Pegasus project turns spotlight on spyware firm NSO's ties to Israeli state

Wednesday 21 July 2021, by HOLMES Oliver, KIRCHGAESSNER Stephanie, WALKER Shaun (Date first published: 20 July 2021).

Disclosures about political figures put Israel under increasing pressure over extent of surveillance.

[Photo: The NSO Group chief executive, Shalev Hulio. A recent transparency report acknowledges the firm is 'closely regulated' by export control authorities in Israel. Composite: Guardian/Reuters]

Back in 2017, few would have disputed that Israel and Saudi Arabia were regional foes. Officially, the countries had no diplomatic ties. Yet for a small group of Israeli businesspeople attending secret meetings with Saudi officials in Vienna, Cyprus and Riyadh that summer, there were signs relations were warming.

The businesspeople represented NSO Group. Their mission was to sell the Saudis NSO's weapons–grade spyware system, Pegasus.

According to a person who attended the meeting in June 2017 in Cyprus, a senior Saudi intelligence official was "amazed" by what he saw. After a lengthy and technical discussion, the Saudi spy, who had brought a new iPhone, was shown how Pegasus could infect the phone and then be used to remotely operate its camera.

"You don't need to understand the language to see they were amazed and excited and that they saw what they needed to," the person said.

NSO Group had been given explicit permission by the Israeli government to try to sell the homegrown hacking tools to the Saudis. It was a classified arrangement and resulted in the sale later being sealed in Riyadh in a deal reportedly worth at least $55m.

"In Israel there is a strong political movement to make diplomacy through business," said the person, speaking on the condition of anonymity. "Business first, diplomacy later. When you make a deal together, it opens a lot of doors to diplomacy."

It is common for governments to help companies export their products. NSO, after all, employs former Israeli cyber-intelligence officials and retains links to the defence ministry.

But revelations about how repressive states such as Saudi Arabia, the United Arab Emirates, Azerbaijan and others have used NSO's technology to target human rights lawyers, activists and journalists raise questions for Israel and have put the issue under fresh scrutiny.

The disclosures threaten to put diplomatic pressure on Israel, amid questions over whether it is using the licensing of NSO's spyware for political leverage – and allowing the software to be sold to undemocratic countries that are likely to misuse it.

A recent transparency report released by NSO Group acknowledged the company was “closely regulated” by export control authorities in Israel. The Defense Export Controls Agency (DECA) within the Israeli defence ministry “strictly restricts” the licensing of some surveillance products based on its own analysis of potential customers from a human rights perspective, the company said, and had rejected NSO requests for export licences “in quite a few cases”.

Moreover, NSO was also subject to an “in-depth” regulatory review by Israel on top of its own “robust internal framework”.

Within NSO, the process Israel uses to assess whether countries can be sold the technology is considered a “state secret”. A person familiar with the process said officials in both Israel’s national security council and prime minister’s office had been known to give their input.

In the case of Saudi Arabia, sources familiar with the matter said the kingdom was temporarily cut off from using Pegasus in 2018, for several months, following the murder of Jamal Khashoggi, but was allowed to begin using the spyware again in 2019 following the intervention of the Israeli government.

It is unclear why the Israeli government urged NSO to reconnect the surveillance tool for Riyadh.

However, the 10 countries that the forensic analysis for the Pegasus project suggests have actually been abusing the technology all enjoy trade relations with Israel or have diplomatic ties with the country that have been improving markedly in recent years.

In two NSO client countries, India and Hungary, it appears governments began using the company’s technology as or after their respective prime ministers met the then Israeli prime minister, Benjamin Netanyahu, in high-profile encounters intended to boost trade and security cooperation. It is understood no countries that are considered enemies of Israel – such as Turkey – have been allowed to buy NSO’s wares.

“Markets dictate what works, I don’t dictate … the only place I have actually intervened … is cybersecurity,” Netanyahu said in a press conference in Hungary in 2017 as he stood next to the country’s prime minister, Viktor Orbán.

What remains unclear is whether Israel’s intelligence agencies might have special privileges with NSO, such as access to surveillance material gathered using its spyware. One person close to the company, who asked to remain anonymous, said it was a frequent topic of speculation. Asked whether Israel could access intelligence gathered by NSO clients, they replied: “The Americans think so.”

That view was supported by current and former US intelligence officials, who told the Washington Post, a partner in the Pegasus project, that there was a presumption that Israel had some access – via a “backdoor” – to intelligence unearthed via such surveillance tools.

John Scott-Railton, a senior researcher at the Citizen Lab at the University of Toronto, said he believed it would be “irresponsible” for a state to allow the large-scale distribution of a powerful surveillance tool such as Pegasus without being able to keep an eye on what was being done with it.

He said court records had revealed that NSO used servers that were not always located on the premises of the client. “What that means is there’s the potential for visibility. And it would be crazy for them [the Israelis] not to have visibility,” he said.

NSO strongly denied that Israel had any access to its customers’ systems.

“NSO Group is a private company. It is not a ‘tool of Israeli diplomacy’; it is not a backdoor for Israeli intelligence; and it does not take direction from any government leader,” NSO’s lawyer said.

In a statement, the Israeli Ministry of Defense said Israel marketed and exported cyber products in accordance with its 2007 Defense Export Control Act and that policy decisions take “national security and strategic considerations” into account, which include adherence to international arrangements.

“As a matter of policy, the state of Israel approves the export of cyber products exclusively to governmental entities, for lawful use, and only for the purpose of preventing and investigating crime and counter-terrorism, under end-use/end-user certificates provided by the acquiring government,” the ministry said.

It said “appropriate measures” were taken in cases where exported items are used in violation of export licences.

The ministry added: “Israel does not have access to the information gathered by NSO’s clients.”

For Israel, few clients whom it has approved to use Pegasus have been as problematic as Saudi. Weeks ago, NSO cut the kingdom off once more, following allegations that Saudi had used Pegasus to hack dozens of Al Jazeera journalists.

Saudi Arabia declined to comment.

Stephanie Kirchgaessner in Washington, **Oliver Holmes** in Jerusalem and **Shaun Walker** in Budapest

---

Box: Quick Guide - What is in the Pegasus project data?

What is in the data leak?

The data leak is a list of more than 50,000 phone numbers that, since 2016, are believed to have been selected as those of people of interest by government clients of NSO Group, which sells surveillance software. The data also contains the time and date that numbers were selected, or entered on to a system. Forbidden Stories, a Paris-based nonprofit journalism organisation, and Amnesty International initially had access to the list and shared access with 16 media organisations including the Guardian. More than 80 journalists have worked together over several months as part of the Pegasus project. Amnesty’s Security Lab, a technical partner on the project, did the forensic analyses.

What does the leak indicate?

The consortium believes the data indicates the potential targets NSO’s government clients identified in advance of possible surveillance. While the data is an indication of intent, the presence of a number in the data does not reveal whether there was an attempt to infect the phone with spyware such as Pegasus, the company’s signature surveillance tool, or whether any attempt succeeded. The presence in the data of a very small number of landlines and US numbers, which NSO says are “technically impossible” to access with its tools, reveals some targets were selected by NSO clients even though they could not be infected with Pegasus. However, forensic examinations of a small sample of mobile phones with numbers on the list found tight correlations between the time and date of a number in the data and the start of Pegasus activity – in some cases as little as a few seconds.

What did forensic analysis reveal?

Amnesty examined 67 smartphones where attacks were suspected. Of those, 23 were successfully infected and 14 showed signs of attempted penetration. For the remaining 30, the tests were inconclusive, in several cases because the handsets had been replaced. Fifteen of the phones were Android devices, none of which showed evidence of successful infection. However, unlike iPhones, phones that use Android do not log the kinds of information required for Amnesty’s detective work. Three Android phones showed signs of targeting, such as Pegasus-linked SMS messages.

Amnesty shared “backup copies” of four iPhones with Citizen Lab, a research group at the University of Toronto that specialises in studying Pegasus, which confirmed that they showed signs of Pegasus infection. Citizen Lab also conducted a peer review of Amnesty’s forensic methods, and found them to be sound.

Which NSO clients were selecting numbers?

While the data is organised into clusters, indicative of individual NSO clients, it does not say which NSO client was responsible for selecting any given number. NSO claims to sell its tools to 60 clients in 40 countries, but refuses to identify them. By closely examining the pattern of targeting by individual clients in the leaked data, media partners were able to identify 10 governments believed to be responsible for selecting the targets: Azerbaijan, Bahrain, Kazakhstan, Mexico, Morocco, Rwanda, Saudi Arabia, Hungary, India, and the United Arab Emirates. Citizen Lab has also found evidence of all 10 being clients of NSO.

What does NSO Group say?

You can read NSO Group’s full statement here. The company has always said it does not have access to the data of its customers’ targets. Through its lawyers, NSO said the consortium had made “incorrect assumptions” about which clients use the company’s technology. It said the 50,000 number was “exaggerated” and that the list could not be a list of numbers “targeted by governments using Pegasus”. The lawyers said NSO had reason to believe the list accessed by the consortium “is not a list of numbers targeted by governments using Pegasus, but instead, may be part of a larger list of numbers that might have been used by NSO Group customers for other purposes”. They said it was a list of numbers that anyone could search on an open source system. After further questions, the lawyers said the consortium was basing its findings “on misleading interpretation of leaked data from accessible and overt basic information, such as HLR Lookup services, which have no bearing on the list of the customers’ targets of Pegasus or any other NSO products … we still do not see any correlation of these lists to anything related to use of NSO Group technologies”. Following publication, they explained that they considered a “target” to be a phone that was the subject of a successful or attempted (but failed) infection by Pegasus, and reiterated that the list of 50,000 phones was too large for it to represent “targets” of Pegasus. They said that the fact that a number appeared on the list was in no way indicative of whether it had been selected for surveillance using Pegasus.

What is HLR lookup data?

The term HLR, or home location register, refers to a database that is essential to operating mobile phone networks. Such registers keep records on the networks of phone users and their general locations, along with other identifying information that is used routinely in routing calls and texts. Telecoms and surveillance experts say HLR data can sometimes be used in the early phase of a surveillance attempt, when identifying whether it is possible to connect to a phone. The consortium understands NSO clients have the capability through an interface on the Pegasus system to conduct HLR lookup inquiries. It is unclear whether Pegasus operators are required to conduct HRL lookup inquiries via its interface to use its software; an NSO source stressed its clients may have different reasons – unrelated to Pegasus – for conducting HLR lookups via an NSO system.

On Tuesday 27 July, at 8pm BST, a panel including Agnès Callamard, secretary general of Amnesty International, will discuss the global implications of the Pegasus project. Book your ticket here: ttps://membership.theguardian.com/event/the-pegasus-project-revealing-a-global-abuse-of-cybersurveillance-163379288851

P.S.

• The Guardian. Tue 20 Jul 2021 12.00 BST. Last modified on Wed 21 Jul 2021 05.09 BST :
https://www.theguardian.com/world/2021/jul/20/pegasus-project-turns-spotlight-on-spyware-firm-nso-ties-to-israeli-state