The NATIONAL INTEREST FOUNDATION

A New York Times Investigation Details Israel's Use of the Heavily Criticized NSO Group's Spyware as a Core Element of Its Diplomacy Efforts

A year-long investigation by the New York Times has documented instances where Israel has used the widely-criticized NSO Group's Pegasus spyware as a tool and form of currency in its diplomacy efforts. The NSO Group, which clears all sales of its product through the Israeli government, has been sold to some of the most repressive perpetrators of human rights abuses in the world. The malware has been deployed by these leaders and their governments – whose track records with respect to human rights and the rule of law should place them at odds with countries who profess to value freedom and democracy – in order to spy on journalists, human rights lawyers and activists, and opposition leaders. Israel has authority to approve or deny the sale of the Pegasus software, and entities that garnered access to it have, among other things, altered their votes at the United Nations to support Israeli policy positions. Nearly all of the signatories to the Abraham Accords were granted a negotiated access to the spyware. Other occurrences uncovered by the investigation include Saudi Arabia, who though not a signatory to the deal, threatened to block it if their contract to use the software was not renewed. Additionally, after Israel formalized an agreement to sell India sophisticated weaponry that included the Pegasus software, India switched its vote in the United Nations to deny observer status to a Palestinian human rights organization. Hungary, a customer of NSO Group too, was the only European Union government to not criticize Israel's annexation plans of Palestinian land in the West Bank back in 2020.

Bahrain has used the software to track critics of the island regime and human rights activists, some of whom are languishing in its prisons today. The United Arab Emirates has also relied on it to hack the phones of civil rights activists who have since been imprisoned. Reports of the UAE leader's use of the spyware to infiltrate the phones of his ex-wife and her legal team during a custody battle have been well-documented. In Saudi Arabia, Pegasus has been deployed to hack the phones of women's rights activists and infamously against the journalist Jamal Khashoggi – whom Saudi operatives killed and dismembered on the orders of Crown Prince Mohammed bin Salman. Regrettably, the malware has made it easier for authoritarian governments and enemies of freedom to repress their own people and spy on human rights activists, lawyers, journalists, and diplomats.

Late last year it was reported that Pegasus had also been used against Palestinian rights activists. An initial investigation into the hacked phones did not reveal which government had deployed it, however, Israeli government policy states that the Pegasus program cannot be used by a foreign government against domestic phones – as those belonging to the hacked Palestinians were. This, along with the well-documented control Israel has over the program's licensure and export, raises fresh and justifiable questions about the ways in which Palestinians are subjected to Israeli human rights abuses.

In November of last year, the United States announced that it was applying sanctions to NSO Group for its activities. The sanctions isolated NSO from American technologies it needs to operate and has put it at risk of being unable to function. The Israeli Defense Ministry, who oversees the NSO Group, expressed anger at the sanctions for what it called "U.S. hypocrisy," as the United States had been secretly using the software for years at home and had exported it in at least one instance to an African country with a track record of human rights abuses. Facebook, who owns WhatsApp, has sued NSO claiming that the company has exploited its product to track 1400 phones around the world, while Apple also has its own lawsuit against NSO alleging that the firm has violated its software.