The NATIONAL INTEREST FOUNDATION

U.S. Lawmakers Urge the Biden Administration to Sanction Four Cyber Surveillance Firms for Enabling Human Rights Abuses

Reports of spyware being sold to authoritarian governments by some cyber surveillance firms in the private sector and being used as a tool to violate human rights have been surfacing in recent months. Now, lawmakers in the United States are calling on the Biden administration to sanction four such companies, including the scandal-plagued Israeli firm NSO Group. More than a dozen Congressional Democrats, led by House Intelligence Chairman Adam Schiff of California and Senator Ron Wyden of Oregon, submitted a letter urging the U.S. Treasury Department to take punitive steps against NSO Group and three others. The lawmakers highlighted how the companies' reprehensible behavior has empowered and enabled the repressive regimes in their efforts to silence, torture, and even murder rights activists and journalists. In one of the most heinous and high-profile instances, NSO Group's widely criticized Pegasus software was used to spy on Saudi journalist and dissident Jamal Khashoggi before he was killed at the Kingdom's consulate in Istanbul back in October of 2018. On top of the NSO Group, the three additional entities spotlighted for enabling human rights abuses are Emirati cybersecurity firm DarkMatter and the two European companies Nexa Technologies and Trovicor.

One of the more public examples of spyware being sold to and used by violent, oppressive authoritarian governments involves the NSO Group and its Pegasus program. Pegasus is a form of malware that infects smartphones to enable the extraction of messages, photos, and emails, while also secretly activating microphones and cameras. It has been sold to 40 unnamed counties but some of the known government clients are Bahrain, India, Kazakhstan, Rwanda, Saudi Arabia, and the United Arab Emirates. The malware program has been used to spy on at least 189 journalists, 85 human rights activists and political dissidents, 65 business executives, and more than 600 politicians and government officials.

In Bahrain, the iPhones belonging to nine Bahraini activists were hacked using Pegasus between June 2020 and February 2021, and reports indicate that the regime there may have begun using the software even before that back in 2017. The Bahraini government has also been alleged to be a client of Trovicor. In Saudi Arabia, the deal to sell Pegasus to Riyadh in 2017 was reportedly worth $55 million, and the regime used the program to surveille journalist Jamal Khashoggi's family after the Saudi crown prince, Mohammed bin Salman, was linked to his brutal murder in Turkey. The phones of the Turkish prosecutor in charge of the Khashoggi murder investigation, Irfan Fidan, as well as his wife, were also hacked via Pegasus. Additionally, there are credible findings which show that Saudi Arabia has used Pegasus to hack dozens of phones belonging to Al Jazeera journalists. In the United Arab Emirates, Prime Minister Sheikh Mohammed bin Rashid al-Maktoum used the spyware to hack the phones of his ex-wife, Princess Haya, and five other people close to her. Emirati human rights activist, Ahmed Mansoor, currently serving a prison sentence, was also the target of the software back in 2016 prior to his detainment the following year in 2017.

The call for further sanctions by U.S. lawmakers comes after the iPhones of State Department employees in Uganda had been hacked by NSO spyware. Sanctions against these companies would isolate them from investors and, it is hoped, put them out of business for good and prevent repressive governments from having access to immense spying powers. An investigation by Google concluded that these spyware programs are on par with elite nation-state capabilities. The Biden administration has repeatedly expressed that human rights considerations are a major component of its cybersecurity policy, and as such, strong sanctions against companies like NSO Group would be consistent with this.