The NATIONAL INTEREST FOUNDATION

Israel's Cognyte Sold Intercept Spyware to Myanmar a Month Before the 2021 Military Coup

According to recently revealed documents, the Israeli spyware firm Cognyte Software sold intercept spyware to a telecommunications firm linked to the Myanmar military. The documents were obtained by the NGO Justice For Myanmar. This sale occurred just a month before the junta launched a military coup in February 2021. The deal was finalized despite a 2017 Israeli Supreme Court ruling banning Israeli firms from making defense technology transfers to Myanmar. Although the U.S. and EU imposed an arms embargo on Myanmar, Israel initially refused to stop the sale of arms to Myanmar. This even continued as Myanmar pursued genocidal policies towards its Rohingya minority in 2016 and 2017. After intense public pressure. Israel claimed to have halted exports in 2018. Israel's Defense Ministry has not responded to questions of whether or not they had approved the sale. The spyware purchased gives the authorities the ability to hear calls, read messages, and even track locations. Eitay Mack, an Israeli human rights lawyer, has called for a criminal investigation against Cognyte and unnamed government officials who facilitated the sale. The document indicated that at the time of the purchase, Myanmar intended to install spyware into all of the country's telecommunications provider's systems. An investigation conducted by Facebook owner Meta Platforms indicated that this was not an isolated incident. There have also been instances of spyware being used in a wide range of countries, including Kenya, Mexico, and Indonesia, where it is used to spy on journalists and politicians.

Cognyte has had a long history of selling advanced monitoring technology to repressive regimes. These past sales were to Azerbaijan, Indonesia, South Sudan, Uzbekistan, and Kazakhstan. The company has a long history of aiding repressive regimes in violating human rights, and it is unclear why they are still allowed to operate. This is also not the first time an Israeli firm has come under scrutiny for the sale of spyware to authoritarian regimes. The cyber-arms company NSO Group has also been condemned multiple times for the sale of their spyware, Pegasus, to less than democratic countries. Pegasus allows the user to access a target's phone remotely, giving them access to everything on the phone, from photos to the microphone. Pegasus uses a zero-click attack, meaning that the spyware requires no user interaction to operate. It is evident from the document that Cognyte was aware of what the spyware would be used for.

Though some type of spyware is employed by nearly every country, there is usually some kind of legal process to assure human rights are not violated, however, repressive regimes, such as the military junta in Myanmar, rarely if ever employ these legal safeguards, opting instead to simply deploy them whenever those in power choose. These spywares are used to suppress pro-democracy institutions, arrest political rivals and journalists, crush protests, and ensure loyalty throughout their governments. It creates a chilling effect among would-be democratic activists, as they know that they could be under constant surveillance.

This spyware is a danger to democratic institutions across the world and must be regulated. Companies with a pattern of selling spyware to repressive governments need to be criminally investigated for aiding and abetting crimes against humanity. Increased accountability and oversight are the only surefire way to ensure that these firms do not sell malicious software to authoritarian regimes.