The NATIONAL INTEREST FOUNDATION

Journalists' Phones are Targeted by the Spyware of an Israeli Firm with Links to a Long List of Past Human Rights Violations

Dozens of journalists, executives, and producers at the Qatar-based Al Jazeera media organization had their personal cell phones hacked with spy software developed by Israeli surveillance firm NSO Group, in an operation widely attributed to the governments of Saudi Arabia and the United Arab Emirates. In total, upward of 35 Al Jazeera employees had their electronic devices compromised. NSO Group has been frequently connected to high-profile cases of serious human rights violations which have raised questions over the future of the company's spyware. NSO's product has been used to target independent journalists in Morocco, political dissidents in Rwanda, pro-democracy actors in Togo, and opposition politicians in Spain, in addition to its connection to the Khashoggi murder and the latest hacking of Al Jazeera journalists. The regimes in Saudi Arabia and the United Arab Emirates have long-standing issues with Al Jazeera, primarily for the organization's reporting on the repressive governments around the Gulf. The hacking is the latest attempt by autocratic Gulf regimes in the Middle East to silence journalists, following upon the murder of Jamal Khashoggi by Saudi operatives two years ago in October of 2018.

The connection of the hacking to the governments of Saudi Arabia and the United Arab Emirates is not at all surprising, considering the two countries have led an effort to blockade and blackmail Qatar over its alleged link to terrorist groups and its ties to Iran. In 2017, Saudi Arabia, the UAE, Bahrain, and Egypt began a diplomatic and economic blockade of Qatar until it complied with a list of demands that included shuttering Al Jazeera. The government of Qatar has emphatically denied any association with terror groups, and the international community has not given any legitimacy to Saudi and Emirati claims to the contrary. Both Saudi Arabia and the UAE also have a shared track record of targeting journalists and silencing voices that amplify criticism of their governments.

The hack was first discovered by researchers at the University of Toronto after Al Jazeera journalist Tamer Almisshal believed his phone to be compromised and turned it over to cybersecurity experts at the university's Citizen Lab. Upon further testing, it was deduced that Almisshal's phone had been infected with spyware called Pegasus, which was developed by Israeli firm NSO Group. The spyware was able to access messages, emails, photos, and had the ability to remotely turn on the device's microphone to record conversations. Some of the affected journalists have voiced concern over private information on their phones being compromised and used to blackmail them in the future. The same spyware was found on the phone of an associate of Jamal Khashoggi after he was murdered by a Saudi hit squad in Istanbul, Turkey. Almisshal has stated that he believes the hacking operation was ordered after he and other Al Jazeera journalists placed calls to Emirati government officials for a story that they were working on.

NSO Group has attempted to argue that the software they sold to the Saudi and Emirati authorities, in addition to other governments, was only supposed to be used to assist them in tracking criminals. However, the clear and consistent pattern of targeting independent journalists, political dissidents, and pro-democracy activists debunks this false claim and highlights how the firm's spyware has been cynically used to aid certain governments in repressing their respective populations.