The NATIONAL INTEREST FOUNDATION

Rights Organizations and Cybersecurity Watchdogs Find That Palestinian Activists' Phones Were Hacked by the Recently Blacklisted NSO Group

An investigation by cybersecurity watchdogs and human rights organizations including Amnesty International found that the cell phones of at least six Palestinian activists were hacked by spyware from the controversial Israeli firm NSO Group. The revelations come amid growing global criticism of the company's activities, which recently prompted the United States to blacklist it. NSO Group develops and sells a spyware software called Pegasus that has been used by repressive governments around the world to secretly penetrate the mobile devices of activists and journalists, extracting its contents and monitoring its location. The malware has been linked to the Israeli government, with independent international computer privacy experts uncovering the latest findings regarding the hacking of Palestinian rights activists' phones. Despite receiving widespread condemnation from social justice organizations and other entities for the behavior, Israel has expressed that it will lobby the United States to try and change course on the rightful blacklisting of the NSO Group.

The Israeli spyware firm's Pegasus program has repeatedly been deployed to violate the personal freedoms and liberties of citizens in countries where abusive governments operate. The software has been utilized by Saudi Arabia, the United Arab Emirates, India, Hungary, and others against dissidents, journalists, and activists that are deemed to be a threat to the ruling regime's grip on power. Thus, the intentionally repressive makeup of the spyware has drawn significant denouncement and worried independent watchdogs, activist groups, and governments across the globe over the deceptive masking of it as "counterterrorism" when in actuality, it is being used as a means to strengthen autocratic control and violate individual human rights in various places.

The new findings against NSO Group also come at a time when Israel is facing criticism for its unjust terror designations against Palestinian civil society and activist groups, a blatant attempt to diminish their work in drawing attention to Israel's wide array of human rights violations and abuses. The Palestinian organizations receive support and funding from the European Union and other reputable sources, and as such, analysts have dismissed the ridiculous nature of the Israeli efforts to damage their standing. The groups themselves have also spoken out against the clear motivations behind the false designations, pointing out its aim to silence them and their humanitarian work from exposing the unlawful activities of the Israeli government. The terror designations also appear to have been used as a pretext for the hacking of the Palestinian activists' phones, with Israeli authorities trying to provide themselves with a cover for why they targeted these individuals. Thankfully though, most impartial observers have seen through this clear ruse and are appropriately condemning the NSO Group and its enablers.

Ultimately, the hacking of activist phones and the consistent repressive behavior that the NSO Group's spyware facilitates is a violation of international law and privacy standards. Therefore, the United States under the Biden administration was right to blacklist the company. This week's latest revelations on the targeting of Palestinian activists as well only serves to further uncover the unlawful acts carried out by the Israeli spyware firm. While Israel tries to defend its actions and lobby the United States for the NSO Group to be removed from the blacklist, it is important that social justice voices counter this by continuing to highlight how the company's software empowers anti-democratic forces.