MIDDLE EAST HIT-JOB COMPANIES WILL STOOP TO THE LOWEST CRIMES TO STEAL AMERICAN TECHNOLOGY FROM U.S. COMPANIES

Over the past few weeks, two revelations have shocked the cyber world. Both involved Israeli companies engaged in dirty ops on behalf of shady client states.

The most prominent was the discovery that NSO Group, which I've written about regularly here and at the *Nation*, devised a hack that permitted it to intercept conversations conducted via WhatsApp. The target/victim was a lawyer who is pursuing a legal case against NSO Group in Israeli courts.

The lawyer turned to Citizens Lab, which has exposed NSO's hacking of the electronic devices of human rights activists, lawyers, journalists, and teachers around the world. As Citizens Lab began to investigate the victim's phone, WhatsApp engineers too began noticing abnormalities in their voice-calling feature, then began warning human rights organizations that they were the targets, which likely became clear in the process of their forensic investigation.

The vulnerability has been fixed, and presumably WhatsApp is secure once more. But the incident should concern not only human rights activists, who appear to have been the main targets of the attack, but tens of millions of users for whom secure communication is important.

It's worthwhile to explore the background of this most recent attack. NSO Group's Pegasus malware infected the cellphone of Saudi-Canadian activist Omar Abdulaziz, who was a colleague of Jamal Khashoggi, the journalist who was murdered by a Saudi death squad in Istanbul last year. It's quite possible that since Abdulaziz was in regular communication with Khashoggi, the hack of the former's phone enabled the Saudi killers to track both men, specifically Khashoggi. Doing so would have been critical to their plans to kill him.

Media reports have confirmed that the Saudi intelligence agency that murdered Khashoggi spent $55 million to purchase Pegasus for use against enemies of the kingdom. It's beyond reasonable to think that the Saudis deployed Pegasus to hack Abdulaziz's phone. He is suing NSO in Israeli courts.

Last month, Citizens Lab announced that it had exposed yet another NSO hack of a Saudi dissident. Ghanem Almasarir is a human rights activist and outspoken opponent of the Saudi regime who maintains a popular Twitter account (four hundred thousand followers) and a YouTube channel (230 million views). The *Guardian* reported the cyber-security organization had discovered that Saudi intelligence had infected his electronic devices with Pegasus:

> Almasarir received suspicious text messages in June 2018. These were tracked by independent experts to a Pegasus operator who was "focused on Saudi Arabia" and were linked to a separate attack against another Saudi critic . . .
>
> Certain indicators on Almasarir's two Apple iPhones, coupled with the fact that he had clicked on corrupt weblinks sent to him, as well as Saudi Arabia's widely reported use of Pegasus, led to the "inevitable conclusion" that the kingdom was responsible for sending Almasarir the texts and for the infection of his devices.
>
> "A vast amount of Mr Almasarir's private information was stored and communicated on his iPhones . . . This included information relating to his personal life, his family, his relationships, his health, his finances, and private matters relating to his work promoting human rights in Saudi Arabia," the letter of claim [against Saudi Arabia filed by Almasarir's attorney] said.

The *Guardian* reports that Almasarir has been under UK police protection since last October, after it determined there were credible threats against his life. The CIA has reportedly notified police authorities in Norway that another Saudi social media activist, Iyad al Bagdhadi, also faces credible threats of harm from Saudi authorities. He too is under police protection there.

Shortly after NSO found out it was being sued by Abdulaziz, mysterious figures began contacting Citizens Lab researchers and others involved in the cases. The callers offered lucrative speaking gigs at international conferences. All they asked in return was to have lunch with the researchers.

At these lunches, the targets discovered that they'd been suckered. The only subject their putative benefactor wanted to talk about was Citizens Lab, and what it knew or thought about the Israeli company. He also tried to elicit prejudicial statements about the target's views on Israel.

It was obvious that the client involved in this masquerade was NSO. Less clear was who was running the operation on that company's behalf.

This mystery too soon revealed itself: a journalist noticed that the man who sent the lunch invitations and pumped the researchers for information had also done similar work on behalf of the Israeli black ops company Black Cube, the firm that Harvey Weinstein hired at the recommendation of Ehud Barak to intimidate the women accusing him of serial sexual abuse and rape.

Black Cube and NSO may use different technical methods in conducting their corporate business, but their goals and clients are remarkably similar: powerful,

wealthy individuals, companies, and states that need to intimidate their enemies through surreptitious means that would embarrass them if made public.

NSO's controlling shareholder, Stephen Peel of Novalpina, who just bought the company at a $1 billion valuation, issued this statement, which only adds insult to injury:

> Founding partner Stephen Peel said Novalpina was "determined to do whatever is necessary to ensure that NSO technology is used for the purpose for which it is intended — the prevention of harm to fundamental human rights arising from terrorism and serious crime — and not abused in a manner that undermines other equally fundamental human rights".

It's a slick bit of sophistry to co-opt the term "human rights," applying it to the aspects of the company's business that the world deems legitimate while ignoring the illegitimate and dangerous uses which are the ones that bring in the most revenue from its unsavory clients. Peel further sought to enlist Amnesty in developing guidelines for NSO's work so that they would promote "enhanced respect for human rights." The idea that his company would sell malware that endangered the lives of Amnesty's staff while inviting the NGO to whitewash its business practices is appalling.

Archimedes Group

Another Israeli company got itself in hot water recently as well: an obscure firm called Archimedes Group, specializing in gun-for-hire election campaign dirty ops on behalf of African despots (aka presidential candidates). The Atlantic Council's Digital Forensic Research Lab first exposed these efforts and reported:

> The tactics employed by Archimedes Group, a private company, closely resemble the types of information warfare tactics often used by governments, and the Kremlin in particular. Unlike government-run information campaigns, however, the DFRLab could not identify any ideological theme across the pages removed, indicating that the activities were profit-driven.

Employing the underhanded tactics Cambridge Analytica and the Internet Research Agency used in the 2016 US presidential election, Archimedes spent nearly $1 million on behalf of shady political clients in countries across Africa (including Nigeria, Senegal, Togo, Angola, Niger, and Tunisia), Latin America, and Southeast Asia:

> Archimedes-linked pages pulled from the playbook of Russian interference in the 2016 U.S. presidential election, with widely amplified yet tailored messages targeting potential voters and "creating a specter of leaked information." Most impostor accounts shared a key tactic: posing as a campaigner for a particular candidate and then sharing opinions that actual supporters would find offensive.

A Jewish minister in the Tunisian government protested Archimedes's hoax posts attacking the ruling coalition. Though he did not specifically name the Israeli company, other sources have independently confirmed that Archimedes was active in Tunisian political races:

> Rene Trabelsi — the country's first Jewish minister — made the comments to a local radio station on Monday.
>
> "Tunisian parties have hired this company to launch a smear campaign against the government and the president," Trabelsi said.
>
> "Unfortunately, they are not happy to see the progress made by the government."

The company created nearly three hundred hoax accounts, which Facebook just announced it has banned.

A Facebook executive described its operations:

> The pages . . . conduct[ed] "coordinated inauthentic behavior," with accounts posting on behalf of certain political candidates, smearing their opponents and presenting as legitimate local news organizations peddling supposedly leaked information . . .
>
> The fake pages, pushing a steady stream of political news, racked up 2.8 million followers. Thousands of people expressed interest in attending at least one of the nine events organized by those behind the pages.

The company began its operations in 2017. It doesn't shy away from its real intent to manipulate political reality. In fact, it boasts that it "take[s] every advantage available in order to change reality according to our client's wishes." Currently, the company's web page consists of a home page. All the other pages were removed, but are archived here. The "Products" page has been removed entirely, including in the archive view.

Israeli media reports say that the mastermind behind Archimedes is a low-level political fixer named Elinadav Heyman. Previously, he was a political aide to the right-wing parliamentarian Anastasia Michaeli and served as a lobbyist and

foreign affairs aide in the European Parliament. He served as an intelligence officer in the Israeli Air Force.

Heyman has friends in high places in the world of Israel Lobby politics. He spoke at last year's AIPAC annual conference, addressing a panel on Israel-Africa relations alongside an Israeli foreign ministry official. He's also spoken before the World Jewish Congress.

Calcalist has also discovered several other company executives including Fabio Goldman, Yuval Harel, Uri Ben Yosef, Ariel Treiger, and Rafi Cesana.

A cyber-security expert quoted in the *Washington Post* warned:

> Archimedes' commercialization of tactics more commonly tied to governments, like Russia, [is] an emerging — and worrying — trend in the global spread of social media disinformation. "These efforts go well beyond what is acceptable in free and democratic societies," Brookie said.

As I've written before, it's no accident that the world leaders in these dirty ops tactics are Israeli companies. It stems from the country's status as a national security state, in which military-intelligence affairs are accorded almost sacred status.

High-tech products, including surveillance technology and advanced weapons, provide a major export boost to the Israeli economy. Almost all of those involved in start-ups that devise these tools learn their trade in military intelligence services like Unit 8200. Regulating or restricting such technology would mean killing the goose that's laying the golden egg — not to mention that it flies in the face of the exalted status accorded to those who protect and defend the country from security threats.

Whatever Israel chooses to do (or not do) to address these issues, the world shouldn't stand by. Otherwise, the pernicious system of cheating, spying, and dirty tricks developed by these Israeli companies will soon become normalized.

Governments around the world must not leave it to social media platforms alone to police their content. There must be strong legal penalties put in place to police such fraudulent behavior. That's why the Mueller indictments of the Internet Research Agency and its executives are welcome, though the chances of bringing any of the targets to justice are slim. There must be more such prosecutions before this behavior can be reined in.

The dirty ops campaigns mounted by Israeli companies like Archimedes, NSO, and Black Cube endanger lives and pollute democratic processes around the

world. Governments must take stronger action to regulate these activities. If they continue to sit back, there will be many more deaths like those of Khashoggi, not to mention the possibility of riots, political instability, and genocide such as Burmese Buddhist monks incited on Facebook against the Rohingya.

Amnesty International is making an excellent start by suing NSO and the Israeli defense ministry, demanding that the latter cease approving export licenses for the malware maker. But this lawsuit doesn't stand much of a chance given the carte blanche offered by the Israeli judiciary to the military-intelligence complex. Legal experts, human rights NGOs, progressive political leaders, and social media companies themselves should devise a common strategy to take on these malefactors.

WhatsApp reported the NSO hack to the Justice Department. We'll see whether it will have as much fortitude in pursuing Israeli hackers as it has in pursuing Russian and Chinese ones. I've queried WhatsApp asking if they planned to sue NSO Group for the damage the hack caused, both financially and in terms of the company's reputation. A public relations firm retained by WhatsApp refused to comment.