GlobalResearch
Center for Research on Globalization

Israel's Cyber Security Firm "NSO Group" Permits Foreign Intelligence Agencies to Spy on Human Rights Activists

By Richard Silverstein
Global Research, June 22, 2017
Tikun Olam 20 June 2017

Region: Middle East & North Africa
Theme: Intelligence, Law and Justice

The NYT's lead story recently featured a chilling story of the infamous Israeli cyber-security firm, NSO Group, whose Pegasus malware has been illegally utilized by Mexican intelligence agencies to spy on legitimate human rights and anti-corruption activists. NSO negotiates lucrative contracts with foreign governments, which purportedly use the malware to hack and control the cell phones of criminals and terrorists. The FBI used a similar tool to break into the iPhone of Rizwan Farook, the San Bernardino Islamist who murdered 15 of his work colleagues at a Christmas party.

But there's a wee problem: one person's human rights advocate is another's terrorist. In other words, there are many governments in the world who don't know the difference between the two, nor do they care. Anyone who threatens the established order is a terrorist. Bahrain used a UK malware developer to hack the phone of an exiled human rights activist. Another activist, perhaps aware of the previous episode, suspected a similar phishing attempt and immediately sent his phone to the Citizen's Lab at the University of Toronto. It discovered yet another piece of malware which would've permitted the hacking of his phone had he clicked on the link.

NSO Group co-founders Omri Lavie and Shalev Hulio (Source: Tikun Olam)

Hacking Team is another such Italy-based company, which has sold its cyber-cracking malware to governments like Morocco and the UAE. They were used to track the communications of human rights activists.

Last year, NSO entered the radar of white-hat cyber-security experts, who noted phishing

attempts against Middle East Eye journalist, Rory Donaghy. He had written articles heavily critical of the autocratic government of UAE. Cyber-sleuths were able to trace the code and domains used in the attack to NSO. The Israeli company had gone far beyond attacking a single journalist. The white-hats discovered that its code was found on 67 different servers and had infiltrated 400 individual devices. 24 of these people were UAE citizens and three were arrested shortly after they inadvertently downloaded the suspect code. A fourth was convicted in absentia of insulting the country's ruler.

Then Ahmed Mansoor, another UAE dissident who'd previously been beaten and robbed by regime goons, sent the white-hat researcher a new phishing exploit. That permitted cyber-detectives to identify with certainty that NSO was directly responsible for the code and malware used in the would-be attack. And it was far the most sophisticated such attack in the history of cyber-hacking: that was the world's introduction to Pegasus.

Economists find that these companies are drilling for cyber-gold, with the market value for these services reaching $5-billion per year. NSO charges a flat $500,000 fee plus $650,000 for each device hacked. That's a lucrative business model!

All of these black-hat companies hide behind a veneer of respectability. One claims that it only sells its products to NATO member countries (its code was used in exploits in Morocco and other Arab *non-NATO* countries). NSO claims that it explicitly forbids its clients from using Pegasus against anything other than criminal and terrorist targets. Then it coyly adds that it can't be expected to know or police who its clients target once the malware is in the hands of the end-user.

This is akin to a gunmaker selling a man a weapon who's used them in the past to kill people, then saying it can't be responsible for how he uses it after they sell it to him. Or alternatively, it's like pharmaceutical companies which manufacture opioids. Though there are legitimate uses for these drugs, once the drugs leave the plant the companies look the other way as doctors and dealers distribute the product to addicts who shouldn't have access to them. Everyone makes money off this scam from Big Pharma to the prescribing doctors. The fact that the drugs wreak havoc throughout homes and towns in America is collateral damage.

Given that NSO is selling code, rather than physical weapons or drugs, we can indeed expect it to be able to track how its products are used by clients. The truth is that NSO doesn't *want* the trouble of having to do so. Nor does it want to know who and how it is used. But the world must crack down on these practices. It must criminalize this behavior.

Doing so will be difficult. In Israel, for example, cyber-security is a huge export bonus to the economy. The government is happy to authorize export licenses for NSO, despite the uses to which its products are put. Israel doesn't exercise oversight regarding the high-tech industry. If necessary, it looks the other way. It doesn't even restrain arms dealers selling advanced Israeli weaponry containing U.S. components to our adversaries. NSO is a perfect expression of the amorality of Israeli commerce.

But perhaps Israel isn't just "looking the other way" in these cases . Perhaps the NSOs of Israel are doing precisely what the government wishes them to. Perhaps Israeli cyber hacking tools are instruments of state. If you examine the company's client list you will find many of the Arab states Israel is attempting to cultivate in its efforts to sabotage the

Palestinian cause. What better way to peel off an authoritarian state from such allegiance than by doing favors for its intelligence agencies; hoping the favor will be returned one day when Israel needs it.

Remember, as well that the Israeli defense ministry approves licenses for the export of all products which have a security component. Meaning the government has direct and complete control of the export process.

NSO's engineers, the ones who developed the most sophisticated and powerful malware programs on the market, are veterans of the IDF's Unit 8200. They learn their trade on Palestinian victims, deemed the enemy of the Israeli state. Sometimes the target might be a terrorist. But sometimes he or she might be a legitimate political or community leader whom Israeli intelligence has deemed vulnerable to blackmail. Perhaps they're gay, or having an affair, or have a child with cancer. All are prime recruits as informers for Israel's Shabak. This is how Israel's most elite hackers learn their craft.

NSO Group offices in Herzliya (Source: Tikun Olam)

There is no oversight, no ethical code governing such behavior. For Israel, the code-word is "security *uber-alles*." The same sordid ethos infects NSO operations in the world. Go where the money is. All the rest be damned.

The closeness between NSO and the Israeli state may be seen in one security consultant's characterization of the Pegasus malware used to jailbreak iPhones:

> "Apple had never seen anything like this—ever. This was an incredibly sophisticated nation-state attack, kind of breathtaking in its scope. This took a herculean effort on their part to patch it so fast. It was Katy-bar-the-door over there."

It's important to note that he called Pegasus a product of a "nation-state attack." *Not* a product of a private company. In other words, a private company, no matter how large or sophisticated would simply not have the resources or skill-set to coordinate so many different elements of this jailbreak tool. Only a huge military SIGINT outfit like Unit 8200 could accomplish such a monumental task.

And NSO was able to commercialize this military-intelligence tool for use by other intelligence agencies around the world. In effect, Israel was exporting not just its products but its flagrant disregard for human or civil rights; and as in the case of other counter-terror strategies it's pioneered like drone assassinations and targeted killing, it's exported a blatant disregard for human life itself.

Let's also not forget that Israel is the fifth largest arms exporter in the world and first on a per capita population basis. It didn't get to this point by scrupulously investigating all the uses of the weapons it was selling, and the dirty pedigrees of many of the nations to whom it was selling.

Featured image: MIT Technology Review
