Beyond Pegasus: The Bigger Picture of Israeli Cyber Spying

Beyond Pegasus: The Bigger Picture of Israeli Cyber Spying

by **James Corbett**, *The Corbett Report*
August 7, 2021

We have been told to live in mortal fear of online hackers and, as the "cyber pandemic" narrative ramps up, the fear-mongering over Chinese, Russian and even North Korean cyberwarriors is going into overdrive.

Strange, then, given this climate of non-stop cybersecurity hysteria, that we rarely hear mention of one of the world's confirmed cyberhacking superpowers: Israel. Just as Israel's nuclear arsenal is the worst kept secret in the world, it seems that mention of Israel's cyber arsenal is strictly forbidden in the maintream press. But it is now undeniable that Israel is running one of the most sophisticated, pervasive and influential cyberhacking operations in the world.

The official silence on Israel's cyber espionage changed last month when the story of Pegasus—a piece of military-grade spyware developed by Israeli surveillance firm NSO Group—made headlines for all the wrong reasons. The software, as *Haaretz* and other MSM half-truth peddlers inform us, is able to hijack the phones of its victims, recording from the phone's cameras and microphone and collecting location data, call logs and contacts, all without the target's knowledge. And, as the consortium of dinosaur media publishers who were

given access to this treasure trove of information report, it is being used by "oppressive regimes" to target "180 journalists" and even scoop up personal contact details of national misleaders like French President Emmanuel Macron and Pakistani Prime Minister Imran Khan.

But there are some very important things you never learned about the Pegasus story in the dinosaur media's coverage of it and, if you *do* rely on the lamestream media for your knowledge, there are a *lot* of things you won't know about the history of Israeli cyberspying. So today, let's take a look at the issue of Israel's high tech espionage.

One severely underreported fact about the Pegasus story shines a light on the much larger story of Israeli cyber spying. According to *Forbes*, the co-founders of the NSO Group, Omri Lavie and Shalev Hulio, "are believed to be alumni of Israel's famous Unit 8200 signals intelligence arm, as are many of the country's security entrepreneurs." NSO's first investor, Eddy Shalev, asserts otherwise ("They didn't come from intelligence"). Hulio himself, meanwhile, spins a rather tall tale about randomly meeting people in line at a cafe who were able to put him in touch with the tech geek who would become the company's first employee and who, Hulio allows, "may have served in Unit 8200." This unlikely story stretches the bonds of credulity so far that it prompts even ynetnews to note that "Some in Israel's defense and intelligence community were skeptical of Hulio's fanatic tale." But the fact that Unit 8200 is in the picture at all is itself telling.

For those who don't know, Unit 8200 is the branch of the Israel Defense Force responsible for signals intelligence, i.e., Israel's equivalent of the NSA. Supposedly founded in 1952 (or was it the 1930s?), the unit was not officially acknowledged until the early 2000s, when stories of the incredible (and incredibly illegal) acts of cyber espionage it has perpetrated over the decades began to be publicized.

One particularly high profile piece of work bearing Unit 8200's fingerprints was Stuxnet, the military-grade cyberweapon that specifically targeted Iran's nuclear enrichment facility at Natanz. It has long been known that Stuxnet was co-developed by the United States and Israel, but it was *New York Times* correspondent David Sanger who revealed that the worm was actually worked on by Unit 8200.

But beyond the cyberweapons and (still largely classified) military exploits of the unit itself is the undeniable fact that a surprisingly large number of high-profile tech startups and Silicon Valley ventures in recent years have been founded by "ex" members of 8200. One such "ex" member, Avishai Abrahami, asserted in 2016 that "there are more than 100 guys from the unit that I personally knew who built startups and sold them for a lot of money" including a team of ten who "created companies where the average market cap is a half-billion dollars." (Abrahami himself created cloud-based web developer Wix, whose market cap currently sits at over $16 billion.)

From communication companies like AudioCodes and Viber to cybersecurity companies like Argus and CheckPoint to GPS navigation software services like Waze, the prevalence of Unit 8200 alumni in the private tech sector has received so much press that even trade publications have been forced to report on the matter, noting that the Israeli military is increasingly out-sourcing cybersecurity and intelligence projects to companies "that in some cases were built for this exact purpose."

Other than NSO, some troubling startups from the "ex"-8200 crowd include:

- **Carbyne911**, a tech startup marketed as a "a Next Generation Call Handling platform" for 9-1-1 and emergency call centers, that, as an in-depth 2019

exposé from *Narrativ* revealed, was founded and run by a gaggle of Israeli military and intelligence officials (including a Unit 8200 alumni) and was bankrolled by the likes of Jeffrey Epstein, Ehud Barak and Peter Thiel.

- **Comverse Infosys**, which made wiretapping software used by US law enforcement that contained—as Carl Cameron reported in a quickly-quashed series on Israeli spying for Fox News in 2001—"a back door through which wiretaps themselves can be intercepted by unauthorized parties" and whose main product (known as "the Logger") was later admitted to be "based on the Unit's [8200's] technology."
- **Cybereason**, a cybersecurity firm founded by "ex"-Unit 8200 member Lior Div and stacked "with many of the unit's members coming from organizations like the NSA and Unit 8200" that, as Whitney Webb has extensively reported, ran a Doomsday Election Simulation for the US government and has Gained Access to the US Gov't's Most Classified Networks.
- And **Toka**, a spyware firm co-founded by Ehud Barak and headed by the former chief of the Israel Defense Forces Cyber Staff, which, as Whitney Webb has also extensively reported, is aiming to provide "a one-stop hacking shop for governments" specializing in IoT ("Internet of Things") devices.

In fact, this represents only a small fraction of Unit 8200's infiltration of the private cybersecurity space in recent years, so if you're unfamiliar with the topic you have a lot to catch up on.

But, given that (as Whitney Webb rightly observes), "The abuse of Pegasus software in this very way has been known for several years" and "other Israeli companies with even deeper ties to Israel's intelligence apparatus have been selling software that not only provides the exact same services to governments and intelligence agencies but purports to go even

farther," the sudden influx of MSM attention to the Pegasus story is curious.

One clue to the mystery of this sudden interest comes in the form of a little tidbit that is embedded in all the MSM articles on the Pegasus scandal (like this one from our friends at *The Bezos Post*):

Forbidden Stories, a Paris-based journalism nonprofit, and Amnesty International, a human rights group, had access to the list [of phones hacked by the Pegasus software] and shared it with the news organizations, which did further research and analysis. Amnesty's Security Lab did the forensic analyses on the smartphones.

Forbidden Stories? What on earth is that?

Well, according to their website: "Forbidden Stories fosters collaboration among journalists to make visible and impactful the work of reporters who can no longer investigate," including gathering "a consortium of local and international media outlets in order to investigate on a large scale." This "consortium" reads like a who's who of worldwide dinosaur media outlets, including *Le Soir* in Belgium, *The Toronto Star* in Canada, *France Télévisions*, *Radio New Zealand*, *Reuters*, *bellingcat*, *The New York Times* and literally dozens of other mockinbird outfits around the world.

And who funds this venture? The usual gaggle of "independent" "charitable" foundations, of course, including UNESCO and (you guessed it) George Soros' Open Society Foundations.

So why are these big hitters and known liars collaborating on this release of information about a known Israeli military front masquerading as a commercial spyware company? If you said "Because it's a limited hangout!" then give yourself a cookie. I think you're right.

But what is this hangout aiming to accomplish, exactly?

Theories abound. Bernard over at Moon of Alabama, for example, has this take on the situation:

The U.S. often uses 'intelligence' as a kind of diplomatic currency that keeps other countries dependent on it. If the Saudis have to ask the U.S. for snooping on someone it is much easier to have influence over them. NSO is disturbing that business. There is also the problem that the first class spying software NSO is selling to somewhat shady customers might well fall into the hands of some big U.S. adversary.

The 'leak' to Amnesty and Forbidden Stories is thus an instrument to keep some monopolistic control over client regimes and over spying technology. (The Panama Papers were a similar kind of U.S. sponsored 'leak', only in the financial field.)

I think Bernard is right to compare this Pegasus story to the Panama Papers story, which was also cross-reported by an international consortium of mockingbird media dinosaurs. In fact, we could even cast our minds back to a much earlier story that was similarly reported by a gaggle of mainstream media conspirators from around the world: the Iraq War Logs, which that totally above-board, crusading secret-exposer Julian Assange made available exclusively to the truth tellers at *The Guardian*, *The New York Times*, *Le Monde* and his other favourite MSM outlets.

However, the idea that this whole story is an attempt by the US "to keep some monopolistic control over client regimes and over spying technology" rings hollow. After all, if the US were really trying to muscle Israel out of the cyberspying arena by dishing the dirt on the NSO Group, what about the many, many, many examples of similar or even worse spying by other Israeli companies (just some of which are listed above)? How would the exposure of this one piece of software upend the entire section of the global cybersecurity industry that has been seeded by the Unit 8200 gang?

No, in this case I believe it's more likely that the powers-that-shouldn't-be are throwing the NSO Group and its Pegasus software under the bus for the sake of *protecting* the larger Israeli military cyberwarfare industry, not undermining it. After all, the NSO Group has been in the crosshairs of cyber privacy activists for years, with even the all-powerful Blackstone Group having to back out of a deal to acquire a 40% stake in the company after it was revealed that Pegasus had been used by the Mexican government to spy on its own citizens.

The NSO Group is already tainted. By "exposing" this story about the company (one that was already known and reported), they are able to take attention away from the Cybereasons, Tokas and other companies that are performing similar functions for the Unit 8200-infested cybersecurity industry under much deeper cover.

Undoubtedly there is more to this story that will come out in bits and pieces in these controlled "Forbidden Stories" reports. But rather than shining a light on the larger question of Israeli cyber espionage and how deep the rabbit hole really goes, the intense focus on this one piece of spyware from this one company will only serve to obscure that story.

Connect with James Corbett

cover image credit: Prettysleepy / pixabay