GlobalResearch
Center for Research on Globalization

Rogues and Spyware: Pegasus Strikes in Spain

By Dr. Binoy Kampmark
Global Research, May 15, 2022

Region: Europe
Theme: Intelligence

***

Weapons, lacking sentience and moral orientation, are there to be used by all. Once out, these creations can never be rebottled. Effective spyware, that most malicious of surveillance tools, is one such creation, available to entities and governments of all stripes. The targets are standard: dissidents, journalists, legislators, activists, even the odd jurist.

Pegasus spyware, the fiendishly effective creation of Israel's unscrupulous NSO Group, has become something of a regular in the news cycles on cyber security. Created in 2010, it was the brainchild of three engineers who had cut their teeth working for the cyber outfit Unit 8200 of the Israeli Defence Forces: **Niv Carmi, Shalev Hulio and Omri Lavie.**

NSO found itself at the vanguard of an Israeli charm offensive, regularly hosting officials from Mossad at its headquarters in Herzliya in the company of delegations from African and Arab countries. Cyber capabilities would be one way of getting into their good books.

The record of the company was such as to pique the interest of the US Department of Commerce, which announced last November that it would be adding NSO Group and another Israeli cyber company Candiru (now renamed Saito Tech) to its entity list "based on evidence that these entities developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers."

In July 2021, the Pegasus Project, an initiative of 17 media organisations and civil society groups, revealed that 50,000 phone numbers of interest to a number of governments had appeared on a list of hackable targets. All had been targets of Pegasus.

The government clients of the NSO Group are extensive, spanning the authoritarian and liberal democratic spectrum. Most notoriously, Pegasus has found its way into the surveillance armoury of the Kingdom of Saudi Arabia, which allegedly monitored calls made by the murdered Saudi journalist **Jamal Khashoggi** and a fellow dissident, **Omar Abdulaziz**. In October 2018, Khashoggi, on orders of Saudi Arabia's **Crown Prince Mohammed bin Salman**, was butchered on the grounds of the Saudi consulate in Istanbul

by a hit squad. NSO subsequently became the subject of a legal suit, with lawyers for Abdulaziz arguing that the hacking of his phone "contributed in a significant manner to the decision to murder Mr Khashoggi."

Spain's **Prime Minister Pedro Sánchez, Defence Minister Margarita Robles, Interior Minister Fernando Grande-Marlaska,** and 18 Catalan separatists are the latest high-profile targets to feature in the Pegasus canon. Sánchez's phone was hacked twice in May 2021, with officials claiming that there was at least one data leak. This was the result of, according to the government, an "illicit and external" operation, conducted by bodies with no state authorisation.

Ironically enough, Robles herself had defended the targeting of the 18 Catalan separatists, claiming that the surveillance had been conducted with court approval. "In this country," she insisted at a press conference, "no-one is investigated for their political ideals."

The backdrop of the entire scandal is even more sinister, with Citizen Lab revealing last month that over 60 Catalan legislators, jurists, Members of the European Parliament, journalists and family members were targeted by the Pegasus spyware between 2015 and 2020. (Citizen Lab found that 63 individuals had been targeted or infected with Pegasus, with four others being the victims of the Candiru spyware.) Confirmed targets include Elisenda Paluzie and Sònia Urpí Garcia, who both work for the Assemblea Nacional Catalana, an organisation that campaigns for the independence of Catalonia.

The phone of Catalan journalist Meritxell Bonet was also hacked in June 2019 during the final days of a Supreme Court case against her husband **Jordi Cuixart**. Cuixart, former president of the Catalan association Òmnium Cultural, was charged and sentenced on grounds of sedition.

The investigation by Citizen Lab did not conclusively attribute "the operations to a specific entity, but strong circumstantial evidence suggests a nexus with Spanish authorities." Amnesty International Technology and Human Rights researcher Likhita Banerji put the case simply. "The Spanish government needs to come clean over whether or not it is a customer of NSO Group. It must also conduct a thorough, independent investigation into the use of Pegasus spyware against the Catalans identified in this investigation."

Heads were bound to roll, and the main casualty in this affair was the first woman to head Spain's CNI intelligence agency, Paz Esteban. Esteban's defence of the Catalan hackings proved identical to that of Robles: they had been done with judicial and legal approval. But she needed a scalp for an increasingly embarrassing situation and had no desire to have her reasons parroted back to her. "You speak of dismissal," she stated tersely, "I speak of substitution."

While the implications for the Spanish government are distinctly smelly, one should not forget who the Victor Frankenstein here is. NSO has had a few scrapes in Israel itself. It survived a lawsuit by Amnesty International in 2020 to review its security export license. But there is little danger of that company losing the support of Israel's Ministry of Defence. In Israel, cybersecurity continues to be the poster child of technological prowess, lucrative, opaque and distinctly unaccountable to parliamentarians and the courts.

*

Note to readers: Please click the share buttons above or below. Follow us on Instagram, Twitter and Facebook. Feel free to repost and share widely Global Research articles.

Dr. Binoy Kampmark *was a Commonwealth Scholar at Selwyn College, Cambridge. He currently lectures at RMIT University. He is a regular contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com*

Featured image is from Indian Punchline

Comment on Global Research Articles on our Facebook page

Become a Member of Global Research

Articles by: **Dr. Binoy Kampmark**