WHO PROFITS The Israeli Occupation Industry

COMPANY FEATURE

NSO GROUP: TECHNOLOGIES OF CONTROL

MAY 2020

With the mounting use of surveillance technologies to monitor and control populations worldwide, there has been a proliferation in cyber technology companies in the global market, where the Israeli hi-tech sector has become a dominant player. Surveillance tech firms have also found ways to capitalize on the crisis caused by COVID-19.

This company feature will present the activities of NSO Group, a private Israeli cyber company with a record of human rights violations, shedding light on the militarized nature of Israel's hi-tech sector. It will highlight the company's dealings with oppressive regimes, as well as its new coronavirus data analytics system, already piloted in several countries.

The Israeli Cybersecurity Sector: Privatization of Military Knowledge

Israel's cybersecurity ecosystem is ranked second globally, and is a significant sector within the Israeli tech industry, totaling some $6.5 billion in annual exports.[1] In 2018, Israeli cybersecurity companies raised $1.19 billion, accounting for almost 20% of global VC investment in that sector.[2] In

[1] Global Start-Up Ecosystem Report 2019. *Start-Up Genome*.

[2] Ibid.

2019, investments continued to rise, reaching $1.88 billion.[3]

Established in 2010, NSO Group is one of the largest Israeli hi-tech companies, specializing in spying,[4] with annual revenues estimated at $200-250 million according the available publications.[5] NSO Group is emblematic of a prevalent trend in the Israeli hi-tech sector, whereby military knowledge, developed in a context of prolonged occupation to enhance the brutal matrix of control over an occupied population, is commercialized and extended to civilian enterprises. The Israeli military enables hi-tech workers and entrepreneurs to benefit from knowledge acquired during military service, and this integration has played a role in shaping the focus of the hi-tech sector on homeland security and surveillance technologies.[6]

A glimpse into the histories of NSO's founders, employees and senior advisors reveals this tight-knit relationship between the Israeli hi-tech industry and the state military apparatus. Shalev Hulio, a co-founder of NSO, served as "a Major in the Israeli army's Search and Rescue unit and continues to serve in the army reserve and has been involved in a number of search and rescue operations in both Israel and abroad".[7] Senior advisor Daniel Reisner served as the head of the Israeli army's International Law Department and was responsible for advising the Israeli leadership on "Israeli-Palestinian relations" and "counter-terrorism operations."[8] Buky Carmeli, another senior advisor, is the former head of Israeli Ministry of Defense (IMOD) Cyber Defense division.[9] In addition, some of the company's employees were veterans of Unit 8200, the Military Intelligence Directorate's main information gathering unit,[10] which is an integral part of the mechanism of military control over Palestinians.[11]

The knowledge acquired from many years of serving in the Israeli state military apparatus is converted by hi-tech companies to cyber technologies that are marketed globally. In the case of NSO, such knowledge is used, among other things, to supply governments and security agencies with technologies to surveil so-called 'suspects' through cellular phones, using highly invasive spyware such as *Pegasus*, which penetrates security features in cellular systems without the user's knowledge or permission.[12] The spyware is believed to be "the world's most invasive mobile spy kit."[13]

[3] Ibid.

[4] Zureik, Elia. "Settler Colonialism, Neoliberalism and Cyber Surveillance: The Case of Israel." *Middle East Critique* (2020): 1-17.

[5] Hazani, Golan (2017). "NSO's Spyware Divides 850 Million NIS in Dividends. *Calcalist.* Last accessed at: 12 April 2020 (available in Hebrew). https://www.calcalist.co.il/internet/articles/0,7340,L-3714021,00.html

[6] Gordon, N. (2009). The Political Economy of Israel's Homeland Security. *The New Transparency*. P.17

[7] https://www.nsogroup.com/about-us/board-of-directors/

[8] https://www.nsogroup.com/about-us/senior-advisors/

[9] Ibid.

[10] Wenkert, Amarelle (2019). "New York Times: Emirati Surveillance Firm Poached NSO Employees". *Calcalist*. Last accessed at: 12 April 2020. https://www.calcalistech.com/ctech/articles/0,7340,L-3758992,00.html

[11] "Israeli Intelligence Veterans` Letter to Netanyahu and Military Chiefs- in Full" (2014). *The Guardian*. Last accessed at:12 April 2020. https://www.theguardian.com/world/2014/sep/12/israeli-intelligence-veterans-letter-netanyahu-military-chiefs

[12] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018) "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries". Citizen Lab Research Report No. 113, University of Toronto, September

[13] Brewster, Thomas (2016). "Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones with a Single Text". *Forbes*. Last accessed at: 12 April 2020. https://www.forbes.com/

Pegasus Software: A Tool for Tyrants

An investigation by Citizen Lab revealed that NSO Group spying technology was allegedly used in at least six countries with a history of tracking human rights activists: Bahrain, Kazakhstan, Mexico, Morocco, Saudi Arabia, and the United Arab Emirates.[14]

According to the investigation, in 2016, dozens of Mexican lawyers, journalists and human rights defenders were targeted by the Mexican government using NSO's Pegasus spyware. During the same year, Pegasus spyware was used to target the UAE activist Ahmad Mansour. The Israeli Defense Export Control Agency (DECA) authorized three deals in the UAE, for the total amount of $80 million.[15]

It has been reported that the company also provided the Saudi government with the spyware to spy on the journalist Jamal Khashoggi before his murder.[16] An associate of Khashoggi filed a suit against the company in an Israeli court, asking to issue an order prohibiting the company from selling its spyware, and halt its installation in Saudi Arabia. The plaintiff has also demanded NIS 600,000 in damages.[17] In October 2019, Amnesty International uncovered targeted digital attacks using Pegasus against two Moroccan human rights defenders.[18] In October 2019, the company was sued by Facebook, which claimed that the company attempted to hack 1,400 "target devices" and steal information from human rights activists, journalists and others using the WhatsApp app.[19] In the lawsuit, WhatsApp claims that servers controlled by NSO rather than government clients were an integral part of the way the hacks were executed.[20]

Profiteering from a Public Health Crisis

The COVID-19 pandemic has provided an opportunity for governments to conduct mass surveillance on populations. This in turn provides cyber companies with an opportunity to profit from the public health crisis.

In March 2020, Bloomberg reported that NSO developed a new product that has the ability analyze huge volumes of data to map people's movement.[21] According to a report by Motherboard, the data is displayed in a user interface that allows analysists "to track where people go, who they meet, for how

sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/#52bd7a0c3997

[14] Marczak, B., Scott-Railton, J., McKune, S., Abdul Razzak, B., & Deibert, R. (2018) "Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries". Citizen Lab Research Report No. 113, University of Toronto, September

[15] Bergman, Ronen (2019). Weaving a Cyber Web. *Ynet News*. Last accessed at: 12 April 2020. https://www.ynetnews.com/articles/0,7340,L-5444998,00.html

[16] Business and Human Rights Resource Center. NSO Group Allegedly Provided Software to Saudi Govt. to Spy on Khashoggi; Citizen Lab who Reported it In Turn Targeted by Undercover Agents. January 2019.

[17] Shahaf, Tal (2018). Saudi Friend of Slain Journalist Sues NSO in Israeli Court. *Globes*. Last accessed on 16 April 2020. https://en.globes.co.il/en/article-saudi-friend-of-murdered-journalist-sues-nso-in-israeli-court-1001263262

[18] Amnesty International. Israel: Stop NSO Group Exporting Spyware to Human Rights Abusers. January 2020. https://www.amnesty.org/en/latest/news/2020/01/israel-nso-spyware-revoke-export-license/

[19] "Facebook Sues Israeli Co NSO for Allegedly Hacking WhatsApp". *Globes*. Last accessed at: 12 April 2020. https://en.globes.co.il/en/article-facebook-sues-israqeli-co-nso-for-allegedly-hacking-whatsapp-1001305184

[20] WhatsApp: "Israeli Firm `Deeply Involved` in Hacking Our Users. *The Guardian*. 29 April, 2020 (last accessed at 3 May 2020).

[21] Ackerman, G.; Benmeleh, Y (2020). Israeli Spyware Firm Wants to Track Data to Stop Coronavirus Spreading. *Bloomberg*. Last accessed at: 12 April 2020. https://www.bloomberg.com/news/articles/2020-03-17/surveillance-company-nso-supplying-data-analysis-to-stop-virus

long, and where."[22] The tool tracks citizens by assigning them random IDs, which the government can de-anonymize at any given moment.[23] According to media reports, the product is already being piloted in a dozen countries.[24]

On 29 March 2020, Israeli Minister of Defense Neftali Bennett published a national plan to fight coronavirus based on a collaboration with the private sector, stating that "This is why we have established in the IMOD in collaboration with the IDF [sic] and civilian companies a centralized data system, into which we will 'spill' all the data […] The system is ready to be operationalized. It is the most advanced system in the world, in my opinion, and will be replicated later (gladly!) all over the world."[25] An investigation by TheMarker revealed that the civilian company in question is NSO.[26]

The proposed plan was announced following the decision of Israeli government to authorize mass surveillance of citizens as part of its COVID-19 response, and the use of technologies previously used to "combat terrorism."[27] The decision also included the participation of Israel's General Security Service (GSS or Shin Bet) and the extension of its powers to gather private information of citizens.[28] Tracking coronavirus patients and those around them is hardly a difficult feat for the Israeli authorities, who have at their disposal an arsenal of surveillance technologies employed to maintain an intricate system of control and tested on an occupied population.[29]

[22] Franceschi- Bicchierai, Lorenzo (2020). We Saw NSO's Covid-19 Software in Action, and Privacy Experts are Worried. *Vice*. Last accessed on: 12 April 2020. https://www.vice.com/en_us/article/epg9jm/nso-covid-19-surveillance-tech-software-tracking-infected-privacy-experts-worried

[23] Ibid.

[24] Ibid.

[25] National Action Plan to Overcome Coronavirus (available in Hebrew).

[26] Goichman, Rafaela (March). Ministry of Defense Collaborated with NSO to Rate the Possibility of Catching Coronavirus. Last accessed on April 22, 2020 (available in Hebrew). https://www.themarker.com/technation/.premium-1.8722025

[27] Konrad, Edo (2020). Equating Coronavirus with Terror, Netanyahu Turns Surveillance Powers on Israelis. *+972 Magazine*. Last accessed at: 12 April 2020. https://www.972mag.com/netanyahu-surveillance-coronavirus/

[28] Arab Joint List, Adalah turn again to Supreme Court, demanding halt to Shin Bet's invasive surveillance of citizens in struggle against coronavirus: https://www.adalah.org/en/content/view/9957

[29] For more information:

The Lab (2013), Documentary Film, CBC Radio Canada, France Télévisions, Gum Films. Directed by Yotam Feldman.
Or Who Profits. Big Brother in Jerusalem's Old City: Israel's Militarized Visual Surveillance System in Occupied East Jerusalem. November 2018.