aulamediterrània
Programa Interuniversitari de l'IEMed.

n.160 22/5/2024

ISRAEL'S TECHNOLOGY OF OPPRESSION

ARTICLE

Shir Hever*

A series of discoveries by investigative journalists have revealed six developments in offensive surveillance technology: spyware that remotely takes control of devices, location tracking by exploiting loopholes in cellular networks, armies of AI-generated social media avatars, mass facial recognition networks for control of entire populations, metadata exploitation through ads for digital surveillance, and finally the mass-production of targets of military strikes through AI.

This dystopian list concerning the abuse of technology in violating human rights describes the tools by which governments through their intelligence services wage espionage war against each other and keep their own populations under control. The technologies are also offered as a package by private companies; in February 2023, through their "Story Killers" project, Forbidden Stories revealed a network of Israeli companies which provide disinformation services to the highest bidders. These services, which take cyber warfare to another level, include campaigns of character assassination, dissemination of fake news, and rigging elections and referendums.

Already in 2018, the Cambridge Analytica scandal was revealed, showing how mass surveillance can be a powerful tool for manipulating public opinion. The Archimedes Group, an Israeli company, was a key technology supplier to Cambridge Analytica, but whistleblower Brittany Kaiser claimed in her testimony that she was not able to remember any of the names of the Israeli Archimedes Group employees. The company has therefore been able to escape accountability.

When disinformation campaigns fueled by digital surveillance are provided by private companies, it almost exclusively involves Israeli companies. Israeli companies did not invent the technology, but no other state allows companies in the private sector to offer military-grade surveillance for sale because of the tremendous potential strategic risk that could occur.

Israel's unique model, offering officers early retirement from military careers, granting rewards in the form of second-career opportunities in the private military and security market, has created a culture in which state regulators turn a blind eye to private companies offering military-grade surveillance technology for profit. Over 80% of surveillance employees in the private sector are graduates of Israel's intelligence units, most famously the unit 8200, which is notorious for using surveillance to blackmail Palestinians into becoming collaborators.

*Manager of the Alliance for Justice between Israelis and Palestinians

Cyber warfare in general and disinformation in particular are very dangerous weapons. They undermine the democratic process when utilized to influence elections by spreading rumors and false information, and they can also become lethal. Incitement based on false information spread through avatars has led to the murder of Indian journalist Gauri Lankesh in 2018. After her murder, the avatars were deleted and the culprits covered their tracks.

Forbidden Stories, together with Amnesty International and Citizen Lab, exposed in July 2021 the way that Israeli companies sell spyware to hack phones and computers of journalists, human rights activists, lawyers and politicians. The "Pegasus Project" revealed how technology, which was tested on Palestinian civilians, was used to enhance repression and grave human rights violations worldwide. In October 2021, Israel accused six Palestinian civil society organizations of terrorism, based on alleged evidence that it collected through spyware. Although forensic analysis confirmed that the Israeli NSO Group infected the phones of the employees of these organizations, Israel failed to provide any credible evidence and the EU sharply criticized the disinformation attempt.

After being tested on Palestinians, Israeli spyware was used as currency to win favor with authoritarian regimes around the world, in what is called "spyware diplomacy".

In 2023 Amnesty International published its report "Automated Apartheid" on the use of massive surveillance through facial recognition software and thousands of cameras (stationary and mobile) deployed by the Israeli security forces to keep Palestinians, especially in Jerusalem and Hebron, in a state of panopticon-like complete surveillance and invasion of privacy even in their own homes.

In 2023 Forbidden Stories investigated how the disinformation industry works. A collaborative effort of journalists from different countries led them to the Israeli city/settlement of Modi'in. The undercover journalists contacted an Israeli disinformation company and were offered a disinformation campaign to influence an election for just six million Euros.

The new revelations about the disinformation industry are a different facet of Israel's mercenary espionage sector. Disinformation companies are a "one stop shop" selling spyware, spy services, hacking emails and messaging software, spreading fake news and otherwise destroying the credibility of political candidates. They do this mostly through the use of fake avatars – profiles of artificial people who never existed. The companies steal pictures of real people but assign them different names, social media accounts and even electronic wallets with real money. The disinformation companies also hire operatives in target countries in order to be able to verify phone numbers and addresses as they build these fake avatars. "Team Jorge", one of the Israeli disinformation companies, has an army of 40,000 such avatars, created with the help of AI.

Aside from "Team Jorge" and the Archimedes Group, the list of Israeli disinformation companies named in the recent investigation include Voyager Labs, Percepto, Cognyte,

Verint, S2T Cyberspace, and Demoman. The Story Killers investigation revealed that Israeli companies spread disinformation in Angola, Burkina Faso, Colombia, France, Indonesia, Malaysia, Mexico, Nigeria, Senegal, Singapore, Sri Lanka, Tunisia and more.

According to Israeli law, companies are forbidden from exporting Israeli military-security technology without approval by the Israeli Ministry of Defense, even if the companies are not registered in Israel. Nevertheless, Tal Hanan of "Team Jorge" told the undercover Forbidden Stories journalists that he can do as he pleases, unregulated by the Israeli authorities. He listed only three countries which he refuses to operate: Russia, the US and Israel. The owner of Israel's spyware Intellexa Tal Dilian, graduate of the Israeli intelligence unit 81, made the same claim.

The Israeli Ministry of Defense operates a special counterintelligence unit called the MALMAB to keep tabs of graduates of the Israeli security organizations. In early March, the MALMAB cracked down on the Israeli spyware company NFV for selling unauthorized spyware. Tal Hanan claims that he has been in the business of disinformation since 1997, operating from Israel. Tal Dilian hired Nir Ben Moshe, former head of the MALMAB, to serve on the board of Intellexa, ensuring a free hand by the Israeli Ministry of Defense to act in the shadows, selling Israeli technology but claiming to do so without Israeli supervision.

The Israeli disinformation industry, alongside the spyware and corporate espionage industries, attempts to implement the experience of enforcing apartheid and military occupation for customers from all over the world. Mostly, this implementation has failed. The Israeli espionage company Black Cube has been exposed multiple times by its victims. The spyware industry has soured Israel's foreign relations, and even the disinformation company "Team Jorge" was exposed for planting fake information with French BFMTV host Rashid M'barki, who was fired for publishing the information without verifying it.

Another company, Percepto, headed by Lior Chorev, a former political advisor to Ariel Sharon and Ehud Olmert, did not balk at hiring the services of a known antisemite in order to distribute smears against the Red Cross in the service of a customer in Burkina Faso, just as he did not balk at working for Israeli war criminals. Among their clients is also the Mexican millionaire Tomás Zerón, wanted in Mexico for charges of kidnapping and torture. Israeli billionaire Dan Gertler, who has a controversial mining empire in the Democratic Republic of Congo (DRC) and is accused of plundering the nation's natural resources and using disinformation campaigns to protect himself from criticism, has hired Lior Chorev to do public relations work for him, as the US authorities are investigating his DRC operations.

Tech giants such as Facebook and Twitter are complicit in the crimes committed by disinformation companies. Meta, formerly known as Facebook, sells data on its users for profit. Both Facebook and Twitter profit from the spread of fake news and disinformation, yet they crack down on human rights activists instead by silencing them, especially if they are Palestinians. Moreover, when a disinformation scandal is exposed, the tech giants quickly delete the fake avatars. They allegedly do so to protect users from disinformation, but in fact they help the disinformation companies cover their tracks.

Israeli governments have allowed the disinformation industry to flourish for two decades as part of a deliberate policy of security-state diplomacy. The gains of such exports are short-term and are recklessly irresponsible in the long run. Although the research by Forbidden Stories is very important in exposing this industry and the extent of damage it causes, this is not enough.

Just as the dangerous combination of spyware to collect and spread information and artificial intelligence to generate mass amounts of fake avatars has given birth to the disinformation industry, so has the combination of facial recognition technology with AI to analyze surveillance footage created the so-called "assassination factory", which the Israeli military is using in the Gaza Strip. As Israeli journalist Yuval Avraham of 972 Magazine revealed, the Israeli assault on the Gaza Strip is the first time in which AI has been weaponized as a weapon of war.

As AI and facial recognition technologies are both deeply biased technologies with inherent flaws generated by the bias of their users, the results were catastrophic. The Israeli intelligence units, which used to produce 5-6 targets per day in Israeli bombing of Gaza, were replaced by AI, which produced over a hundred targets per day, of much lower quality. It has escalated the Israeli attacks on Gaza, which were periodic war crimes within a framework of an illegal occupation, to the level of genocide. This point must be repeated: AI has become a weapon of genocide.

In December the Palestinian digital rights organization 7amleh published a report on Israeli digital repression tools. It listed spyware, facial recognition, disinformation and AI. In the midst of genocide, which is committed with physical weapons, the decision by a Palestinian organization to focus on the surveillance and disinformation technology is not coincidental.

On October 18, Israel bombed the Al-Ahli Baptist Hospital in the northern Gaza Strip, and promptly launched a disinformation campaign to shift the blame to Palestinians for allegedly bombing their own hospital. This campaign was based on spyware as well as manipulation of social media discourse, coordinated by the private companies mentioned above. The genocide perpetrated by Israel is only possible as long as international, especially western, support is forthcoming, and therefore Israel invests as many resources in disinformation as it spends on explosives.

If this threat is not highlighted, and mechanisms are not established to prevent the weaponization of AI, the unchecked spread of spyware and the impunity of disinformation companies, then there is no reason to believe that the atrocities of Gaza will be an isolated incident. Also used here in Barcelona to repress the Catalan independence movement, what starts with political oppression and violation of privacy can escalate into incitement through disinformation and eventually murder.