**Israeli surveillance**

Haythem Guesmi

Thursday, Oct 07, 2021

It is not a coincidence that Israel is home to two of the leading tech companies producing highly invasive spyware today. After all, the Israeli state has been using Palestinians as guinea pigs to perfect its mercenary surveillance technologies for decades. It has, for example, long been using state of the art facial recognition software at checkpoints to screen Palestinians in the West Bank. According to the Citizen Lab, NSO Group and Candiru recruit their staff from the ranks of Israel’s intelligence services.

There is another reason why Israel is a world leader in producing surveillance tech: the Israeli state is not interested in holding its surveillance industry accountable for its excesses. Even after the Pegasus scandal, which led several international NGOs to call for the Israeli surveillance industry to be regulated, there is no sign that companies like NSO Group and Candiru will face any sanction or serious investigation for selling their products to authoritarian, corrupt and even violent governments and putting the lives, livelihoods and reputations of tens of thousands of journalists, politicians, activists and dissidents at risk.

International institutions and global powers are also not interested in pressuring Israel to keep its powerful surveillance industry in check, or taking legal action directly against these Israeli tech companies. Indeed, in the immediate aftermath of the Pegasus scandal, the United Nations and the European Union voiced their concerns about the Pegasus spyware, but fell short of launching a legal case against the company that developed and sold it.

The lack of accountability surrounding Israel’s surveillance industry is a threat to independent journalism, political participation and activism around the world, and especially in the MENA region.

As Pegasus and other military-grade spyware produced by Israel’s surveillance industry turn smartphones and computers into surveillance devices, activists, politicians and journalists across the Arab world are becoming aware that every private photo they take, every phone conversation they have, and every message they send could one day be used against them. This is particularly true for those who are critical of Israel’s genocidal policies against the Palestinians or those who are taking a stance against the many human rights and international law violations of Israel and its powerful allies in the region.

This is not paranoia or hyperbole. Israel has for decades spied on and blackmailed Palestinians who resisted its occupation and oppression. It has even tried to spy on its closest allies including, as revealed by news magazine Politico in 2019, the Trump administration in Washington. It provided governments that support its foreign policy ambitions with technologies that allowed them to spy on dissidents, rights activists, and political opponents.

There is no reason to doubt that the apartheid state is using, and will continue to use, all spyware at its service to collect data on and consequently blackmail activists, politicians and even common citizens acting and speaking against its interests. What happened to [Ghada] Oueiss and many other pro-Palestine Arabs will become a standard tactic used against the future generations of MENA politicians and activists critical of Israeli policies.

Some may claim none of this is anything to worry about for those who have ‘nothing to hide’ or those who are ‘doing nothing wrong’. But an action does not need to be ‘wrong’to be politically and socially damaging. As was seen in the case of Oueiss, something as inconspicuous as a swimsuit photo can easily be turned into something much sinister by those intent on doing harm. As is the case with Israel’s many other policies in the region, spreading fear is the point.

Israel’s growing surveillance empire, which serves not only Israel but also its allies, means that politicians, activists and journalists in the MENA region can no longer separate their work and public personas from their private lives.

It means young Arab politicians and activists are facing a disturbing choice: they will either self-censor and keep quiet about Israel’s many crimes to protect themselves and their loved ones from terrifying hacks and leak attacks, or they will give up their right to online privacy and stop using services and products that are central to modern life as well as political and civic activism just to be able to continue their work without fear of Israeli blackmail.

Pegasus, and undoubtedly other Israeli spyware we have not yet heard about, have turned our phones and computers into surveillance devices at the service of the Israeli state and its allies.

There is little hope that the international community will act to regulate the Israeli surveillance industry anytime soon.

Excerpted: ‘Israeli surveillance and the end of politics as we know it’

Aljazeera.com