GlobalResearch
Center for Research on Globalization

Pegasus Project: Why I was Targeted by Israeli Spyware

My work to expose the crimes of the Saudi regime led to a hacking attempt on my phone. Today, I am overwhelmed by feelings of vulnerability and intrusion.

By Madawi Al-Rasheed
Global Research, July 22, 2021
Middle East Eye 20 July 2021

The Orwellian prediction finally came true. I knew it was only a matter of time before the Saudi regime tried to hack my phone, using Pegasus software manufactured by the private Israeli security company NSO Group.

This development highlights the consolidation of a new axis of evil: Israel, Saudi Arabia and the UAE have become a chorus of malicious powers aiming to stifle activism and the quest for democracy in the region. Israel provides knowledge; the others provide funds.

> "I have spent more than half my life writing, researching and teaching. You wouldn't expect me to be hacked. But such professional activities are a crime in Saudi Arabia"

The privatisation of the Israeli security apparatus, and the mushrooming of private companies founded by ex-defence and ex-Mossad agents, is a threat not only to Palestinians in Israel, Gaza and the occupied West Bank, but also to all Gulf citizens, with Israeli spyware sold to dictatorships across the Arab world.

In return, Israel gains access to the inner intelligence circles and deep states of the Gulf – enabling it to hold them hostage for a long time to come. Israel supports Gulf autocracies, thinking that this guarantees its own security forever. But Israel is wrong.

Normalisation with Israel is not only immoral because of the Palestinian plight; it is also an existential threat to all Gulf nationals seeking political reform in their own countries. The so-called "only democracy in the Middle East" has so entrenched its apartheid system that no propaganda can salvage it, and strong public objections to Arab regimes' normalisation with Israel will only intensify in the months and years ahead.

Saga of surveillance

The UAE plays a key role in the saga of surveillance by Israeli private companies. Saudi Crown Prince Mohammed bin Salman has fallen under the spell of Mohammed bin Zayed, his UAE counterpart. Forget the "tallest building, busiest airport and ministries of tolerance and happiness" – which are at the core of UAE propaganda – and remember that bin Zayed is bin Salman's mentor.

The two are united by their hatred of democracy, political diversity, freedom of speech and

human rights. Both are now key to an axis of evil overseen by malicious Israeli technology, whose alleged raison d'etre is to help governments catch criminals and terrorists. Yet, it is being used against peaceful activists.

Forbidden Stories, a Paris-based NGO specialising in defending journalists and human rights activists, obtained more than 50,000 telephone numbers targeted globally by Israeli malware on behalf of NSO clients, mainly governments. They alerted various media outlets, and with the support of Amnesty International, launched the Pegasus Project.

The findings showed that in April 2019, there was an attempt to hack my phone, but it was unsuccessful. While this is a relief, I am overwhelmed by feelings of vulnerability and intrusion.

To obtain evidence from the Pegasus Project, I had to submit the contents of my phone – in which my private and professional life was stored – to their technology team.

I sat in front of a computer screen for three hours, watching my virtual life travel to the Amnesty International lab, where a search for malware was conducted. I received evidence of the failed April hacking attempt the same day.

Controlling the narrative

As a British citizen of Saudi origin, I have spent more than half my life writing, researching and teaching. You wouldn't expect me to be hacked. But such professional activities are a crime in Saudi Arabia, where the regime is determined to control the narrative about the past, present and future.

My crime is that I punctured this narrative, using academic research skills and access to Saudis whose voices remain muted. All my research has focused on giving a voice to the voiceless, which inevitably involves interviewing Saudis inside and outside the country. My debunking of official Saudi lies bothers the regime, which has spared no opportunity to tarnish my reputation, accusing me of being an agent of western governments, Turkey, Iran, Qatar, and previously Libya and Iraq.

Saudi government agents murdered Jamal Khashoggi in Istanbul in October 2018 (AFP)

In the 1990s, the regime targeted me with direct threats of violence – but with the advent of the internet, such threats have become virtual, propagated by regime agents. Hacking my phone is only the latest episode.

In 2014, my Twitter account was hacked in search of sensational scandals, and possibly clandestine plots with other Saudi exiles. The hackers must have been disappointed not to find any of this, but they did expose my private conversation with Sheikh Awad al-Qarni, a key Islamist figure who sent me greetings and asked me not to augment my criticism of the Islamist movement's silence when prominent Saudi human rights leaders were detained.

Regime spies launched a campaign to discredit Qarni for sending a direct message to an unveiled woman, such as myself. Qarni has been in prison for several years.

Lives in danger

I never had anything to hide, as everything I knew was documented and published in books and articles. I had no secrets, but this was not the point. I cherished my privacy and loathed the Saudi intrusion into my life. I also worried about those who communicate with me from within the country, as their lives could be in danger.

Among the charges against Mohammed al-Otaibi, a human right activist, was storing my books and articles on his computer. He is still in prison. It is my responsibility to protect those who confide in me and want their voices to be heard.

> "While the April 2019 assault on my device was unsuccessful, I am sure there will be other attempts in the future"

The murder of Jamal Khashoggi in October 2018 coincided with greater Saudi surveillance of exiles in Britain, Canada and elsewhere. The shock over the gruesome details of chopping up a peaceful journalist was compounded by fears of hacking. This was the first time exiles had heard of NSO helping the Saudis to hack the phone of a young exile based in Canada, Omar al-Zahrani, who had communicated with Khashoggi about establishing a media platform to debunk Saudi propaganda.

The financial cost of securing my phone was colossal, but it was worth it. While the April 2019 assault on my device was unsuccessful, I am sure there will be other attempts in the future.

Back in 2019, I was involved in discussions with other exiles in three countries about forming a political party, which could explain the attempt to infiltrate my phone at that time. The regime wanted more details about who would sponsor such a project – and who the culprits were. The project materialised on 23 September 2020, the day the kingdom celebrates its national day, as a small group of activists, including myself, announced the establishment of the Saudi National Assembly (NAAS). Yahya Asiri, the general secretary, was hacked, and his name appears in the Pegasus files.

Standing against oppression

I moved from academia to political activism because the Saudi regime committed heinous crimes, and the lives of exiles, including my own, were in danger. The Saudi regime targeted

me when I was an academic, and again after I became an activist. Such attacks will surely continue in the months and years ahead.

In April 2019, I was also writing a book on state-society relations. The villain was none other than bin Salman, who has detained hundreds of Saudis and precipitated the flight of scores more.

I was baffled by western media depictions of the prince as a modern reformer, while Saudi prisons were bulging with innocent prisoners of conscience, women were campaigning against discrimination, and a young diaspora was coming together around the globe. My book, *The Son King*, was definitely a faux pas.

In 2019, a new virtual Saudi opposition-in-exile was beginning to be formed, standing against oppression and dictatorship. NAAS relies on social media to connect and exchange ideas, making it extremely vulnerable, as the murder of Khashoggi and the hacking of activists' phones has demonstrated. In the wake of the Pegasus Project revelations, NAAS will surely revert to old methods of mobilisation, meetings and activism.

Thanks to Israeli malware, UAE complicity and Saudi intrusions, exiles will have to search for secure methods to share information and to mobilise. As many have taken refuge in the US, Canada, Britain and across Europe, these states have a responsibility to protect them from Saudi surveillance. Otherwise, there is a real risk the Khashoggi saga could be repeated.

Diplomacy must be activated to stop the axis of evil from spreading more fear, apprehension and possibly murder – and if that doesn't work, sanctions should be pursued, at the very least in Britain, where two of the founders of NAAS reside.

The views expressed in this article belong to the author and do not necessarily reflect the editorial policy of Middle East Eye.

*

Madawi al-Rasheed is visiting professor at the Middle East Institute of the London School of Economics. She has written extensively on the Arabian Peninsula, Arab migration, globalisation, religious transnationalism and gender issues. You can follow her on Twitter: @MadawiDr

---

Articles by: Madawi Al-Rasheed