United Nations A/HRC/48/NGO/24

General Assembly

Distr.: General
10 September 2021

English only

Human Rights Council
Forty-eighth session
13 September–1 October 2021
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

Written statement* submitted by Institut International pour les Droits et le Développement, a non-governmental organization in special consultative status

The Secretary-General has received the following written statement which is circulated in accordance with Economic and Social Council resolution 1996/31.

[18 August 2021]

* Issued as received, in the language(s) of submission only.

Pegasus Project: The United Arab Emirates Building a superpower of cyber espionage

Monday 19 July 2021, an international consortium of news outlets reported that several authoritarian governments including Mexico, Morocco and the United Arab Emirates used spyware developed by an Israeli surveillance company called NSO Group to hack into the phones of thousands of their most vocal critics, including journalists, activists, politicians and business executives.

Named "Pegasus", the NSO-developed spyware is able to hack into and secretly take control of a mobile phone, allowing access to all data, messages and even turn on a phone's microphone or camera remotely, without leaving a digital fingerprint. Following a massive data leak of 50,000 phone numbers of potential surveillance targets of phone numbers, French-based Forbidden Stories undertook an investigation with a consortium of 17 media groups, including The Guardian and Le Monde, revealing that the software was abused by foreign governments – customers of NSO – to spy on "persons of interest".

Researchers at Amnesty, whose work was reviewed by the Citizen Lab at the University of Toronto,[1] found that NSO can deliver Pegasus by sending a victim a link which when opened infects the phone, or silently and without any interaction at all through a "zero-click" exploit, which takes advantage of vulnerabilities in the iPhone's software. Citizen Lab researcher Bill Marczak said in a tweet that NSO's zero-clicks worked on iOS 14.6, which until today was the most up-to-date version. The Moblie Verification Toolkit, or MVT, works on both iPhones and Android devices, but slightly differently.

while NSO and its customers insist that it is meant to target global terrorism and organised crime networks. The records revealed that at least 13 heads of state, diplomats, prominent human rights lawyers, activists and political opposition were targeted by ten foreign government clients of NSO. Among them, at least 10,000 phone numbers were listed by the UAE, making the Gulf federation the second most massive user of the spyware, behind Mexico.

Geopolitics, human rights and family dissidents

Data thus suggest that political and military figures in the Gulf and the wider Middle East were spied upon through their phones at the request of the UAE and/or Saudi Arabia, which also took interest in using the Israeli spyware.

The Lebanese President Michel Aoun, his son-in-law and ex-foreign minister Gebran Bassil, the PM-designate Saad Hariri, the Central Bank Governor Riad Salame, as well as Abbas Ibrahim, chief of the main security service and several Hezbollah executives are the highest ranking officials whose details appear in the lengthy list investigated by Le Monde.

Iraq: the list includes President Barham Saleh, Prime Minister Adel Abdel-Mahdi, and intelligence chief Mustafa Al-Kadhimi, who has since become head of government.

Several commanders of Hachd Al-Chaabi (Popular Mobilisation), a coalition of Shiite militias who are seen as the Islamic Republic of Iran proxies were also targeted by the Israeli spy programmes. Among them, Abu Mahdi Al-Mohandes, an Iraqi lieutenant close to Iranian General Qassem Soleimani, with whom he was killed, in an American strike in January 2020.

Yemen: the "persons of interest" list for the Emirati services, including the son and cabinet director of President Abd Rabbo Mansour Hadi.

Qatar, the Emir of Qatar Sheikh Tamim al-Thani was targeted from 2016.

Earlier this year, Toronto University watchdog CitizenLab had revealed that the spyware had been used to hack the phones of at least 36 Al-Jazeera journalists. The journalists' phones

[1] The citizen lab, University of torinto: The Great iPwnJournalists Hacked with Suspected NSO Group iMessage 'Zero-Click' Exploit. By Bill Marczak, John Scott-Railton, Noura Al-Jizawi, Siena Anstis, and Ron Deibert, December, 2020.

were hacked by four Pegasus operators, attributed to Saudi Arabia and the UAE. CitizenLab revealed earlier this year that New York Times journalist Ben Hubbard had also been targeted by Pegasus, a case reported by the Council on Foreign Relations (CFR).

Mathew Hedges, a British doctoral researcher focusing on the security strategies of the UAE and conducting field research and interviews, was also under Emirati surveillance. He was arrested and detained for several months in 2018.

Rodney Dixon, a prominent London-based human rights lawyer and Hedges' representative, also figures among the United Kingdom of Great Britain and Northern Ireland phone numbers of more than 400 people who appear to have been selected by the UAE government. These include a member of the House of Lords, the chief executive of the International Institute for Strategic Studies (IISS) defence think tank and the editor of the Financial Times.

Agnes Callamard, the UN Special Rapporteur on extrajudicial, summary or arbitrary executions who led an investigation into Khashoggi's 2018 murder, was herself targeted online.

The UK hacking list also suggests that the spyware was used for intra-family disputes. The phones of Princess Haya and Princess Latifa of Dubai were hacked along with those of their close associates and confidants. Princess Haya is embroiled in a bitter custody case against her ex-husband, the Emir of Dubai, Sheikh Mohammed bin Rashid al-Maktoum. His daughter, Princess Latifa, has made two unsuccessful attempts to escape from Dubai since 2018, where she is allegedly being held against her will.[2]

The attacks not only puts a renewed focus on the shadowy world of surveillance spyware, but also the companies having to defend against it. Apple rests much of its public image on advocating privacy for its users and building secure devices, like iPhones, designed to be hardened against the bulk of attacks. But no technology is impervious to security bugs. In 2016, Reuters reported that UAE-based cybersecurity firm DarkMatter bought a zero-click exploit to target iMessage, which they referred to as "Karma." The exploit worked even if the user did not actively use the messaging app.

Building a superpower of cyber espionage

Investing billions of dollars and human capital into strengthening its "digital national security", the UAE has become, in the past decade, one of the world leaders in cyber-intelligence and digital espionage. According to Le Monde, this activism bears the mark of Crown Prince of Abu Dhabi Mohammed Bin-Zayed (MBZ), a military man by training, known for his very flexible interpretation of national security and his taste for clandestine operations. Under his supervision, the UAE passed from the creation of the "Dread" unit in 2008 (Development Research Exploitation and Analysis Department, later renamed the "Raven project"), to the contract with NSO in 2016, developing a policy of "industrial scale surveillance" within a few years.

Conclusion

Human rights organizations have long raised concerns about the UAE's aggressive acquisition of cyber-surveillance technology and its misuse to target journalists, human rights defenders, and other perceived critics.

IRDG is too concerned about the results of the Pegasus spyware report and the link relation between this program and some countries, including the United Arab Emirates. We express our strong dissatisfaction and warn against the role that the UAE can play within the umbrella of the so-called technology and innovation in EXPO 2020 from being a major trap for many international companies, governments, businessmen and civil society organizations, knowing

[2] Pegasus Project: The UAE conduct "industrial scale surveillance",by Stella Athanasoulia, 26 July 2021.

that Israel, the UAE’s ally, will also be present with its technologies in Expo 2020 as one of the prominent workers in technology.

IRDG is too worried about UAE's troubling record of abusing technology to launch attacks on human rights defenders and other critics of the government. Amid the official promotion for Expo 2020 - designed to showcase Dubai as a hub of technological innovation, cultural tolerance, and visionary leadership - it is important to remember the UAE's record of crushing any form of dissent expressed offline or online, frequently in the name of security.

IRDG asks the Human Rights Council to raise the awarness for Expo 2020 visitors who should be aware of the draconian cyber-security laws in the UAE, used in the past and recent against foreigners.

IRDG consider that the Participation in international events in the UAE has a high risk of privacy without addressing human rights concerns.

Despite some limited efforts at regulating the surveillance trade, a lot more needs to be done by companies themselves currently turning a blind eye to how their technology might be used by governments like the UAE to silence independent voices.

Expo 2020 serves to promote the UAE's brand as modern, tech-savvy and open for business and investment, while they are using these technology in spying and and spreading of grave violationsthat the UAE witnessing and heate feelings among human rights defenders.

Initially aimed at monitoring “irritating” voices such as human rights activists, journalists and researchers, this cutting-edge surveillance technology progressively became a paramount tool for an aggressive and muscular Emirati foreign policy within the Middle East and beyond.