ALQST for Human Rights
Contact@ALQST.ORG 02073851311 Unit 24.7, Coda Studios, 189 Munster Rd, Fulham,
ALQST.ORG ALQST_ORG London SW6 6AW | Registration no: 09093387

PEGA - Committee to investigate the use of Pegasus surveillance spyware
European Parliament
60 rue Wiertz
B-1047 – Bruxelles

RE: Pegasus cyberattacks against human rights activist on British soil

24 January 2023

Distinguished members of the PEGA Committee,

I would like to bring to your attention the case of **Mr Yahya Assiri**, a prominent Saudi human rights activist who while resident in the United Kingdom has been the victim of several cyberattacks by the Saudi authorities using Pegasus spyware.

Mr Assiri is a founding member and former Secretary General of the National Assembly Party ("NAAS"), a Saudi opposition party most of whose members are currently in exile. He is also the founder of ALQST for Human Rights, an independent non-governmental organisation that documents human rights violations in Saudi Arabia, and Diwan London, a discussion forum on the Arabian Peninsula aimed at consolidating the values of justice and freedom.

In 2018 and 2020 two of Mr Assiri's mobile telephones were targeted by the Saudi authorities with spyware known as "Pegasus" acquired from Q Cyber Technologies Ltd and/or NSO Group Technologies Ltd, an Israeli technology firm specialising in cyber intelligence services and products. Mr Assiri's devices were infected with Pegasus by the Saudi authorities in collaboration with NSO while he was in the United Kingdom. The covert installation of Pegasus onto Mr Assiri's devices enabled the Saudi authorities secretly and remotely to collect, modify, extract and record all information stored on and communicated via his devices. The Saudi authorities would have been able to control the camera and audio recording facilities on the devices so as to secretly monitor and record activities in the vicinity of the devices. The infection of his devices thus resulted in a wide-ranging invasion of Mr Assiri's privacy and endangered all the people with whom he had been communicating via these devices.

Mr Assiri subsequently brought a legal claim in the United Kingdom against the Kingdom of Saudi Arabia for (i) breach of the General Data Protection Regulation; (ii) misuse of private information; (iii) harassment, contrary to the Protection from Harassment Act 1997; and (iv) trespass to goods. The interference with Mr Assiri's devices by Pegasus spyware violated his rights under the GDPR and/or Data Protection Act 1998; misused his private information; subjected him to harassment, contrary to sections 1 and 3 of the PHA 1997; and committed trespass to his goods. As a result of these unlawful acts Mr Assiri suffered damage to or loss of tangible property,

distress, anxiety, loss of privacy and loss of amenity and autonomy. This damage to or loss of tangible property (and other unlawful acts) was caused by acts or omissions in the United Kingdom.

In May 2018 Mr Assiri was sent a malicious text message containing a link to Saudi Arabia-focused Pegasus installation domains that matched other attacks on Saudi dissidents by the Saudi authorities. Independent analysis of the data on Mr Assiri's devices was conducted by Citizen Lab, which confirmed that Mr Assiri's devices had been infiltrated by Pegasus, and that this occurred on 11 July 2020 with a further attempt on 26 July 2020. There was also evidence of a further (undated) Pegasus infection.

Mr. Assiri was in the United Kingdom on 11 and 26 July 2020 when the confirmed Pegasus infiltrations occurred. Around this time, he was working on a number of issues of acute interest to the Saudi authorities, including:

- work with the United Nations on documenting instances of enforced disappearance, including some involving torture at the hands of Saud al-Qahtani (a close advisor to Crown Prince Mohammed Bin Salman until the murder of Jamal Khashoggi);
- advocating for the imposition of sanctions on KSA officials;
- supporting the challenge brought by Campaign Against Arms Trade against UK government licensing of arms sales to KSA;
- investigating and publishing stories about the death of Dr Abdullah al-Hamid, a leading activist who had died on 23 April 2020 in detention in KSA, and Saleh al-Shehi, a journalist who died on 19 July 2020 shortly after being unexpectedly released from detention in KSA;
- arranging an annual conference of Saudi activists;
- working on the case of Jamal Khashoggi;
- taking preparatory steps towards the launch of the NAAS party; and
- efforts to encourage a UK boycott of the Saudi-hosted G20.

At each and all of the times Mr Assiri's devices were infiltrated with Pegasus, they contained information that was confidential, private and personal to him and others in Saudi Arabia. Mr Assiri used the devices for phone calls, text and WhatsApp messaging, e-mail, internet browsing and other purposes relevant to his private and professional life. He stored extremely sensitive and confidential information on the devices, including court documents, contact information for people in Saudi Arabia, photos of identification documents of human rights defenders in Saudi Arabia, consent forms from individuals in Saudi Arabia for the purposes of advocacy before the United Nations Human Rights Council, information about activists' families, friends and colleagues, and information about how to reach his contacts if they disappeared. The Saudi

authorities' potential acquisition of this data was and is nothing short of catastrophic for Mr Assiri and his contacts in Saudi Arabia.

Requests

Given the United Kingdom was part of the European Union until 2020 and remains a neighbouring and partner country to the Union, we kindly ask that you consider the information provided in this brief and urge you to:

1) organise a hearing with human rights activists who have become victims of cyber surveillance with the Pegasus technology; and

2) set up a litigation fund for victims of cyberattacks.

And to push the European Commission to:

3) put in place stricter EU-wide export control policies on all dual use goods;

4) establish a moratorium on the sale, acquisition, transfer and use of spyware; and

5) put in place blacklists for technology companies selling digital tools used for repression, contrary to the national security interests of the EU, including the NSO Group.

Thank you for your consideration of this matter. The ALQST team would be pleased to answer any questions you may have.

Sincerely,

Julia Legner
Executive Director
ALQST for Human Rights