LAYLA MORAN MP

Liberal Democrat MP for Oxford West and Abingdon
www.laylamoran.com
Unit C5, Grange Court, Abingdon Science Park, Barton Lane, Abingdon, OX14 3NB

The Rt Hon. Boris Johnson MP
Prime Minister
10 Downing Street
London
SW1A 2AA
By email to: Pmpost.ext@no10.gov.uk

CC: Private.Office@fcdo.gov.uk; sofs-privateoffice@mod.gov.uk; PSMinisterCleverlyAction@fcdo.gov.uk; mindp-privateoffice@mod.gov.uk

11th November 2021
Our ref: LM44456

Dear Prime Minister,

We are writing in light of the recent decision by the Biden administration to blacklist Israeli spyware firm NSO Group to urge you to take similarly robust action to sanction this company and introduce measures to protect people living in the UK from further cyberattacks.

On 3 November 2021, the U.S. Department of Commerce announced that NSO Group would be added to the U.S. 'Entity List' based on evidence that foreign governments used their spyware products to "maliciously target" civil society figures around the world and enabled them to "conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent."

Use of NSO Group's Pegasus Software on UK Soil

NSO Group's activities are of particular concern given the findings of ongoing investigations by *The Guardian* and other media outlets which revealed that the company's Pegasus spyware was used by the governments of Saudi Arabia, the United Arab Emirates (UAE) and Bahrain to conduct cyberattacks in the UK. These attacks targeted Gulf nationals living in the UK, many of whom are refugees in this country, as well as UK citizens.

Among the most serious hacking incidents were attempts to undermine the judicial system in this country by Sheikh Mohammed Al Maktoum, the ruler of Dubai. In October 2021, it was revealed that the High Court had ruled that Sheikh Mohammed interfered with British justice by hacking the phone of his ex-wife, Princess Haya of Jordan and her solicitors, including British peer Baroness Shackleton, during a legal dispute over custody of their children. The court described the hack as "abuse of power" by Sheikh Mohammed and "interference with the process of this court and the mother's access to justice."

Governments in the Gulf have also used NSO products to target activists living in the UK. In July 2021, *The Guardian*'s 'Pegasus Project' investigations revealed further cyber attacks targeting UK-based activists by the Emirati government, including Sayed Ahmed Alwadaei, a refugee and Director of Advocacy at the London-based Bahrain Institute for Rights and Democracy and Alaa Al-Siddiq, former Executive Director of ALQST, a UK-based NGO which campaigns for human rights in Saudi Arabia, who died tragically in a car accident earlier this year. The recently appointed editor of the Financial Times and the newspaper's first female editor, Roula Khalaf, was also revealed to have been named as a potential target for surveillance with Pegasus software in 2018. Investigations by CitizenLab, a research group at the University of Toronto, further found that Pegasus was used to infiltrate mobile devices of

LAYLA MORAN MP
Liberal Democrat MP for Oxford West and Abingdon
www.laylamoran.com
Unit C5, Grange Court, Abingdon Science Park, Barton Lane, Abingdon, OX14 3NB

a further three Bahraini activists currently living as refugees in the UK, while in 2019 the government of Saudi Arabia was found to have hacked the phones of Saudi satirist Ghanem al-Masarir, who is a refugee in the UK.

In August 2021, UK legal firm Bindmans announced that they had been instructed to proceed with investigating claims on behalf of a group of individuals based in the UK targeted by foreign governments using Pegasus, including Alwadaei, UK peer Baroness Manzila Pola Uddin and Raghad Altikriti, President of the Muslim Association of Britain, as well as prominent academics, human rights activists and civil society leaders. Baroness Uddin stated that if there was spying on members of parliament it would amount to "a great breach of trust" which "contravenes our sovereignty" and raises the question of whether the UK government was aware.

UK Government's Failure to Act

These cyberattacks represent egregious breaches of domestic and international human rights law, including Article 8 of the Human Rights Act 1998 and Article 17 of the International Convention on Civil and Political Rights prohibiting "arbitrary or unlawful interference" with an individuals "privacy, family, home or correspondence." Despite this, we are concerned that your government has failed to publicly condemn the actions of either NSO Group or the Saudi, Emirati and Bahraini governments or take substantive action to protect UK nationals and residents, including those living under British protection as refugees, from cyber attacks.

The decision not to condemn these attacks is particularly concerning given they were conducted by Gulf Cooperation Council (GCC) states closely allied with the UK government. As a parliamentary report published by the All-Party Parliamentary Group on Democracy and Human Rights in the Gulf revealed earlier this year, Saudi Arabia, Bahrain and the UAE are among six GCC states who have benefited from at least £53.4 million pounds from the British taxpayer in technical and military support since 2016 through the Integrated Activity Fund (IAF) and its successor, the Gulf Strategy Fund (GSF). Both of these funds have received sustained criticism for their lack of transparency and recipients of IAF/GSF funding in Bahrain and Saudi Arabia have also been implicated in serious human rights abuses and war crimes.

In addition, between 2015 and 2019 the UK government sold millions of pounds worth of spyware and other surveillance equipment to Gulf regimes. Despite recent compelling evidence that such technology has been misused by GCC states to conduct both internal and transnational repression, earlier this year the government announced plans to use GSF funding to establish a "cyber ambassador" to help "Gulf partners to defend themselves against cyber security attacks.". While the government states that such cooperation will "benefit […] UK national security" and "provid[e] opportunities for UK companies to export cyber security products and services", the cyberattacks referenced above appear to show a blatant disregard by these GCC states for both UK and international law and suggest therefore that the continued supply of surveillance equipment and services, as well as of advanced military and technical training and equipment to Saudi Arabia, the UAE and Bahrain, may in fact pose a serious threat to our national security.

Our requests

When announcing the decision to blacklist NSO Group and another Israeli spyware firm Candiru, U.S. Secretary of Commerce Gina M. Raimondo stated that the action is "part of the Biden-Harris Administration's efforts to put human rights at the center of U.S. foreign policy,

LAYLA MORAN MP
Liberal Democrat MP for Oxford West and Abingdon
www.laylamoran.com
Unit C5, Grange Court, Abingdon Science Park, Barton Lane, Abingdon, OX14 3NB

including by working to stem the proliferation of digital tools used for repression." In light of this, and further to the stated intent in the Integrated Review for the UK to be a force for good in the world by defending human rights, we urge you to take a similarly human rights-focused approach to foreign policy by taking the following actions:

- Follow the example of the US Government in backlisting the NSO Group, by imposing a trade sanction upon the company, and ensure there is much tighter supervision on the licensing of relevant software in compliance with international human rights law;
- Suspend all UK spyware licenses and cybersecurity contracts to Gulf nations implicated in cyberattacks in the UK, namely the UAE, Saudi Arabia and Bahrain, pending an independent investigation;
- Suspend GSF funding to GCC states pending an independent review into the human rights implications of said funding, per the recommendation of the APPG on Democracy and Human Rights in the Gulf report published in June 2021; and
- Make representations to the governments of the UAE, Saudi Arabia and Bahrain in order to publicly raise serious concerns over their roles in cyberattacks carried out in the UK using NSO Group's Pegasus spyware.

Yours sincerely,

Layla Moran MP, Liberal Democrat Foreign Affairs Spokesperson[1]
Brendan O'Hara MP, Chair of the All-Party Parliamentary Group for Democracy and Human Rights in the Gulf
Andy Slaughter MP
Paula Barker MP
Lloyd Russell Moyle MP
Richard Burgon MP
Martyn Day MP
Lord Scriven
Baroness Bennett of Manor Castle
Baroness Jones of Mouslecoomb

[1] Declaration of Interest: 5 January 2021, received £3,000 from Bindmans LLP, 236 Gray's Inn Road, London WC1X 8HB, for work done as a member of a detention review panel. Hours: 40 hrs. (Registered 19 January 2021)
https://publications.parliament.uk/pa/cm/cmregmem/211101/moran_layla.htm