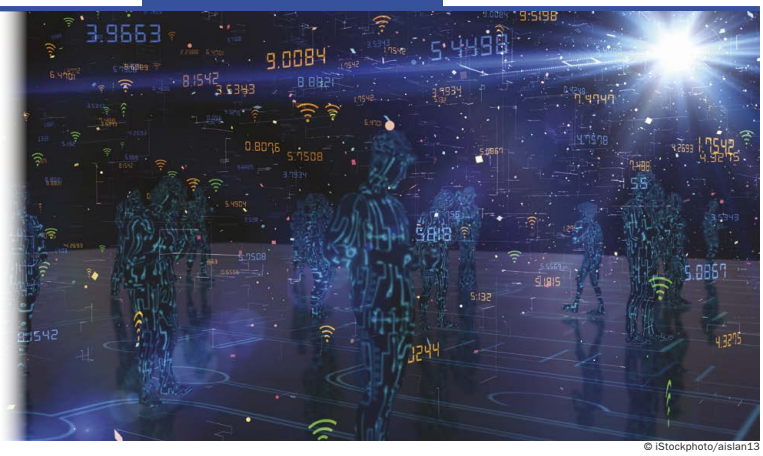
Every breath you take, every move you make…

Flavia Kenyon discusses the dangers of cyber espionage & global insecurity



© iStockphoto/aislan13

IN BRIEF

- An unregulated market lacking legal scrutiny and transparency.
- The impact of Pegasus: a powerful and pernicious spyware product.
- Holding spyware companies accountable.

According to Privacy International more than five hundred private companies are currently selling spyware products to governments in a cyber security market expected to be worth $300bn by 2025, a market that is unregulated and lacks legal scrutiny and transparency.

Surveillance of individuals—often journalists, activists, opposition figures, critics, and others exercising their right to freedom of expression—has been shown to lead to arbitrary detention, oppression, sometimes to torture and possibly to extrajudicial killings.

The most powerful and pernicious spyware product on the market today is 'Pegasus', developed by Israel's NSO Group. Earlier this year, UK private equity firm Novalpina Capital acquired majority ownership of the NSO group.

Pegasus

Pegasus penetrates security features in popular operating systems, such as WhatsApp, and silently installs the malware on a target's phone without the user's knowledge or permission. Once Pegasus is installed it begins to harvest the target's private data, including passwords, contact lists, calendar events, text messages, and live voice calls. The 'operator' can turn on the phone's camera and microphone to capture activity in the phone's vicinity, (even when the phone is switched off), and use the GPS function to track a target's location and movements. Never before has surveillance reached such heights of intrusion into an individual's personal data, little wonder then that Pegasus is classified as a 'weapon', and is subject to special export licensing laws.

There are legitimate applications for Pegasus. It is a valuable weapon in combatting serious organised crime and terrorism. In 2016 it helped in the capture of Mexican drugs baron, El Chapo. But the Mexican government went on to use it for spying on political opponents, journalists, and human rights defenders.

Citizen Lab

The Citizen Lab—a team of cyber researchers at the University of Toronto—has published numerous reports about the abuses carried out by NSO Group spyware in the last couple of years as a result of being sold to governments with questionable human rights records. In 2018 they identified Pegasus as responsible for attacks in 45 countries, including Mexico, Bahrain, Saudi Arabia, the United Arab Emirates, Canada, the United Kingdom, and the United States. Some of the victims are UK nationals, targeted because of their political views. They include a human rights blogger and a lawyer at Amnesty International, Saudi and UAE dissidents living in exile in the UK and in Canada.

To date there has been no legal remedy for these victims and the attacks have remained unaccounted for.

In May 2019, WhatsApp identified and shortly thereafter fixed the vulnerability that enabled attackers to inject commercial spyware onto phones simply by ringing the number of a target's device.

In October 2019, WhatsApp publicly attributed the attacks to the NSO Group, and is currently suing the NSO Group through the US federal court. This is expected to become a landmark case with far reaching consequences for the international spyware market and a much needed regulatory framework.

Sensational

From an evidential standpoint, the most sensational finding of the Citizen Lab researchers is that Pegasus was used against a friend of murdered Saudi journalist, Jamal Khashoggi. Unable to infect Mr Khashoggi's phone directly, Pegasus was used to infect the phone of human rights activist Omar Abdulaziz, who was residing in Canada at the time, as a way of harvesting information on Khashoggi himself. The two men's WhatsApp conversations were being spied upon, thus giving Saudi authorities confidential information about Mr Khashoggi's plans for social media activism, and possibly allowing his location data to be used to follow him in the months leading up to his assassination.

It appears there may be an evidential link between the WhatsApp attack by Pegasus and the conspiracy to kill Mr Khashoggi. If it can be proved that the misuse of NSO spyware by the Saudis played a part in bringing about the conspiracy to kill Mr Khashoggi then the maker/supplier, the NSO Group/Novalpina should face serious legal consequences.

Accountability

Spyware companies such as the NSO Group must be held accountable, and the use of their products should be properly scrutinised through our courts. It is time the UK government, through its justice system, took a clear stance nationally and internationally against this type of espionage on civilians, thus protecting the fundamental rights of individuals not just in the UK but worldwide.

The Computer Misuse Act 1990 (CMA 1990) and its more recent changes offer the legal scope for a prosecution to be brought against the NSO Group. Sections 3, 3A, and 3ZA provide sufficient legal tools to bring before a jury the maker and the supplier of spyware technology.

Section 37 of the Police and Justice Act 2006 amended CMA 1990 by creating a new offence, 3A of 'making, supplying or obtaining articles for use in computer misuse offences'. The section clearly targets the creation, supply, and use of so-called 'hacker's tools'. Pegasus is such a tool, a super-tool, in fact a cyber weapon.

The mens rea for the supplying offence, under s 3A(2) is lowered and can attract criminal liability where a person 'is guilty of an offence if he supplies, or offers to supply any article believing that it is likely to be used to commit, or to assist in the commission of, an offence under sections 1, 3, or 3ZA'. In short, mere belief is sufficient.

Comment

Given the broad public knowledge of the

The Citizen Lab

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs & Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

What is NSO? NSO Group, which also goes by the name Q Cyber Technologies, is an Israeli-based company which develops and sells spyware technology. It is majority owned by Novalpina Capital, a European private equity firm. NSO Group claims it sells its spyware strictly to government clients only, and all of its exports are undertaken in accordance with Israeli government export laws and oversight mechanisms. However, the number of cases in which their technology is used to target members of civil society continues to grow.

Citizen Lab—along with organizations such as R3D, Privacy International, EFF, and Amnesty International—has closely tracked how NSO Group's surveillance technology has been turned against political dissidents, lawyers, journalists, and human rights defenders. Among the many companies Citizen Lab has tracked, NSO Group stands out in terms of the reckless abuse of its spyware by government clients. Although the technology is marketed as a tool to assist governments in lawful investigations into crime and terrorism, Citizen Lab has identified dozens of cases where journalists, human rights activists and defenders, lawyers, international investigators, political opposition groups, and other members of civil society have been targeted with its spyware, called 'Pegasus'.

What is Pegasus? NSO Group / Q Cyber Technologies' flagship spyware, which is usually branded as Pegasus but which may have other names (including Q Suite), is among some of the most sophisticated spyware available on the market and can infiltrate both iOS and Android devices. To monitor a target, a Pegasus operator uses multiple vectors and tactics (see: 'How Do Infections Happen?'), including zero-day exploits and deception, to penetrate security features in popular operating systems and silently install Pegasus without the user's knowledge or permission.

What Can Pegasus Do? Once Pegasus is installed, it begins contacting the operator's command and control (C&C) servers to receive and execute operators' commands, and send back the target's private data, including passwords, contact lists, calendar events, text messages, and live voice calls from popular mobile messaging apps. The operator can even turn on the phone's camera and microphone to capture activity in the phone's vicinity and use the GPS function to track a target's location and movements.

For more on Citizen Lab's research pls go to www.citizenlab.ca

repression practised by many of their clients, and faced with the wealth of evidence against governments such as Saudi Arabia, the NSO Group cannot seriously claim to lack insight into the illegal uses of their tools. Even if they were to claim lack of knowledge, it seems s 3A(2) is wide enough to bite.

The UK legislation has been cleverly drafted here to meet the ever-expanding challenges of cyber security and to make suppliers of such technology think carefully about the people to whom they might sell their products. The NSO Group is no exception, particularly now that it has made our jurisdiction its home, and the illegal/unauthorised uses of its products have continued.

The global market for spyware continues to grow and, as it does, more governments and security services with histories of abuse will acquire this technology. The expanding and unregulated use of spyware like Pegasus will enable a growing number of authoritarian states to pry into the digital lives of their own citizens, but also into phones and computers in pockets and purses around the globe, making anyone, including the author of this article a potential target. **NLJ**

Flavia Kenyon, barrister, 36 Commercial (*https://36group.co.uk/commercial*).