DE JURE NEXUS LAW JOURNAL

Author:

Maitri Pachori

Symbiosis Law School, Noida

2nd Year, BA LL.B.

ISSUE OF PEGASUS SPYWARE

The Pegasus Spyware problem is currently a major subject in India. Spyware is any harmful program that infiltrates your computer, collects your data, and sends it to a third party without your permission. NSO Group's Pegasus is arguably the most potent malware ever built. Its goal is to hack Android and iOS cell phones and transform them into surveillance devices. Spear phishing is used to execute this type of monitoring.

What is Spear phishing?

Pegasus is a Greek mythological figure who is the offspring of Poseidon as well as a white flying horse with two enormous wings. Bellerophon sits on Pegasus. Bellerophon was a warrior who tamed this mythological horse, believing that by riding it to the summit of Mount Olympus and then to heaven, he would reach the pinnacle of the world. He collapsed and died while on his way. This warrior Bellerophon is shown carrying a spear, in images and paintings. Now, we can say that maybe the spear is a metaphor for these spear-phishing technologies. Spear phishing refers to punching holes in something and then passing through. It's very similar to the way the coronavirus invades our cells. The coronavirus has spikes that hook onto our ACE2 receptors and then basically borrow a hole in the cell to implant itself in our cells, and that is exactly what this software does. It's called spear phishing for a reason.

The term Pegasus here does not allude to the horse, but to the weapon that the warrior bears. So, symbolically, we might argue that, just as that warrior failed, perhaps this has also failed, because Pegasus and the business that manufactures it, NSO, are now in disarray all over the

world. It is already the subject of several lawsuits in the United States, and it seems likely that the firm is on the edge of bankruptcy.

The initials NSO stand for Niv Carmi, Shalev Hulio, and Omri Lavie, the company's three founders. These three used to be part of a top-secret and very successful Israeli intelligence organization known as Unit 8200, which has just one purpose: to create electronic intelligence. So, in 2013-14, these specialists resigned and started their own company. It was invested in by a foreign company/investor, and it was sold for more than a billion dollars in 2017. It was sold to Shalev Hulio and Omri Lavie, two of the three founders, as well as a fund called Novalpina Capital. They went on to become a global success as a consequence of this. This company claims to be legitimate and also says that it helps the government fight terrorists, traffickers, etc. The business's initial fame came from the Mexicans very early on, when they created a very primitive form of this type of software and Mexico utilized it to arrest El Chapo, which earned them a reputation since the Mexican president at the time publicly thanked the company. As a result of this, their popularity expanded around the world, and other countries became aware of it. These nations figured out a variety of additional applications for it, and many of the countries that are generating worldwide news as a result of this joint project are now known for undermining civil liberties, targeting political opponents, and so on.

So, Pegasus is a weapon that fell in the wrong hands. The wrong hands are not ordinary criminals, Mafiosi, smugglers, or terrorists. These wrong hands were the states that wanted to use this weapon against their rivals like journalists, politicians, activists, judges, etc[1].

The majority of the figures from the list were geographically concentrated in ten countries: India, Hungary, Morocco, Azerbaijan, Kazakhstan, Rwanda, the United Arab Emirates, Bahrain, Mexico, and Saudi Arabia.

There was a certain pattern in the kind of people who were being targeted in these countries and unfortunately, India is a part of this list.

This controversy broke almost 2 years back but on a much smaller scale.

Pegasus software is a weapon system, not software; it meets the definition of a weapon system. The Israeli government considers it a weapon system that is subject to export regulations, which implies that NSO cannot export any of its products. In reality, all of NSO's products are protected exports, which means they must first be approved by the Israeli government before

[1] Section 66C of the Information Technology Act, 2000.

they can proceed. There is an application from a certain country's government, and NSO can only sell to other sovereign governments, and that application must be approved by the Israeli government, because many agreements have been established around the world to control the exports of dangerous weapons and, more importantly, dual-use technologies i.e., the technologies that can be used to protect good people from bad people but technologies that can also be used to harm good people on behalf of bad people.

Many nations across the world have jurisdiction over dual-use technology. In actuality, the Wassenaar Arrangement governs this and India joined the Wassenaar Agreement in 2017. This implies that these nations will exchange notes and information on sensitive technology that they may be exporting, and the Wassenaar agreement will have a separate list with varying priorities, such as sensitive, more sensitive, and most sensitive. Pegasus software qualifies as a weapon system that targets specific individuals, and so would be classified as the most sensitive weapon. As a result, numerous regulations will be in place, including what is known as an End User Monitoring Agreement (EUMA), which states that the nation selling it to the other country has the right to monitor its use. Thus, the Israeli government and the NSO have the right and the responsibility to keep track of how this is being used.

Pegasus can send trap links that plant malware into a system[2].

However, because Israel's government has changed, NSO is now likely to be in serious trouble. It's not like this government would just go after this because Netanyahu allowed it to happen, but the Israeli government will have to take action against NSO due to the global opprobrium it caused.

PM Modi became the first Indian Prime Minister to visit Israel in July 2017, and facts reveal that the initial list of numbers to be monitored in India was picked only a week after that visit. As a result, these dates are matching up. We now know that this software was given to India sometime in 2017 since the pattern is extremely apparent.

According to evidence, whoever was using Pegasus in India was not just targeting adversaries but also their people. Prahlad Patel and Ashwini Vaishnav, for example. Friends of the BJP who have been placed under surveillance include both those who have been upgraded and those who have been downgraded from their posts in the recent cabinet shuffle. As a result, there isn't a straight line.

[2] Article 21 of the Indian Constitution.

There is one more name among the hundreds that have surfaced: Pakistani Prime Minister Imran Khan. This is a name that any Indian intelligence agency would consider legitimate to put under surveillance. But there's a catch: Imran Khan may be unaware of what's going on in Pakistan concerning India since Pakistan's authority is held by someone else. So, it's possible that catching someone at GHQ would have been preferable.

The government cannot even claim that some rogue element was involved in this instance because NSO only sells to sovereign governments and is unable to sell without the approval of the Israeli government.

Conclusion

Even if the software is lawful and has been supplied to the government legally, determining who it is used against must be done in accordance to the law[3]. And that is the law that the Supreme Court has established, under which several agencies (with the authority to tap citizens' phones or communications) have been notified that before tapping people's phones or communications, they must give a legitimate reason, put those names on a list, go through a series of clearances and finally have the Home Secretary of India sign off on them[4]. They are not made public but these things are done so that there are checks and balances and such powers are not misused[5]. So, I believe the Supreme Court should ensure that the laws and rules it formed are updated in light of changing technologies, but the principle that the government can track people's communications if there is a legitimate reason must be established through a transparent process with checks and balances.

[3] Section 5(2) of the Indian Telegraphic Act, 1885.
[4] Section 26 of the Indian Telegraphic Act, 1885.
[5] Section 66E of the Information Technology Act, 2000.