Source : www.thehindu.com Date : 2021-07-26

JOINING THE DOTS IN THE SECOND COMING OF PEGASUS

Relevant for: Security Related Matters | Topic: Basics of Cyber Security and related matters

Pegasus is not a stranger to our shores. It first surfaced in our public discourse towards the end of 2019. Researchers from University of Toronto's Citizen Lab called up some telephone numbers in our country and informed them that their WhatsApp chats were compromised. There were some stirrings, but the controversy died out quietly and disappeared from our public discourse. The attention then was predominantly on the issue of how secure WhatsApp was and how weak its claims of end-to-end encryption were. WhatsApp's public relations exercise to reassure its customers of its safety and privacy grabbed disproportionate attention. All these deflected the public's attention from our Government's involvement in the ugly saga and the misuse of NSO of Israel's spyware to snoop on its own citizens. Parliament and civil society let the Government off easily. Perhaps, the impression that the surveillance then was largely confined to the Bhima-Koregaon happenings also contributed to its limited appeal.

Most of us failed to connect the dots. The frequent and prolonged instances of Internet shutdowns; use of the sedition law on critics of the Government's policies; use of the Unlawful Activities (Prevention) Act (UAPA); rushing of crucial pieces of legislation affecting core sectors of our economy through the Houses of Parliament; consigning the data privacy Bill to a select committee; the framing of rules to rein in digital news platforms, and the demonic efficiency with which State governments were toppled appeared less dramatic and had no shock value as unconnected events. But if connected with each other, and the Pegasus spyware running in the background, they present a picture of India's descent into a surveillance state.

Pegasus is India's Watergate moment

Treated separately, each one of those incidents, caused little more than a few days of screaming headlines, reprimanding editorials, raucous prime-time television debates, weak and short-lived protests by political parties and rights activists. The probability that the second coming of Pegasus into our political discourse will not be very different from its first appears very real, if this too is treated as a separate and isolated event. Fortunately, this time it came with two major differences.

This time the attention is exclusively on the Government's role and there are no red herrings in the form of questions about the safety of encryptions offered by service providers. The people involved in the revelations are not just little known activists. They range from the Leader of the Opposition, a constitutional authority, a number of journalists, human rights activists, Ministers in the Government, ruling party leaders, several political leaders, serving or retired officers. The list also revealed that the government agencies made no distinction between state interests and the interests of the ruling party. The expansiveness of the global list of people named as intended targets of the spyware and the prestige of publications involved in cross-border collaboration are indeed arresting.

Pegasus's second coming has yet another distinction. It foregrounds the collusion between government and weapons grade surveillance tech that has no intermediary functions to confuse us. The episodes that were hitherto played out as government versus tech in our country allowed the combatants to compete for our support. The government and the tech companies claimed to fight one another on our behalf. However, they were actually fights between tech and government for possession and control of our data. Government sought its possession to control

society, to eliminate dissent and opposition. But it tried to portray to us that it sought to tame the tech companies to protect our interests, privacy, and the security of the realm. Tech companies sought to possess our data sets to make prediction products out of them and sell them to advertisers. Both the Government and tech companies vied for surveillance over us. One for control and the other for profits. However, there is always the undetected possibility of their interests coalescing. In the case of Pegasus the collusion is evident. The NSO Group does not compete with the Government for the possession of data surplus of its application. It is a pure and simple provider of surveillance-as-a-service to the Government. In the event, Pegasus this time shines a light on the Government for civil society to see it as a clear accountable entity.

Explained | Pegasus and the laws on surveillance in India

It is evident that the Indian government till now is acting out of a standard play book. It is stonewalling. It has so far evaded the essential questions that are raised by the revelations. Ministers and representatives of the ruling party are questioning the credibility of claims made by the global consortium of media organisations that announced the startling revelations. They are accusing the publications of acting with ulterior motives to undermine India's democratic institutions. Supporters of the Government's narrative charge the publications with attempting to defame the country. The Government's, and its supporters', defence so far is essentially semantic quibble and based on raising doubts on the source of the telephone numbers that the media consortium says is from a leaked list accessed by media portal Forbidden Stories.

The uncommonly cautious wording of the preface to the consortium's admittedly limited claims to their findings is sought to be used to undermine the extraordinary significance of its revelations. The consortium desisted from making sweeping claims. It said, the leaked list of 50,000 numbers "are believed to have been selected as those of people of interest by government clients of NSO Group". The consortium also said that the list "indicates the potential targets" identified in advance by the NSO's clients for "possible surveillance". The list is only "an indication of intent" and the appearance of a number in it does not reveal "whether there was an attempt to infect the phone" or "whether any attempt succeeded".

NSO Group | The spy who came in for the phone

But amidst all this extraordinary caution is this devastating revelation which the Indian government chooses to deliberately ignore to indulge in semantic wrangling: "However, forensic examination of a small sample of mobile phones with numbers on the list found tight correlations between the time and date of a number in the data and the start of Pegasus activity — in some cases in as little as a few seconds." Amnesty International's forensic lab found that of the 67 phones examined, 23 were infected and 14 showed signs of attempts to penetrate. The rest were cases of possible change of devices or those using the Android operating system that did not keep record of logs needed for forensic work. By any standard this is considered an overwhelming basis for further investigation. It establishes an unquestionable basis for subjecting all the rest of the numbers from the list of 50,000 numbers for investigation. And in India's case, all the 300 numbers from the country that were found in the list. Already, over 10 of them were forensically examined and found to be either successfully infected by Pegasus or attempted to be penetrated. That is enough of a case for a comprehensive investigation into the claims of the media consortium. But the Government narrative harps on words such as 'indicative,' 'possible' and 'potential' as being too general and dismisses snooping charges.

The Indian government's defence that rests on questioning the source of the list has little merit. Investigative journalism is under no obligation to reveal its sources. In fact, it is ethically bound to not reveal in order to protect the identity of its sources.

Editorial | Spy in hand: On Pegasus spyware issue

As important as the questions that the Government forcefully articulates is its remorseless stonewalling of the most important question repeatedly asked of it. It does not tell us in unequivocal terms whether it has or has not purchased the Pegasus spyware. It did not answer that question during the country's first brush with the spyware in 2019 too. Even today it seems to be firm in its resolve not to answer. It hopes to wear down the political opposition, activists, human rights groups, and civil society. It evidently thinks that it can wait out the news cycles to run their course. It probably can. Civil society and the media, cannot, beyond a point, keep the pressure on. A government with brazen determination, brute majority in the legislature, and as yet unchallenged political capital, can afford to wait out the limited firepower of its political opponents' artillery.

The only institution in the present situation that can make the Government accountable is the judiciary. The track record of our top court on major issues of defining importance to our national life is at best mixed in the recent past. What it chooses to do or not do now can make a difference to India. The options before it are clear as they are stark. To allow the present government a free run in turning India into a surveillance state is one. The other is to stop the Government in its tracks, restore to its people the gift of a free and liberal state that the founding fathers of the Republic gave them. The country has very little time.

Parakala Prabhakar is a political economist and heads RightFOLIO, a Hyderabad-based knowledge enterprise

Our code of editorial values

END