Did hacker-for-hire mercenary gangs target Bhima Koregaon-16?

Alpa ShahTIMESOFINDIA.COM
Mar 20, 2024, 14:40 IST

In her new book, "The Incarcerations", the noted LSE anthropologist makes a case for how the evidence, which was used to incarcerate 16 people in the Bhima Koregaon case, was 'likely to have been implanted remotely through a hacker-for-hire mercenary gang infrastructure that has clients all over the world, but whose epicentre is in India'

What was the hacker group ModifiedElephant? Was it the Pune City Police itself? Was it a cell somewhere in the Indian government? In the NIA [National Investigation Agency]? Juan [Andres Guerrero-Saade of SentinelLabs] and Tom Hegel's report [his colleague] had made it clear that it had many victims, multiple unrelated targets beyond the Bhima Koregaon (BK) case, and had been running for years. In fact, it was still in operation in 2022 when SentinelOne's report was published.

Both the [cyber security firms] Arsenal and the SentinelOne reports had clarified that it was a group with enormous time and resources. I had gathered that the kind of hacking work that went into the BK case over many years would take a team working full-time.

I had noticed that though the Arsenal reports had said that Rona Wilson and Stan Swamy had been targeted since late 2014, a

date which I noted coincided with just after the Narendra Modi government was elected, SentinelOne had traced ModifiedElephant's activity back to 2012 in their report. So I asked Juan and Tom about these discrepancies in dates of operation.

Juan explained, 'Countries tend to develop these capabilities as part of their intelligence services, sometimes law enforcement services, separate from the incumbent governments. The problems start with how incumbent governments decide to use those capabilities.' 'Got it!' I said to Juan. 'The infrastructure for the hacking and the malware is in place earlier. But then how it's actually used can be dependent on particular governments,' I summarised.

'There's also another element to this,' Juan said. 'When you don't have a proper legal framework and you don't have any oversight capabilities, sometimes you'll see much lower tier organisations – let's say the local police of a particular region – deciding that they can just use those capabilities without anybody even knowing at the top of the government.

'Let me add another curveball that's particularly relevant to India,' Juan continued.

'There are a lot of private mercenary hacker-for-hire organisations that get involved in the middle of the Indian ecosystem. So it's still the government. But you're hiring out, or you're dealing with a company, and then suddenly, you pay them to become a part of your organisation, or you hire them for jobs that you don't want to officially avow.'

Juan said, 'It's not necessarily it was the police themselves doing all the hacking. They could have been paying, let's say, a company that does all this work for different Indian police.'

Hacker group ModifiedElephant is linked to the 16 targeted in the Bhima Koregaon case (Photo: Freepik)

My mind was racing to keep up. Private mercenary hackers-for hire? It all sounded very exotic. I butted in, 'So can you tell where these people are based? Are they foreign or are they Indian?'

Tom said, 'We're typically unable to gain that perspective… But yeah, a lot of the Indian threat actors do operate straight out of India, for the most part. At least the ones that we've dealt with so far.'

Juan added in a matter-of-fact way, 'It's a pretty safe haven, right? So, there's not a lot of reason for them not to be running out of India. I don't know if there's any local prosecutions of hackers that we don't know about, but we've never heard of someone getting picked up over there and have the screws put to them on principle, because they're not supposed to be doing that. So even the ecosystem that supports hacker-for-hire companies that are doing business abroad show India as a safe haven for that kind of activity.'

Juan continued, 'I mean in the US you could never have a company like that. You're basically advertising burglary services, right? Like it would never fly. But India has been very successful providing those services abroad. I think, precisely because there's so little enforcement that they almost treat it like they're legitimate businesses.'

It dawned on me how obvious what they were suggesting was. I said, 'Yes, of course. And it's the place where global companies used to go for IT services. For example, all the call centres of

European companies were there. Everyone went to India to get IT services cheap right?' The Indian hacker-for-hire gangs in a way seemed just another extension of IT services like call centres or programming. 'That makes complete sense. I hadn't thought about any of that before,' I said.

Juan and Tom were both smiling and nodding. Finally, I seemed to get the picture they were painting. I asked them, 'Are you able to make a connection between ModifiedElephant and hackers-for hire? Are you able to tell this from your data?' Juan was smiling as Tom responded, 'Yeah, it's in the works. We're trying to nail it down very precisely. There's very likely connections that they are. But coming up with irrefutable data on that is still kind of in the process.'

Juan explained further, 'There's one Indian company that's well-known for having kind of started a lot of that. It was called Appin.

And this company has been well recorded and well-known for many years. And we saw connections in the early ModifiedElephant infrastructure with Appin. 'But, oddly enough, the metaphor we've been using is that Appin is kind of the trunk from which the whole tree of Indian cyber espionage sparks out. There are many companies that seem to be derived from Appin, many government teams that seem to in some way be related to what was old Appin, and it just seems like they kind of permeated the Indian ecosystem.'

Violence during a celebratory gathering on Jan 1, 2018 at Bhima Koregaon, Maharashtra, to mark 200th anniversary of Battle of Bhima Koregaon. 16 were arrested for inciting riots (File photo)

That night I stumbled upon an undercover operation undertaken by *The Sunday Times* and the Bureau of Investigative Journalism

published in November 2022, which helped me build a stronger picture of Appin and hacker-for-hire mercenary gangs.

Two reporters had gone to Delhi posing as former agents of Britain's secret services who had set up a Mayfair-based corporate investigation company on retirement. They met with a series of hackers and even gained access to an Indian hacker gang's database. Those the gang tried to hack for clients included Chris Mason, the BBC political editor, the president of Switzerland and his deputy, and Philip Hammond the then chancellor of the UK government.

The list was vast and high-profile – the former head of European football, a British-based Russian oligarch, critics of Qatar who threatened to expose the wrongdoing by the Gulf state in the run-up to the World Cup.

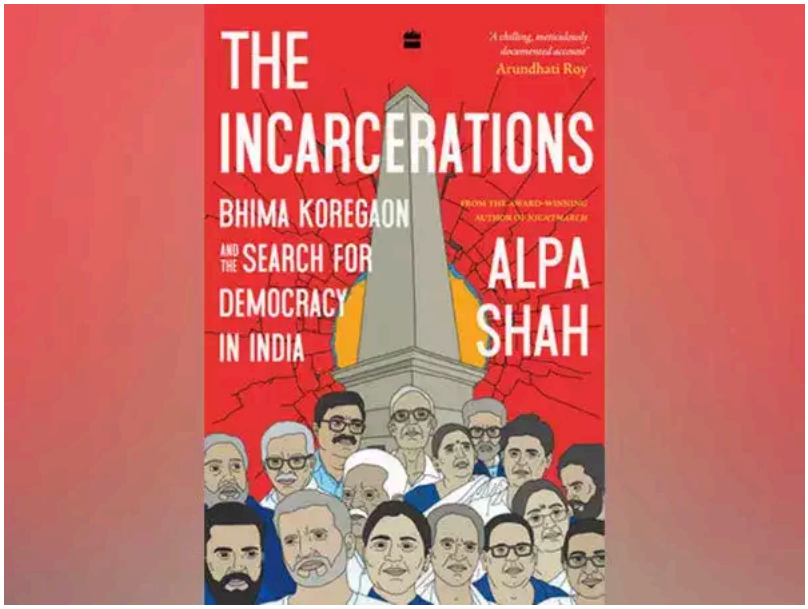
Their report revealed that hackers from India were being hired all over the world by private investigators and corporate intelligence companies to break into email accounts and smartphones to spy on cheating partners, for corporate espionage, and even murder. Major law firms, including those with bases in the City of London, were clients.

British investigators were able to commission Indian hacker-for-hire firms for their clients with little fear that they will be prosecuted for breaking the UK's computer misuse laws. A whole global underworld of hackers-for-hire mercenary networks was revealed with its epicentre in India, but what caught my eye was the fact that *The Sunday Times* too said that one of the hacking industry's 'founding fathers' was a firm called Appin.

The Sunday Times even managed to interview one of the hackers trained by Appin: Utkarsh Bhargava, who had been a hacker for almost a decade. Bhargava told them that all 17 students from his cyber security course had been recruited by a Delhi-based hacking firm working very closely with the Indian government, doing all their hacking work.

The firm used Appin to train them for a year to hack computers. On completing Appin's 'finishing school', *The Sunday Times* reported, 'Bhargava said he was ordered to start a series of cyber attacks on the governments of Turkey, Pakistan, Egypt and Cambodia at the behest of the Indian state.

The targets were typically secret documents and files in the other country's ministries. One of his colleagues was trying to break into the Canadian government's computer systems.'



The cover of "The Incarcerations: Bhima Koregaon And The Search For Democracy In India" (Photo: ANI)

Bhargava told *The Sunday Times* , 'We were not allowed to have questions. It was just, "Hey, this is the target. You have got three months of time. Do whatever you want to do we need results."

That's how it works...They will say, "Hey, this is the ministry of this particular country, we need this data." Our job was to get the data dump and hand it over to the [Indian] agency . . . [The target] can be the external affairs ministry, it can be home, it can be defence, it can be finance. It depends what kind of intelligence they are seeking.'

Appin was set up in Delhi more than a dozen years ago supposedly to train 'ethical' hackers who could help safeguard individuals and businesses from cyber attacks. In fact, it had a lucrative side-line taking cash from clients around the world – including corporate intelligence companies based in Britain – to hack individuals, said *The Sunday Times* report. But Appin was exposed by Norwegian cyber security experts who linked it to hacks in a dozen countries.

Tom had alerted me to this Norwegian exposition of 2013, called 'Operation Hangover'. When the Norwegian telecom sector was hacked through spear phishing emails sent to people in the upper tiers of management, it filed a case with the Norwegian criminal

police over unlawful intrusion into their computer network. This unfolded a threat intelligence operation, which ultimately exposed a hacker network in India.

In fact, the Norwegian exposé showed that a major target of attack of this Indian hacker group was cyber espionage against targets of national security interest, particularly victims in Pakistan.

Tom had said that the Norwegian operation published all of their data, which made it possible for him and Juan to see a relationship in the technical infrastructure used by the hacker group at the centre of 'Operation Hangover' and that used by ModifiedElephant.

The same servers for malware communications had been reused by ModifiedElephant. Tom had concluded, 'So they are likely the same threat actor. Or, they are sharing technical resources because they're using the same server for their attacks.'

This all correlated with *The Sunday Times* report which said that after Appin's exposure by the Norwegians, 'its well-trained former employees scattered like seeds and set up new firms to utilise their freshly acquired talents in the computer dark arts. This created a more diversified Indian hacking industry.' Several had set up offices in Gurgaon (or Gurugram), a satellite city that had developed on Delhi's outskirts and which housed some of the world's biggest technology companies.

The *Sunday Times* helped add colour to Tom and Juan's accounts. Now I could see offices in Gurgaon's apartment blocks belonging to different hacker-for-hire companies/gangs, sometimes sharing infrastructure, malware, products. Perhaps they had spread to other Indian cities too – Bangalore? Their young, tech-savvy employees working in rooms full of computers, executing the task they were given.

For those trained in computer studies and cyber security, as *The Sunday Times* had noted, computer 'offensive' work – the term used for hacking – was much better paid than 'defensive work' protecting systems. Like the young Bhargava, perhaps they were just doing the best-paid job their IT-related degrees and position in society could offer them: hacking. If they had the contacts, the know-how, and enough capital for the resources, they may even,

like Bhargava, eventually branch off and set up their own hacker-for-hire firm.

It seemed likely that somewhere in that dark underworld of the linked-up proliferation of hacker-for-hire mercenary gangs – or 'companies' if you want them to appear more respectable – was the one that Juan and Tom had named ModifiedElephant, that had perhaps been commissioned by some section/s of the Indian state to target the BK-16 and other victims.

Activists Arun Ferreira, Vernon Gonsalves and Sudha Bharadwaj were among the BK-16. According to a report, they were victims of "state-linked snooping...and incriminating document delivery aka planting of evidence"

Tom had reminded me that Rona was also attacked by phishing emails from a different hacker group called SideWinder, sometimes at the same time as ModifiedElephant. 'SideWinder is a well-known Indian threat actor that typically leans less towards individual targets and more towards targets for espionage purposes. They've historically gone after Pakistan. It's well reported throughout many people in the industry. Their toolkit's different, their infrastructure is all different,' Tom had said when we met online.

I had said, 'Right, so this is another thing I found weird in what you had identified and also in Arsenal's reports, which is that some of these folks were being targeted multiple times. Because once you've got access, you've got access...why do you need to keep going for the same target? What would explain that kind of behaviour?'

Nodding, Tom had shared, 'Initially, we're kinda like, maybe it's multiple threat actors that are being assigned tasks by one priority customer who said whoever gets there first into their email wins. So SideWinder tried to jump in too.'

Juan had added that it could be different organisations in the state targeting the same person using different hacker groups. He had said, 'So just because ModifiedElephant has access and, let's say, ModifiedElephant is working for the police, it doesn't mean that the Intelligence Agency won't try to go after them too (through a different hacker group). Rona was a kind of magnet of threats in this case. We see two or three different hacker groups, trying to get at him at the same time.'

Juan then added, 'You have to consider kind of the reality of government bureaucracy . . . just because one hand has reached out, it does not mean the other one knows, or that they won't try to do the same thing. Or that they won't mistrust the other people.'

What Juan said spoke to what I knew of Indian state bureaucracy or for that matter bureaucracy anywhere. 'We have that a lot with Chinese threat actors, as well, and you know some of the less organised folks, where they will just go kind of after their own missions,' Juan had said.

I recalled that at some point in the conversation, Juan had shared candidly, 'It gets very scary once you get to the actor tracking part...Because we know that an actor that is willing to throw innocent people in prison has been active for more years than people knew about, has been going after way more targets than people are aware . . . other university professors, Christian missionaries, all kinds of activists, and you know, political figures in this space.'

Juan had explained that what they found particularly distressing was that the ModifiedElephant hacker group was not a very sophisticated threat actor. 'That's something that kinda kills us...I mean, we've dealt with all kinds of threat actors and you get unbelievable top tier folk using amazing tools and exploits and all these things.

That's not what is happening with ModifiedElephant. It does not have great tooling. It does not have great operational security.' In fact, it was because they were not that sophisticated, that tracking ModifiedElephant had been relatively easy for Juan and Tom.

'They'd even put Shivaji Pawar's [BK investigating officer, Pune] phone number and email address as the recovery address for Rona's email account?' I had asked at one point.

Juan replied, 'If that's what was asked for. If that is their method.' I said, 'Wow! Well, as stupid as that, I mean?' Tom said, 'Yeah, exactly.'

Juan added, 'That's where we started this conversation. It's idiocy all the way down!' He said, 'It's not very satisfying. It's so low brow. But it's still life altering.

'It's been sort of very soul crushing to see that something so unsophisticated, almost rudimentary in its capabilities, has had such a detrimental effect on very real human lives to this day, and God knows how many more that we don't even know about,' Juan had said.

'How many other cases are there with tampered, manufactured digital evidence? That just didn't have the luck of attracting enough attention, of getting external consultants that were capable, willing, brave enough to dedicate their time and figure out that folks are being entrapped,' Juan asked.

Perhaps we will never know exactly who the hacker group ModifiedElephant is/was and their exact links with the Indian state, or the specific sections of the Indian state that were involved. And no doubt by the time this book comes out, the hacker group and its relationship with the Indian state may have morphed into something different, hard to trace.

But I had never dreamt when I first began research for the book that it would lead me into an entirely new domain of warfare – cyber warfare – and an Indian speciality in hacker-for-hire mercenary gangs that could be employed globally by anyone, including the Indian state, and were likely to be central to how and why the BK-16 were incarcerated.

Before we had said goodbye, I had asked Juan and Tom what they hoped from their SentinelOne ModifiedElephant report. In a very calm, measured and humble way, Juan had said, 'There's no glory in it for us. We would have really loved to see them [the BK-16] get released. I think that's the biggest thing. But India is

going through its "Trump moment", and it's very hard to expect any good outcomes without a massive sea change there.'

I sensed a certain despondence in Juan even if he did well to show it as just being realistic. But the collective efforts of Juan Andrés Guerrero-Saade and Tom Hegel and their team at SentinelOne, alongside Mark Spencer and his team at Arsenal, and all the others outside of India who had taken an interest in the cyber warfare at the centre of this case — Citizen Lab, Amnesty International, Andy Greenberg and Wired, *The Washington Post* and *The Guardian* — had played a major role to expose that the BK-16 had been victims of state-linked snooping, hacking and incriminating document delivery aka planting of evidence.

Excerpted with permission from 'The Incarcerations: Bhima Koregaon And The Search For Democracy In India' (published by HarperCollins India)