India Trains Its Sights on Dissent in Chhattisgarh

Allison West 2022-10-28T08:00:47

Development in the form of profit-driven resource exploitation ventures in India's central state of Chhattisgarh, led by corporations and facilitated by the state, have wreaked havoc on the lives and livelihoods of the region's indigenous Adivasi peoples. In the face of widespread dispossession, corporate land grabs, environmental degradation and militarized policing in Chhattisgarh, Adivasi activists and organized civil society play a vital role in monitoring, documenting and challenging ongoing human rights violations on the ground. For this work, Adivasi leaders, trade union activists, lawyers, journalists and researchers in Chhattisgarh have often been targets of state and vigilante harassment and violence. Recent revelations of targeted Netwire and Pegasus spyware attacks suggest the state is escalating its efforts, with alarming implications for Adivasi rights, the rule of law, and democratic civic space in India.

Phishing for Human Rights Defenders in India: The 2019 NetWire Attacks

In 2020, Amnesty International and Citizen Lab uncovered a coordinated spyware campaign targeting nine human rights defenders in India, including several active in Chhattisgarh. Between January and October 2019, the targets received spearphishing emails with malicious links that, if opened, would have installed NetWire, a commercially manufactured Windows spyware that monitors a user's actions and communications. Spearphishing is often performed by sending carefully crafted, personally tailored emails that seem to be legitimate messages. For example, the activists and lawyers targeted in the 2019 NetWire attacks received emails mimicking plausible legal notices, with subjects reading "Reminder Summons for Rioting Case" and "Summons Notice Jagdalpur Arson Case," as well as a believable message from what appeared to be a journalist warning a law collective that it had been blacklisted by the state government.

The common link between the human rights defenders targeted in the NetWire attack seemed to be a record of speaking out on behalf of those imprisoned in the 2018 Bhima Koregaon Case. In the case in question, prominent Chhattisgarh activist and lawyer Sudha Bharadwaj was among several activists, lawyers, scholars and artists arrested and charged with terrorism-related offences for giving speeches at a public event on 31 December 2017 in Bhima Koregaon (Maharashtra State), which authorities allege instigated the violence that erupted in the streets the following day between Dalits and Hindu nationalists. In the Netwire attack, two human rights defenders active in Chhattisgarh were targeted – Dalit grassroots organizer and Vice President of the Chhattisgarh chapter of the of People's Union for Civil Liberties, Degree Prasad Chouhan, and lawyer Isha Khandelwal. Jagdalpur Legal Aid Group (JAGLAG), a Chhattisgarh-based human rights collective providing legal aid to

Adivasi and other marginalized communities, and of which Khandelwal is a member, was also targeted.

Having worked with Adivasi villagers to resist the unlawful dispossession of their land by corporations and to provide legal assistance to Adivasis subjected to alleged human rights abuses by police or falsely accused of being Naxalite terrorists or sympathizers, Chouhan and lawyers from JAGLAG were no strangers to being targeted by the state and powerful corporate actors. While they had faced harassment, intimidation, and threats of violence in the past, the NetWire attack appeared to be an intensification of state efforts. Subsequent revelations as part of the Pegasus Project revealed that many more activists, lawyers, academics, and journalists across India had been targeted with Pegasus spyware produced by the Israeli NSO Group and reportedly acquired by the Indian government under Prime Minister Narendra Modi as part of a 2017 weapons deal with Israel.

Carrying the Spy in Your Pocket: Chhattisgarh Activists Targeted with Pegasus

Degree Prasad Chouhan, targeted in the Netwire attack, was also targeted with the NSO Group's surveillance tools, as was lawyer and member of JAGLAG Shalini Gera. Other Chhattisgarh activists targeted by Pegasus include Soni Sori, an Adivasi school teacher turned village political party leader and advocate against police violence and human rights violations in south Chhattisgarh. Alok Shukla, a Chhattisgarh-based environmental activist who has worked alongside Adivasi communities battling to assert their legal rights against powerful mining corporations in Chhattisgarh's Hasdeo forests, was also targeted, as was Bela Bhatia, a well-known activist and human rights lawyer practicing in the District courts of Bastar division in south Chhattisgarh.

Unlike NetWire, Pegasus is not commercially available, but only sold to states. Despite its proven use against many throughout India, Modi's government denies purchasing it from Israel, though has neither confirmed nor denied its use. Pegasus is more pernicious than NetWire, as infection can be achieved through zero-click attacks that do not require a user to click a link or download a file. If successfully installed, spyware like NetWire and Pegasus turn computers and phones into wiretaps, giving remote users access to all of the information carried on the device: emails, calls, calendars, passwords, one's browsing history and GPS locations. The remote user can even listen in on conversations or peek through the camera. "You are carrying the spy in your pocket with you everywhere you go" says targeted Chhattisgarh-based activist Bela Bhatia, "It is much more than one had imagined that the Indian state could do."

Spyware's Impacts on Human Rights and the Rule of Law

The use of intrusive spyware threatens a wide range of human rights, key among them rights to privacy and freedom of expression. While these rights are not absolute, human rights frameworks – whether at the national, regional or international level – typically circumscribe strict conditions under which state interference in these rights may be justified. For instance, to avoid arbitrariness,

any interferences with these rights must be prescribed by law, pursue legitimate aims, and be *necessary* for pursing those aims in a democratic society, with effective mechanisms in place for oversight and redress. The laws prescribing possible interferences with these rights must also be accessible, foreseeable, precise and sufficiently clear regarding the conditions under which surveillance may be authorized and carried out, with the scope of aims deemed legitimate, such as notions of "national security," clearly interpreted in domestic law.

The use of Pegasus-style spyware is not adequately prescribed in Indian law, where existing legislation falls well short of the proportionality, legality and necessity requirements of legitimate infringements on the right to privacy embodied in international human rights standards and upheld by the Supreme Court of India in its landmark ruling in K.S. Puttaswamy v. Union of India, which declared privacy – including informational privacy – to be a fundamental right linked with those to life and livelihood. India's existing surveillance laws, namely the Information Technology Act, 2000("IT Act") and the Indian Telegraph Act, 1885, permit targeted surveillance, but remain problematic in their opacity, lack of adequate oversight mechanisms, broad loopholes for national security and public order, and exclusion of security agencies from their remit. A 2009 amendment to the IT Act, specifically Section 69, undermines the Telegraph Act's tighter circumstantial "necessity" requirements for surveillance and instead gives authorities sweeping powers to intercept, monitor and decrypt digital information whenever deemed "necessary or expedient" for purposes of national security, public order, law enforcement or criminal investigations. Yet, even under the broad surveillance powers provided by these laws, the use of spyware like Pegasus, which involves hacking digital devices such as computers, mobile phones and apps, is not permitted, as hacking is a criminal offence under the IT Act. Several petitions challenging the constitutionality of India's surveillance laws are pending before the Delhi High Court and India's Supreme Court, but substantive progress has yet to be made.

Because spyware like Pegasus allows surveillance to be conducted completely anonymously, remotely, and ultimately unchecked, its use undermines the rule of law and integrity of democratic institutions premised on checks and balances. Another challenge in this regard involves the use of information collected through spyware as evidence in court. The Bhima Koregaon case, for example, relies almost entirely on digital evidence obtained from the devices of the arrested activists. A recent report by a US-based digital forensics company, however, shows how a hacker planted key files on an accused activist's computer via NetWire, which then served as the basis of evidence upon which the activists were arrested and charged under the Unlawful Activities (Prevention) Act, India's main anti-terror law. Currently, Indian law allows, and indeed courts have upheld, the use of illegally obtained evidence when deemed "relevant" and "genuine." The mounting evidence suggesting that the accused are actually victims of an elaborate plot in which extralegal spyware was used to plant fabricated evidence, points to one of many dangerous ways in which this type of covert, unregulated surveillance can compromise the rule of law to facilitate criminalization. In recognition of the gravity of the challenges posed by spyware to human rights and the rule of law, India's Supreme Court has now appointed an independent expert technical committee headed by Justice R.V. Raveendran,

a former apex court judge, to examine allegations into the government's use of Pegasus. Its work remains ongoing.

Shrinking Space for Civil Society

Spyware carries significant risks for the functioning of civic space necessary for a thriving democracy. In addition to the legal uncertainty outlined above, the knowledge that the state can monitor and track activists every word and move also creates a chilling effect on expression and assembly, sowing constant doubt as to whether one is doing enough to stay safe on digital devices. Spyware's ubiquity can also breed distrust regarding communication and collaboration with others. For many activists and lawyers operating in Chhattisgarh, technology provides crucial tools for their work – for documenting violations, organizing and mobilizing action, and communicating between each other and with the world. Yet, like in other places in India and around the world, surveillance technology used to target, intimidate and generally shrink space for Adivasi activists and others in Chhattisgsarh now poses new uncertainties about the tradeoffs between connectivity and security. The novel legal challenges presented by Pegasus and similar spyware will continue to be major concerns for human rights and the rule of law in the years to come.
