Here's where we are:

High confidence India office is compromised - people, facility, and selection of cell phones and laptops. RAW - they often gain physical access through commandeering a unit of Delhi's special cell and using them to show up physically as a cover (setup camera gear and reporters would cover otherwise conspicuous sigint activities)

Here's what "they" are going to do and try to accomplish.

RAW literally has a charter of "compromising foreign govt's and corporations" - to gain information and ~~influence~~ to strategically advantage the Court and the government (BJP presently).

Try to gain leverage to influence Twitter. They've seen how we react to pressuring our employees (former Counsel employee and [redacted]). They now have a strategic person in place to amplify this leverage.

Attempt to gain complimentary information from within the office and from electronic communications to understand where Twitter's head is. What options we are considering wrt India's wants / demands. Explore Twitter's internal systems for other strategic value.

If they have not discovered already, they will learn that engineers can access production. (they will want to maintain this valuable abilitiy to shape the public conversation to India's purposes instead of Twitter's. Identify, Target, silence,

All of this will work against the mission of Twitter to serve the public conversation and to improve the health of the public conversation.

If we don't do anything and just stay the course - we will not win. India is presently leading this dance and we have done nothing but follow/react. Will give some options change this in a moment.

This is not a one off, here are the other countries that will attempt to manipulate or exploit:

China
KSA (remember their agent? That wasn't even the A-team and it was very damaging)
Turkey
Russia (new law for physical presence)

Here are our immediate options and what they buy us.

Pause hiring - conveys that we have options. Conveys that there may be risk to other companies' consideration of leaving the market. Buys time.

Could message we are pulling out.

Messaging to slow down RAW and give them pause. Especially to advantage counsel and court efforts (otherwise the court will be prepositioned against everything we present)

Coordinate "hunting" messaging and activity with Counsel legal efforts. Reset credentials, collect laptops, etc. TSCM visit. Adds meaningful cost to Intelligence activities and may protect some optionality for legal and business.

Most challenging option: full speed ahead and massive hiring. Confidence cannot close on the 10 year security deficit while knowing that we have a tumor internally and that the tumor is growing out of control.

Here's the longer term plan for solving this as a total problem.

Engineers out of production.
Data isolation / privacy enforcement
Positive Control of laptops and phones
Defined operational parameters for execution within "hostile" markets.
Position to neighboring countries to service target environments (e.g. Ghana v Nigeria)
Repeatable framework for offices in these environments and rolesfunctions we can/cannot support

what if we find them

SIM - 144

Cookies - Regulators

FTC - Dish DPC - CNIL -

under the hood we're fucked -

Dev Birch don't understand state of affairs technically under the hood

(~~Project TAO~~?)