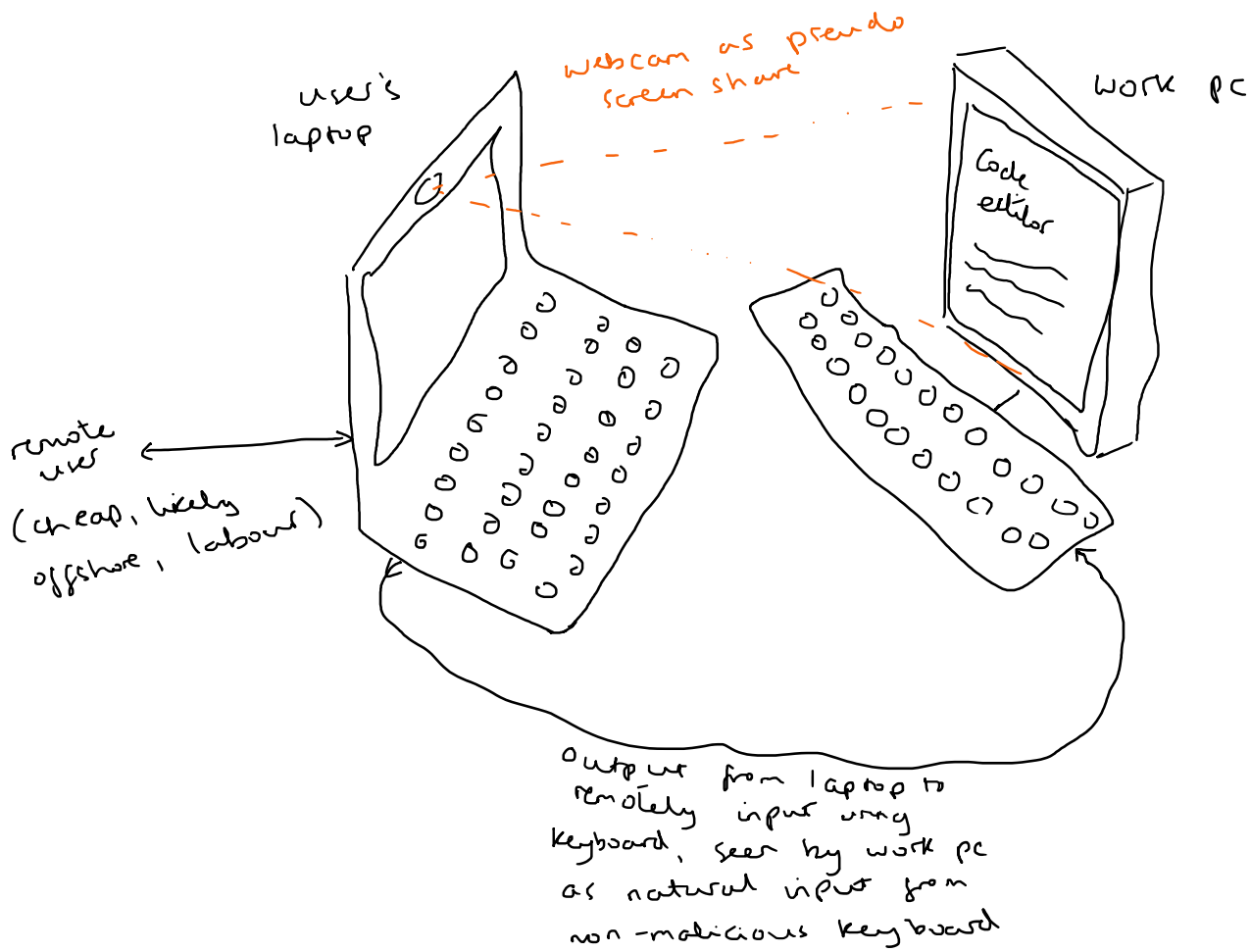


No doubt this has been done before.



'But <insert investigative group> would find out!'
Not with sufficient preparation and a sufficiently connected handling organization.

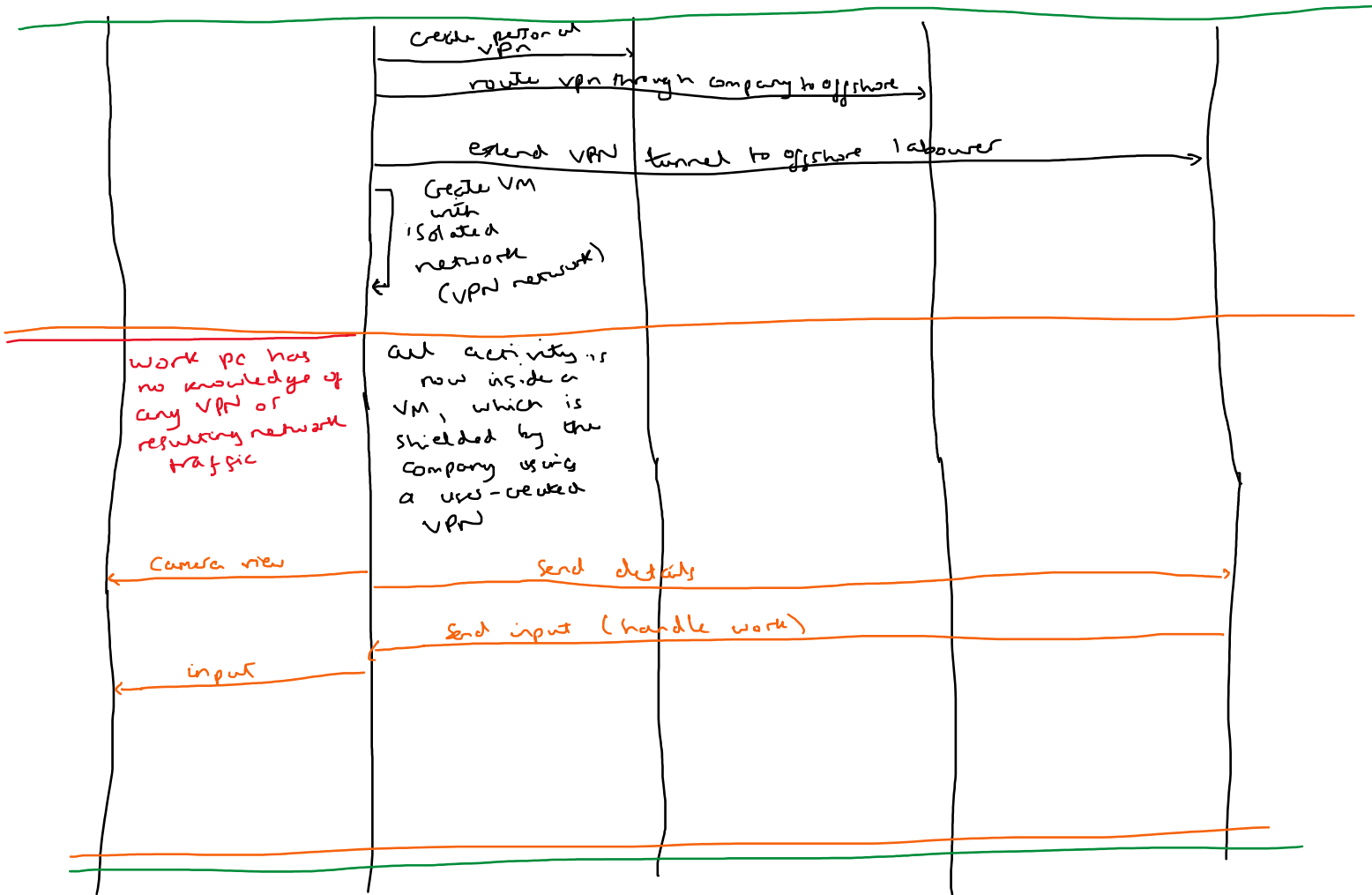
The ideal scenario for a bad actor is to be doing this inside an infrastructure - as - a - service company that has locations in the offshore location and local working location.

This would allow traffic to be secured from snooping organizations that may be otherwise protecting the employer.

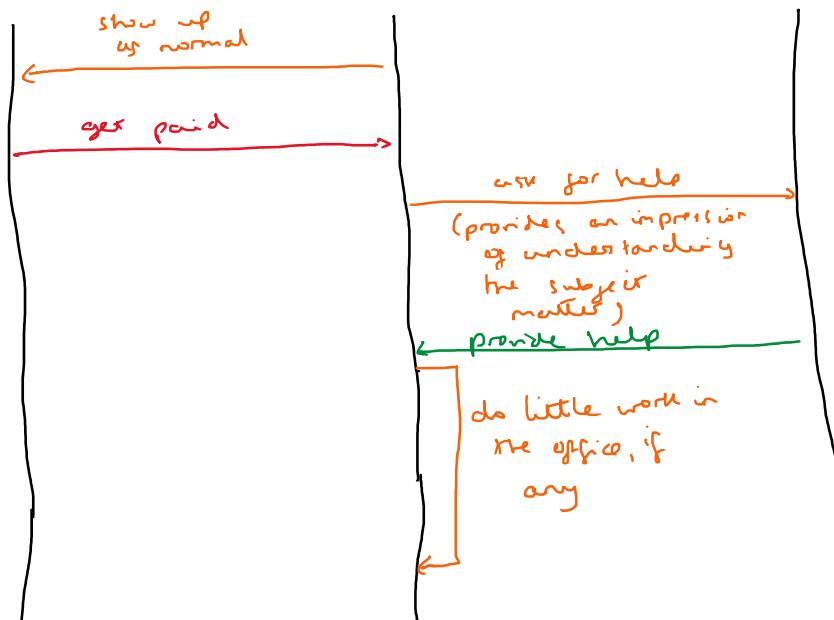
Protecting it, using the employer's resources and infrastructure!

Locations offshore and local is to guarantee end-to-end privacy, given this would undoubtedly be against contract and maybe even illegal.

work pc bad actor's laptop local infra offices offshore infra offices offshore labourer



work bad actor Coworkers



in-office discussions
will be avoided
where possible and there
will be minimal value
added if present

presenting suspicion will
include attending
routine operational
meetings in office
(standups, on call handoff,
ops meetings)

go
home

all work done at
home using
offshore worker
through company
protected VPN
tunnel setup

remote meetings will
include valuable
additions through
real-time communication
with offshore worker

may note initial
responses are always
delayed but ignore if
as "just them"