Twitter Thread by Eric Geller

Eric Geller
@ericgeller

So far, hearing that cyber risks of the Capitol attack were low.

* Congress isn't one big network
* Vulnerable machines held unclassified files
* Hill leaks so much already that truly sensitive stuff is walled off
* Rioters weren't there long enough for thorough, careful access

The only computer reported stolen so far was from Senator Merkley's office. His staff declined to share details, citing an ongoing investigation.

For those wondering about the SCIFs, used for classified files and conversations, their doors were built to withstand embassy sieges, and they're swept for bugs before every use.

We haven't seen any indication that they were even targeted, much less seriously attacked.

Could one of the terrorists have seen a sensitive but unclassified email somewhere? Yes.

Could there have been Russian spies in the terrorist mob? Yes.

But there is no evidence for these claims. Hill IT staff will need to prioritize their response according to risk modeling.

One *real* problem I'm hearing about:

The House and Senate's central IT offices — which don't directly manage as much as you think — may have logs of some activity (email searches, shared drive access) but they will struggle to build a complete picture of what was opened & seen.

For one thing, they'll have to contact every office whose computers were accessed to determine whether it was a terrorist infiltrator or a staffer sheltering in place.

There's a lot we don't know, e.g.:

* Which computers auto-lock after a set time period? (Senate doesn’t have an auto-lock policy.)
* How robust is IT staff's central monitoring software?

Re: Merkley's laptop being stolen, all Senate computers purchased after October 2018 have been encrypted by default. Owners of computers purchased before that have to specifically request this.

I’m obviously not saying that there was zero risk — just that the risk is lower than you might imagine, depending on how many misconceptions you have about how Hill IT works.

Capitol security staff may just decide to inspect every machine in every compromised room. Better safe than sorry, I guess. But that will take a ton of time. The immediate response will prioritize the most likely issues.