"The voting machines are not connected to the internet" is a deceptive lie. They're using a "Zero Tunnel" network. See Verizon's 18 page White Paper, link below.

Municipal election modem's using Verizon's Private Network don't send data over the public Internet. Each cellular device connects to Verizon's Radio Access Network (RAN), which routes encrypted data through a Private Network Gateway - not an Internet gateway.

Note: there are a dozens ways this could be setup.
For standard setups, that gateway links to the county's internal router via a Virtual Private Network (VPN), a Multiprotocol Label Switching (MPLS), or a dedicated circuit.

But in a Zero Tunnel configuration, the system is mobile-to-mobile only: data moves within Verizon's private IP pools, forming a hub-and-spoke network where the county's central router (the "hub") communicates directly with municipal field devices (the "spokes").

Supposedly, no traffic leaves Verizon's closed system or touches the open Internet; instead, it tunnels privately through Verizon's infrastructure into the county's main network, creating a closed cellular backhaul path between local tabulators and the county office.

See how they get away with saying "not connected to the internet" - they configured the setup differently then used their own vernacular. They changed the words.

Here's the problem: the cellular network itself isn't "the internet," but it is still a routed IP network. Verizon's Private Network setup (including Zero Tunnel mode) creates a segregated subnet that bypasses public internet gateways.

However, it's still IP-routable within Verizon's backbone, meaning that any approved third party (like CrowdStrike's monitoring nodes or Dept. of Homeland Security's MS-ISAC's Albert sensors) can reach endpoints through the Verizon private backbone as long as they are authorized peers or VPN participants.

Guess what: Crowdstrike's Falcon Endpoint Services nor Albert Sensors are certified by the federal Election Assistance Commission nor by any Sec. of State or Commission of elections. Nor are the Cradlepoint routers - you'll see how in upcoming videos to be posted soon.

Thousands of counties have signed contracts with Crowdstrike or with the Center for Internet Security (non-profit of the fed. govt.) = Albert Sensors. **And they gaining access.**

The Cradlepoint routers, which are made in China (I've already published the federal Bill of Ladings in previous tweets), are not certified by anyone. The routers are made in a plant in China, shipped to Taiwan, relabeled/packaged, then put on a US flagged ship -

per FISMA/NIST requirements. It's a common scam for many key computer components the USA uses.

So even when a county says “it’s not connected to the internet,” what they mean is: it’s not accessible through the public Internet (e.g., Google, Comcast, etc.) - but it is accessible through Verizon’s internal routed infrastructure, which CrowdStrike or an Albert Sensor connects to via a service-level integration or VPN hub.

The election vote counts still pass through Verizon computer towers and computer servers.

Why chain of custody and security is a joke: Verizon controls addressing and routing - meaning they (and any integrated vendor like CrowdStrike or Albert) can see, trace, and reach the election devices inside their MPLS backbone (Multiprotocol Label Switching, its a data technique that uses labels to direct traffic across a network efficiently).

It is possible **one person** could access the vote counts and change an entire election, in particular see the vote counts and then tell bad actors who then know how many ballots to stuff into the box.

The Internet Protocol (IP) space is Verizon’s, then the “private” network belongs to Verizon, not the countys'.
The counties are a tenant, not the owners.

This is what allows CrowdStrike’s Falcon cloud software or the Albert sensor to maintain visibility - they rely on Verizon’s routing tables and IP pools to reach the Cradlepoint endpoints in real time. They can see all of the digital traffic of a county. This is under contract!

Bet your county supervisors are clueless to all this, ask them. Its worse, the Crowdstrike and Albert Sensor contracts mandate the counties give all their IP addresses to them. Crowdstrike is the corrupt company who set up the servers in Hillary Clinton's closet.

Case No. 2023CV001258 Peter Bernegger vs. Clerk of Outagamie County Exhibit B was introduced into evidence when I took the sworn deposition of Verizon employee Ms. Mangless. @hotgovernment1 @EmeraldRobinson @RealAlexJones @EagleEdMartin @HarmeetKDhillon @KurtOlsen_USA @ParikhClay @joeoltmannX @theprofsrecord @JanelBrandtjen @RonJohnsonWI @DanEastman2023 @KevinMoncla

Verizon 18 page White Paper:
issuu.com/electionwatch/…