BUZZ CHRONICLES > SOCIETY
Saved by @Alex1Powell
See On Twitter

# Twitter Thread by ■■ JFK 2 DJT ■■

**■■ JFK 2 DJT ■■**
@jfk2djt

### The Nashville Operation - A Battle in the War

### A thread exploring the Nashville bombing in the context of the 2020 Digital War (via SolarWinds) against the United States perpetrated by our enemies, likely China, Iran and/or Russia.

SolarWinds Hack

A digital "Pearl Harbor" moment for the United States, whoever was responsible had access to the keys to the kingdom for months during 2020, including sensitive military infrastructure. This is war!

https://t.co/pTJc1YBtO7

SunGard + SolarWinds

SolarWinds software company is owned by same company that owns SunGard, which essentially provides data center services. A secure place to host internet servers with redundant power and "big pipe" data connections.

https://t.co/U3P3SrrkM1

SunGard Data Center

In Nashville, around the corner from their "big pipe" connection, AT&T. Like any data center, highly secure. Only authorized personnel can enter, and even fewer can access the actual server rooms. Backup generators are available in case of power failure.

If the SunGard hardware was being used to "host" critical command and control software related to SolarWinds, the US powers would be very interested in gaining special access keys that are stored on the hard-drives of specific servers.

The Achilles heel of the data center security is it's power. A huge generator and large supplies of fuel are available in case of loss of grid power. With electricity the complex can stay staffed and secure, but without electricity the security features are disabled.

And if an extraordinary situation creates an environment where even the backup generator must be turned off and staff evacuated, that data center is vulnerable. Cameras can not record intruders. Alarms cannot sound.

And data could potentially be copied directly from hard-drives without needing grid power and without leaving a trace.

The bombing was done in a way to minimize risk to life, detonating early Christmas morning, only after a built-in warning system verbally warned people away. From media reports we know SunGard was directed to turn off it's backup generator by authorities, leaving them exposed.

With the area evacuated and data center empty, specially placed teams could easily complete such a mission leaving no trace.

The data would be used to build cryptographic keys to access data and evidence related to the SolarWinds hacking throughout their networks, and ultimately towards Avenging the act of war against the US military, government and commerce by the perpetrators of the SolarWinds hack.

@threadreaderapp unroll please