BEHIND LEGION OF DOOM: BREAKING "ENCRYPTED ELECTRONIC COMMUNICATIONS BETWEEN HIGH LEVEL AL QAEDA LEADERS"

[youtube]xY-wsEh6CZk[/youtube]

David Garteinstein-Ross, who did his own research into the Daily Beast Legion of Doom story, noted a couple of things via Twitter that I have been pointing to: the conference call behind the Legion of Doom scare wasn't the first intercept, and Al Qaeda leaders on the conference call (which Eli Lake clarified wasn't via telephone) assumed the call was secure.

> 3) There has been more than one intercept related to the plot. The report refers to a captured courier in addition to the conference call.
>
> 5) Many reactions to the report assume AQ completely broke OPSEC. The report states that AQ leaders assumed the call was secure.

And in the appearance above on MSNBC, he describes the conference call as,

> Encrypted electronic communications between high level Al Qaeda leaders in which they were discussing this plot.
>
> [snip]
>
> This is encrypted communication. It's hard to penetrate their communications. And if you make clear that we have, and which communications we've penetrated, then they're simply going to adapt.

In general, that suggests that something the government got from the courier allowed them to break the encrypted conference call. And, if Gartenstein-Ross is accurately informed, that we did, in fact, break their encrypted communications.

While that doesn’t prove or disprove my outtamyarse guess that the Tor compromise had a connection to Legion of Doom, it does make it more likely.

It also means the leaks are that much more damaging, in that they would have ended the period when we had location data on operatives they didn’t realize had been exposed.