“ENCRYPTION” IS JUST INTEL CODE FOR “FAILURE TO ACHIEVE OMNISCIENCE”

After receiving a briefing on the San Bernardino attack, Richard Burr went out and made two contradictory claims. First, Burr — and or other sources for The Hill — said that there was no evidence the Tashfeen Malik and Syed Rizwan Farook used encryption.

> Lawmakers on Thursday said there was no evidence yet that the two suspected shooters used encryption to hide from authorities in the lead-up to last week’s San Bernardino, Calif., terror attack that killed 14 people.
>
> “We don’t know whether it played a part in this attack,” Senate Intelligence Committee Chairman Richard Burr (R-N.C.) told reporters following a closed-door briefing with federal officials on the shootings.

That’s consistent with what we know so far. After all, a husband and wife wouldn’t need to — or have a way of — encrypting their communications with each other, as it would be mostly face-to-face. The fact that they tried to destroy their devices (and apparently got rid of a still undiscovered hard drive) suggests they weren’t protecting that via encryption, but rather via physical destruction. That doesn’t rule out using both, but the FBI would presumably know if the devices they’re reconstructed were encrypted.

So it makes sense that the San Bernardino attacks did not use encryption.

But then later in the same discussion with reporters, Burr suggested Malik and Farook must

have used encryption because the IC didn't know about their attack.

> Burr suggested it might have even played a role in the accused San Bernardino shooters – Tashfeen Malik and Syed Rizwan Farook – going unnoticed for years, despite the FBI saying they had been radicalized for some time.
>
> "Any time you glean less information at the beginning, clearly encryption probably played a role in it," he said. "And there were a lot of conversations that went on between these two individuals before [Malik] came to the United States that you would love to have some insight to other than after an attack took place."

This is a remarkable comment!

After all, the FBI and NSA don't even read all the conversations of foreigners, as Malik would still have legally been, that they can. Indeed, if these conversations were in Arabic or Urdu, the IC would only have had them translated if there were some reason to find them interesting. And even in spite of the pair's early shooting training, it's not apparent they had extensive conversations, particularly not online, to guide that training.

Those details would make it likely that the IC would have had no reason to be interested. To say nothing of the fact that ultimately "radicalization" is a state of mind, and thus far, NSA doesn't have a way to decrypt thoughts.

But this is the second attack in a row, with Paris, where Burr and others have suggested that their lack of foreknowledge of the attack makes it probable the planners used encryption. Burr doesn't even seem to be considering a number of other things, such as good operational security, languages, and metadata failures might lead the IC to miss warning signs, even assuming they're collecting everything (there should have been no

legal limits to their ability to collect on Malik).

We’re not having a debate about encryption anymore. We’re debating making the Internet less secure *to excuse* the IC’s less-than-perfect-omniscience.