# HOUSE HOMELAND SECURITY COMMITTEE APPARENTLY KNOWS LITTLE ABOUT HOMELAND SECURITY

Here are the first 36 words of an otherwise useful House Homeland Security Committee report on encryption:

> Public engagement on encryption issues surged following the 2015 terrorist attacks in Paris and San Bernardino, particularly when it became clear that the attackers used encrypted communications to evade detection—a phenomenon known as "going dark."

The statement has grains of truth to it. It is true that engagement on encryption surged following the Paris attacks, largely because intelligence committee sources ran around assuming (and probably briefing the White House) that encryption must explain why those same intelligence committee sources had missed the attack. It surged further months later when FBI chose to pick a fight with Apple over Syed Rizwan Farook's work phone which — it was clear from the start — had no evidence relating to the attack on it.

It is also true that ISIS had been using Telegram leading up to the Paris attack; in its wake, the social media company shut down a bunch of channels tied to the group. But there has never been a public claim the plotters used Telegram to plan their attack.

It is also true that an ISIS recruit, arrested and interrogated months before the Paris attack, had told French authorities he had been trained to use a Truecrypt key and an elaborate dead drop method to communicate back to Syria.

But it is not true that the Paris attackers used encryption to hide their plot. They used a great many burner phones, a close-knit network (and with it face-to-face planning), an unusual dialect. But even the one phone that had an encrypted product loaded on it was not using that service.

It is also not true that the San Bernardino attackers used encryption to evade detection. They used physical tools to destroy the phones presumably used to plan the attack. They hid a hard drive via some other, unidentified means. But the only known use of encryption — the encryption that came standard on Farook's work phone — was shown, after the FBI paid to bypass it, not to be hiding anything at all.

Now it's possible there was encryption involved in these attacks we don't know about, that HLSC has gotten classified briefings on. But even if there was, it could not very well have led to a public surge of engagement last year, because it would not be public.

There are reasons to discuss encryption. But factually false claims about terrorists' use of encryption are not among those reasons.

h/t to Access Now's Nathaniel White, who pointed out this bogosity on Twitter.

Update: See this Grugq post laying out what little encryption ISIS has been known to use in any attack.