WHAT CLAIMS DID THE INTELLIGENCE COMMUNITY MAKE ABOUT THE PARIS ATTACK TO GET THE WHITE HOUSE TO CHANGE ON ENCRYPTION?

I’m going to do a series of posts laying out the timeline behind the Administration’s changed approach to encryption. In this, I’d like to make a point about when the National Security Council adopted a “decision memo” more aggressively seeking to bypass encryption. Bloomberg reported on the memo last week, in the wake of the FBI’s demand that Apple help it brute force Syed Rezwan Farook’s work phone.

But note the date: The meeting at which the memo was adopted was convened “around Thanksgiving.”

> Silicon Valley celebrated last fall when the White House revealed it would not seek legislation forcing technology makers to install “backdoors” in their software — secret listening posts where investigators could pierce the veil of secrecy on users’ encrypted data, from text messages to video chats. But while the companies may have thought that was the final word, in fact the government was working on a Plan B.
>
> *In a secret meeting convened by the White House around Thanksgiving*, senior national security officials ordered agencies across the U.S. government to find ways to counter encryption software and gain access to the most heavily protected user data on the most secure

> consumer devices, including Apple Inc.’s iPhone, the marquee product of one of America’s most valuable companies, according to two people familiar with the decision.
>
> The approach was formalized in a confidential National Security Council “decision memo,” tasking government agencies with developing encryption workarounds, estimating additional budgets and identifying laws that may need to be changed to counter what FBI Director James Comey calls the “going dark” problem: investigators being unable to access the contents of encrypted data stored on mobile devices or traveling across the Internet. Details of the memo reveal that, in private, the government was honing a sharper edge to its relationship with Silicon Valley alongside more public signs of rapprochement. [my emphasis]

That is, the meeting was convened in the wake of the November 13 ISIS attack on Paris.

We know that last August, Bob Litt had recommended keeping options open until such time as a terrorist attack presented the opportunity to revisit the issue and demand that companies back door encryption.

> Privately, law enforcement officials have acknowledged that prospects for congressional action this year are remote. Although “the legislative environment is very hostile today,” the intelligence community’s top lawyer, Robert S. Litt, said to colleagues in an August e-mail, which was obtained by The Post, “it could turn in the event of a terrorist attack or criminal event where strong encryption can be shown to have hindered law enforcement.”
>
> There is value, he said, in “keeping our

> options open for such a situation."
>
> Litt was commenting on a draft paper prepared by National Security Council staff members in July, which also was obtained by The Post, that analyzed several options. They included explicitly rejecting a legislative mandate, deferring legislation and remaining undecided while discussions continue.

It appears that is precisely what happened — that the intelligence community, in the wake of a big attack on Paris, went to the White House and convinced them to change their approach.

So I want to know what claims the intelligence community made about the use of encryption in the attack that convinced the White House to change approach. Because there is nothing in the public record that indicates encryption was important at all.

It is true that a lot of ISIS associates were using Telegram; shortly after the attack Telegram shut down a bunch of channels they were using. But reportedly Telegram's encryption would be easy for the NSA to break. The difficulty with Telegram — which the IC should consider seriously before they make Apple back door its products — is that its offshore location probably made it harder for our counterterrorism analysts to get the metadata.

It is also true that an ISIS recruit whom French authorities had interrogated during the summer (and who warned them very specifically about attacks on sporting events and concerts) had been given an encryption key on a thumb drive.

But it's also true the phone recovered after the attack — which the attackers used to communicate during the attack — was not encrypted. It's true, too, that French and Belgian authorities knew just about every known participant in the attack, especially the ringleader. From reports, it sounds like operational security — the use of a series of burner phones – was more critical to his ability to move unnoticed through Europe. There are also reports that the authorities had a difficult time translating the dialect of (probably) Berber the attackers used.

From what we know, though, encryption is not the reason authorities failed to prevent the French attack. And a lot of other tools that are designed to identify potential attacks – like the metadata dragnet – failed.

I hate to be cynical (though comments like Litt's – plus the way the IC used a bogus terrorist threat in 2004 to get the torture and Internet dragnet programs reauthorized – invite such cynicism). But it sure looks like the IC failed to prevent the November attack, and immediately used their own (human, unavoidable) failure to demand a new approach to encryption.

Update: In testimony before the House Judiciary Committee today, Microsoft General Counsel Brad Smith repeated a claim MSFT witnesses have made before: they provided Parisian law enforcement email from the Paris attackers within 45 minutes. That implies, of course, that the data was accessible under PRISM and not encrypted.