FOR COUNTERTERRORISM EXPERTS, ABSENCE OF EVIDENCE EQUALS ENCRYPTION

The NYT has a fascinating story based on shared criminal files and attack review, describing what authorities currently know about how ISIS pulled off the Paris attack. It describes continued problems with transliteration (though it's not clear that played a role in this attack).

> "We don't share information," said Alain Chouet, a former head of French intelligence. "We even didn't agree on the translations of people's names that are in Arabic or Cyrillic, so if someone comes into Europe through Estonia or Denmark, maybe that's not how we register them in France or Spain."

It describes, over and over, the volume of burner and borrowed phones the attackers used, including a lot of calls that ended up being easy to trace.

> After numerous delays, one of the attackers began using a hostage's cellphone to send text messages to a contact outside. At one point, one of the gunmen turned to a second and said in fluent French, "I haven't gotten any news yet," suggesting they were waiting for an update from an accomplice. Then they switched and continued the discussion in Arabic, according to the police report.
>
> [snip]
>
> The attackers seized cellphones from the

> hostages and tried to use them to get onto the Internet, but data reception was not functioning, Mr. Goeppinger told the police. Their use of hostages' phones is one of the many details, revealed in the police investigation, pointing to how the Islamic State had refined its tradecraft. Court records and public accounts have detailed how earlier operatives sent to Europe in 2014 and early 2015 made phone calls or sent unencrypted messages that were intercepted, allowing the police to track and disrupt their plots. But the three teams in Paris were comparatively disciplined. They used only new phones that they would then discard, including several activated minutes before the attacks, or phones seized from their victims.
>
> [snip]
>
> Everywhere they went, the attackers left behind their throwaway phones, including in Bobigny, at a villa rented in the name of Ibrahim Abdeslam. When the brigade charged with sweeping the location arrived, it found two unused cellphones still inside their boxes.
>
> New phones linked to the assailants at the stadium and the restaurant also showed calls to Belgium in the hours and minutes before the attacks, suggesting a rear base manned by a web of still unidentified accomplices.
>
> Security camera footage showed Bilal Hadfi, the youngest of the assailants, as he paced outside the stadium, talking on a cellphone. The phone was activated less than an hour before he detonated his vest. From 8:41 p.m. until just before he died at 9:28 p.m., the phone was in constant touch with a phone inside the rental car being driven by Mr. Abaaoud. It also repeatedly called a

> cellphone in Belgium.

Remember, earlier reports on some of these same terrorists described them using a Moroccan dialect for which Belgian authorities, at least, did not have ready translators, which would make voice calls almost as effective as encrypted communications, especially so long as that common phone number in Belgium remained unknown. The story describes the attackers using Arabic, though doesn't say whether it was a dialect.

> After numerous delays, one of the attackers began using a hostage's cellphone to send text messages to a contact outside. At one point, one of the gunmen turned to a second and said in fluent French, "I haven't gotten any news yet," suggesting they were waiting for an update from an accomplice. Then they switched and continued the discussion in Arabic, according to the police report.

But it then makes an enormous logical leap, from the very first line of the story, that absence of emails equates to some operational security pertaining to emails.

> Investigators found crates' worth of disposable cellphones, meticulously scoured of email data. [See note]
>
> [snip]
>
> According to the police report and interviews with officials, none of the attackers' emails or other electronic communications have been found, prompting the authorities to conclude that the group used encryption. What kind of encryption remains unknown, and is among the details that Mr. Abdeslam's capture could help reveal.
>
> [snip]

> Most striking is what was not found on the phones: Not a single email or online chat from the attackers has surfaced so far.

What seems most likely from this description is that for phones terrorists used as burners, they simply didn't load them with apps to conduct more extensive communication. And why would they, especially if they knew from past reporting that their language was proving hard to "decrypt" for authorities, even with time?

Then there's this description of a laptop that might have used encryption.

> One of the terrorists pulled out a laptop, propping it open against the wall, said the 40-year-old woman. When the laptop powered on, she saw a line of gibberish across the screen: "It was bizarre — he was looking at a bunch of lines, like lines of code. There was no image, no Internet," she said. Her description matches the look of certain encryption software, which ISIS claims to have used during the Paris attacks.

I asked one of the reporters on this story, Rukmini Callimachi, whether the computer showed up in the report; it did not. Which either suggests it was destroyed in one of the suicide vest explosions beyond all forensic use, or wasn't one of the terrorist laptops at all (or was misremembered by the eyewitness, which would be unsurprising given the unreliable nature of even witnesses who are not, by nature of being hostages, very stressed).

Yet even if this computer had full disc encryption (as opposed to just being a Linux machine, as some people have suggested), there's no reason to assume there'd be emails. And, as the story makes clear, the phone recovered outside of Bataclan was not encrypted (this was the one that had a text on it).

> As the bodies of the dead were being bagged, the police found a white Samsung phone in a trash can outside the Bataclan.
>
> It had Belgian SIM card that had been in use only since the day before the attack. The phone had called just one other number — belonging to an unidentified user in Belgium. Another new detail from the report showed that the phone's photo album police found images of the concert hall's layout, as well as Internet searches for "fnacspectacles.com," a website that sells concert tickets; "bataclan.fr"; and the phrase "Eagles of Death at the Bataclan."
>
> [snip]
>
> Even though one of the disposable phones was found to have had a Gmail account with the username "yjeanyves1," the police discovered it was empty, with no messages in the sent or draft folders.

Note, that account name is very French, not at all similar to the names of the perpetrators (see the list here), which makes me wonder whether it's an artefact of a prior owner, from whom this phone could have been stolen.

My suspicion is that, as had been reported, rather than emails ISIS relied on Telegram, but used in such a fashion that would make it less useful on burner phones ("secret" Telegram chat are device specific, meaning you'd need a persistent phone number to use that function). But if these terrorists did use Telegram, they probably eluded authorities not because of encryption, but because it's fairly easy to make such chats temporary (again, using the secret function). Without Telegram being part of PRISM, the NSA would have had to obtain the metadata for chats via other means, and by the time they IDed the phones of interest, there may have been

no metadata left.

The authorities now have a great deal of evidence on these terrorists. And what it shows is that burner phones used with discipline serve as a far more important operational security tool than encryption. Indeed, at this point, the authorities only claim the terrorists used encryption because they have no evidence of it!

And yet, that doesn't appear to have stopped the IC from convincing Obama that the Paris terrorists used encryption and so we have to break it here.

Note: On Twitter, Callimachi acknowledged that that first line makes no sense and said she would try to have it changed.

Update: And now it reads like this:

> Investigators found crates' worth of disposable cellphones.