IT'S NOT JUST WHETHER NIDAL HASAN'S EMAILS STUCK OUT, IT'S WHETHER ABDULMUTALLAB'S DID

I've been meaning to return to the Webster report on Nidal Hasan's conversations with Anwar al-Awlaki. This conversation between Gunpowder & Lead and Intelwire about how alarming those emails were will be a start provides a good place to start.

Hasan's emails should have raised more concern—but probably didn't because of the sheer volume of Awlaki intercepts

G&L notes that certain details from the emails—such as his invocation of Hasan Akbar, a Muslim-American soldier who killed two officers in Kuwait—as an example that should have raised more concern than it did.

> But more significant, his question to Awlaki didn't actually deal with the valid question that he raised, the feeling of inner conflict between one's faith and serving in the U.S. military. Instead, he leaped right to a question that should rightly trigger alarm: *if Hasan Akbar died while attacking fellow soldiers, would he be a martyr*? Hasan skipped over questions about whether serving in the U.S. military is religiously acceptable; whether going to war against fellow Muslims is a violation of religious principles. Instead, in addressing "some" soldiers who felt conflicted about fighting fellow Muslims, Hasan right away asked whether it was permissible to kill other U.S. soldiers in the way Hasan Akbar.

After a close analysis of a number of the emails, G&L refutes the representation of these emails as “fairly benign.”

I agree with that assessment (and would add that the suggestion, in a February 22, 2009 email, that Hasan was donating to entities that his mosque would not is another troubling detail). But I also agree with Intelwire. These emails, from an Army officer, surely merited more attention. But these emails, as they likely appeared among the stream of Anwar al-Awlaki communications, probably did not stick out.

> Based on who Hasan was (a military officer), who he was talking to (a suspected 9/11 accomplice), and the fact he repeatedly tried to get Awlaki’s attention using a variety of stratagems, the case should have been escalated and Hasan’s superiors should have been informed.
>
> But when you place the *content* of Hasan’s messages alongside all the other raw intelligence that counterterrorism investigations generate, it’s extremely hard to argue from a subjective, non-psychoanalytical reading that they represented a red flag.

Which is why this report has seemed poorly scoped to me. Because not only did Nidal Hasan’s emails fail to trigger further attention, but Umar Farouk Abdulmutallab’s contacts with Awlaki before Fort Hood did too.

In spite of the fact that the FBI had two people spending a significant chunk of each day (they claimed it took 40% or 3 hours of their work day; 88) reviewing communications tied to Awlaki, in spite of the fact that two men about to attack the US were in contact with Awlaki, “the FBI’s full understanding of Aulaqi’s operational ambitions developed only after the attempted bombing of Northwest Airlines Flight 253 on Christmas Day 2009.” (72)

The government also failed to respond to Abdulmutallab intercepts leading up to the Fort Hood attack

Consider: according to the report itself, Robert Mueller formally asked William Webster to conduct this inquiry on December 17, 2009 (though Webster's appointment was reported over a week before then). Just 8 days later, another terrorist who had been in contact with Awlaki struck the US. Just 5 days after that, sources started leaking details of NSA intercepts from 4 months earlier (so around August) that might have warned about the attack.

> Intelligence intercepts from Yemen beginning in early August, when Abdulmutallab arrived in that country, contained "bits and pieces about where he was, what his plans were, what he was telling people his plans were," as well as information about planning by the al-Qaeda branch in Yemen, a senior administration official said. "At first blush, not all these things appear to be related" to the 23-year-old Nigerian and the bombing attempt, he said, "but we believe they were."

It's unclear how many of these intercepts were directly between Abdulmutallab and Awlaki, and therefore presumably reviewed by the FBI team in San Diego. But at least according to the sentencing materials submitted in the Abdulmutallab case (there are reasons to treat this with a bit of skepticism), there were substantive communications between Awlaki and Abdulmutallab.

> Defendant provided this individual [who offered to connect him with Awlaki] with the number for his Yemeni cellular telephone. Thereafter, defendant received a text message from Awlaki telling defendant to call him, which defendant did. During their brief telephone conversation, it was agreed

> that defendant would send Awlaki a written message explaining why he wanted to become involved in jihad. Defendant took several days to write his message to Awlaki, telling him of his desire to become involved in jihad, and seeking Awlaki's guidance. After receiving defendant's message, Awlaki sent defendant a response, telling him that Awlaki would find a way for defendant to become involved in jihad.

Now, it's possible this communication didn't show up in the San Diego stream. Maybe the NSA didn't share all its Awlaki intercepts with the San Diego team. The report notes that Awlaki and his allies were using means to hide their contacts (127). The report notes some forms of VOIP are not included under CALEA, which may have affected Abdulmutallab's call. (128) And the month after the Abdulmutallab attack and after Pete Hoekstra revealed the NSA intercepts on Awlaki, he allegedly implemented a sophisticated encryption system with Rajib Karim. But if the Awlaki collection, as it existed in 2009, failed both because of volume and because of technical reasons, shouldn't those be part of the same inquiry?

By the end of December 2009, the FBI and NSA knew they had collected, reviewed, and failed to adequately respond to intercepts from two future terrorists. Why not include both in this study?

Hasan's contacts (and presumably Abdulmutallab's) were dissociated needles in an Awlaki haystack

The Webster report doesn't provide exact details of how much intelligence was coming in on the Awlaki investigation. They redact the number of leads, investigations, and Information Intelligence Reports the intercepts produced—though they appear to be 3-digit numbers (see page 35). The report suggests that the San Diego team focused attention on Awlaki-related intercepts starting on March 16, 2008

(87; interestingly, in the extension period for PAA and before FAA imposed new protections for Americans overseas). Between March 2008 and November 2009, the JTTF team in San Diego reviewed over 29,000 intercepts. And the volume was growing: in earlier phases of the Hasan investigation, the San Diego team was averaging 1,420 intercepts a month; that number grew to 1,525 by the time of the Fort Hood attack. The daily average went from 65-70 intercepts a day to 70-75, though some days the team reviewed over 130 intercepts. And while he obviously had reasons to play up the volume involved, the Analyst on the San Diego team considered it a "crushing volume" of intercepts to review. Discussions of the volume of intercepts appear on page 35, 36, 46, 61, 87, 88, 92.

In any case, the emails between Hasan and Awlaki made up just one quarter of one percent of the volume the FBI reviewers reviewed over this period. While we don't know how these emails compared to the rest of the traffic (a point the Webster report makes, (88) it is clear they made up just a tiny fraction of what the FBI reviewed.

There are two factors that must have made this review process more difficult.

First, the FBI's database of intercepts sucked. When the first Hasan intercepts came in, it allowed only keyword searches; tests the Webster team ran showed it would have taken some finesse even to return all the contacts between Hasan and Awlaki consistently. More importantly, it was not until February 2009 that the database provided some way to link related emails, so the Awlaki team in San Diego relied on spreadsheets, notes, or just their memory to link intercepts. (91) But even then, the database only linked formal emails; a number of Hasan's "emails" to Awlaki were actually web contacts, (100) which would not trigger the database's automatic linking function. In any case, it appears the Awlaki team never pulled all the emails between Hasan and Awlaki and read them together, which

would have made Hasan seem much more worrisome (though when the San Diego agent set the alert for the second email, he searched and found the first one).

In addition, the Agent in charge of the investigation took on a supervisory role in mid-July 2009, just before Abdulmutallab came on the scene. (45) Given that the computer didn't allow for any institutional memory, losing an investigative team member would effectively lose the work on any given investigation.

One more factor would have made it harder to respond appropriately to early Abdulmutallab intercepts. At least some of those reportedly needed to be translated (this also suggests that some of the most interesting intercepts involving Abdulmutallab weren't between Awlaki and the Nigerian, as English would be the natural language for the two to converse in).

Even tracking the communications of one terrorist radicalizer, we're drowning in data

All of which suggests we're still collecting more information than we can even analyze. Whatever else I've said about the government's evidence against Awlaki, I absolutely believe he was an obvious target for collection. But if we don't have the technical capabilities to exploit even that one stream, what does that say about our intelligence gathering?

The Webster report does say that many of the problems with FBI's intercepts database were fixed with a September 2011 update. And FBI changed training and access rules before that point to make sure key members of the JTTFs can use the database. But several of the recommendations made by the Webster team pertain to enhancing the database with both hardware and software improvements.

One of the big takeaways from the Webster report, it seems to me, is we were asking FBI officers to analyze a flood of data using the most archaic tools. Sure, there was reason enough they should have escalated the

investigation into Nidal Hasan. But far more attention needs to be focused on our continued data failures, particularly among the belief more data is a cure-all.