Intelligence Functions: Signals Intelligence (SIGINT)

The other major collection discipline besides human intelligence that is most often used in counterterrorism is signals intelligence, or SIGINT, to use the term of art. That means basically the interception of electronic communications of any sort. And here in the United States, it's practiced most extensively by the National Security Agency, headquartered out at Fort Meade. SIGINT, or SI, as it's sometimes also called, is sometimes taken as the most definitive and conclusive form of intelligence, about especially, past terrorist attacks. Because it's seen as not just someone reporting about something that he heard or saw, but is seen as direct evidence.

[SIGINT INTERCEPTS]

SIGINT is often taken as the most conclusive form of intelligence, especially when it comes to proving responsibility for some past terrorist attack. For example, back in 1986 when the Libyan government was behind the bombing of a nightclub in Berlin that was frequented by U.S. servicemen, it was SIGINT, and specifically some intercepts of Libyan government communication that the Reagan administration later made public, that were taken as the conclusive proof of Libyan responsibility for that bombing that had killed US servicemen.

Well, despite the advantages of SIGINT, it like human intelligence has its limitations as well. And there are two main ones when it comes to SIGINT. One is that terrorists expect that their intercepted communications will be used. And when they talk on the telephone or use the Internet or any other kinds of electronic means, they're generally very careful about not saying explicitly what they are really doing.

So they use code words. Something might be referred to as a tomato when they're really talking about explosives. Or they might refer to a wedding when they're really talking about a terrorist attack. So part of the task for intelligence analysts, when they intercept that kind of message, is to figure out exactly what they're talking about. And sometimes that's not all that easy.

The other major limitation is that terrorists may not use electronic communications at all, precisely because they expect it to be intercepted. And so they instead use human couriers, or face-to-face contact or some other means. But at least that has the advantage of forcing the terrorist to use means that can be exploited in other ways. For example, when Osama bin Laden was finally located in his hideout in Abbottabad, Pakistan, it was a courier that he was using and relying on instead of electronic communications that provided the key means to identify the house that he was hiding out in.