Harvard National Security Journal Forum

Connecting the Dots and the Christmas Plot

Paul Rosenzweig

"We slipped up." That's what Patrick F. Kennedy, the Undersecretary of State for Management, said at a Senate hearing last week about the Christmas day bomb plot and the arrest of Umar Farouk Abdulmutallab.

He has a gift for understatement.

But the real question isn't whether we "slipped up"—everyone knows we did. It's rather how and why we did. The truth is that this was a failure of policy, not of law. We did it to ourselves. In the immediate aftermath of 9/11 the Defense Advanced Research Projects Administration (DARPA) began work on techniques of data analysis called "knowledge discovery" techniques. They gave the project an unfortunate name—Total Information Awareness—and did a poor job of reassuring troubled civil libertarians that the program would not become a "Big Brother" tool. The research was killed. But the concept behind the research was visionary and those are precisely the tools that, if we had them today, would have made it more likely that we would have connected the "dots" of the Abdulmutallab plot. Here's why:

The evidence is increasingly clear that the problem was not a failure of intelligence collection. If public news reports are to be believed, it now appears that there was a reasonable amount of information about or related to Abdulmutallab. According to the New York Times, we knew about possible underwear bombs, we knew about an unnamed Nigerian who might strike America during Christmas, and we knew from his father that Abdulmutallab had become increasingly radicalized and had been in contact with Anwar al-Alwaki, a Yemeni radical. We had a partial name for a terror plotter—"Umar Farouk." And we may even have known (though it is not yet certain) that the British had denied Abdulmutallab a visa, a boon that we, on the other hand, had granted him.

But what to do with all that information? And why didn't the dots get connected in the way we would have wanted? Some, like my colleague Nathan Sales, think that there still remain institutional barriers to sharing information and that means that agencies are still hoarding data. No doubt.

But there is a deeper and more insidious problem—one that institutionally we have yet to overcome. The problem is that there is simply too much information out there. And information without context is nothing but noise. Only context and analysis transform information into knowledge and only knowledge is actionable.

Consider: The National Counter Terrorism Center (NCTC) is one of two institutions we rely on to conduct all-source analysis of terror threats (the other is the CIA). The NCTC's computer systems have links to more than 30 separate government systems, with more than 80 distinct databases. According to the Director of National Intelligence, Admiral Dennis Blair, each day the NCTC gets thousands of pieces of intelligence from around the world, reviews thousands of names, and puts 350 new names onto the watchlist—the list that Adbulmutallab was not put on.

This is a veritable flood of data. In hindsight, of course, it is very easy to see the pieces that connect together to form a picture of Abdulmutallab's plot. But those 10 or so bits of information were floating in an ocean of other data—literally millions of different individual entries from thousands of different sources in a host of different databases.

Hindsight is always 20/20. What we need is foresight. And the problem is that we continue to fixate on a human solution to our lack of foresight. We continue to rely on the intuition of analysts to provide the insight we need. It is all well and good to say "with the NSA intercept about a Nigerian we should have started looking at all Nigerians" or "we should have begun looking at everyone named Umar Farouk," but those leaps of insight and anticipation are not routine—they require analysis and consideration. And that requires time—time to ponder the necessity of making precisely that inquiry.

But time is what our analysts don't have. At least not enough of it. Not with the flood of data we are seeing. They have to prioritize and move certain lines of inquiry to the top of the pile. Probably, as Admiral Blair has said, the warning from Abdulmutallab's father should have moved the "Yemen/Nigeria/Bomb" issue to the top of everyone's pile. But as that question moves up to the top, other intelligence questions move down. The truth is that not all of the pieces of information rise above the noise level . . . and so long as we rely on human intuition to tell us what to pull out of the noise and what not to, we are going to make mistakes.

What we lack is not human intuition. Rather we lack the tools to make human intuition effective and automated. The head of the NCTC told a rather shocked Senate committee the other day that, in effect, NCTC analysts don't have a "Google-like" tool for database inquiries. They can't, for example, simply type in "Umar Farouk" and pull up all the pages with links to that name.

But even that wouldn't be enough—because there would likely still be far too many "Umar Farouk" pages for any analyst to review (especially if instead the name we had was, for example, "Omar Abdul"). What is necessary, as the Markle Foundation has said persistently, is for us to authorize and invest in tools that allow for automated analytics—things like tagged data (so that corrections to information are automatically transmitted for updates), identity resolution techniques (so that "Umar" and "Omar" are both considered), and persistent queries (so that a question that an analyst asked last month about Umar Farouk persists in the databases and is automatically linked to a father's warning about his son Umar when that comes in three weeks later). We need automated knowledge discovery systems—ones that run continuously and repeatedly so that every day we check for new information about "Umar Farouk" and about all the other hundreds of thousands of intelligence leads. These are tasks that take time, and time is what computers have plenty of.

We don't have those tools now. In part it's a question of investment and development. But at its core it is a question of policy and politics. Without the tools needed, we develop what Jeff Jonas calls "enterprise amnesia." He's right, and it's our own fault.

All decisions have consequences. Our decision to stop research on data analytic tools back in 2003 has led, in an almost straight line, to our analysts' difficulty in sifting the signal of a real terrorist, like Abdulmutallab, from the noise of thousands of bits of data. It's time to rethink our priorities and our policies.

—Paul Rosenzweig is the Principal at Red Branch Consulting PLLC and the former Deputy Assistant Secretary for Policy at the Department of Homeland Security.