Discussion Point: It’s not Big Data, but Little Data, that Prevents Terrorist Attacks.

The following is an editorial authored on July 25, 2013 by Erik Dahl of the Naval Postgraduate School and member of the START Consortium (National Consortium for the Study of Terrorism and Responses to Terrorism, a centre of excellence of the U.S. Department of Homeland Security based at the University of Maryland).

Many Americans are worried by what we have been learning about the National Security Agency (NSA) and its extensive surveillance programs. It appears to many of us that the government wants to snoop into every aspect of our lives, including “metadata” about our phone calls, information about our Internet use, and who knows what else. This concern is understandable, because these intelligence collection programs do appear to suck in a tremendous amount of data about ordinary Americans—not to mention about people from other countries. And American history shows that intelligence and law enforcement agencies often start out gathering information for a good purpose, but then mission creep sets in and they collect more, and use it for other purposes, than was originally intended.

What should we make of all this? It helps to start by understanding how the data collected by the NSA programs may be useful to the U.S. intelligence community. We don’t actually know much about these programs, of course, beyond what has been leaked by Edward Snowden and the claims by intelligence community officials that this data has helped to stop a number of terrorist plots. But from what has been revealed publicly, it seems that these collection programs are useful for what is often the first part of any intelligence effort: gathering a lot more information than is actually needed. This first step is sometimes called a broad area search, as intelligence agencies look in a lot of places, gathering a lot of useless information, before they find the clues that help them narrow the search down to the second step, a focused search for useful, actionable intelligence.

This two-step approach was used in the search for Osama bin Laden. After the 9/11 attacks he could have been anywhere, so the intelligence community spent a lot of time running down leads that led to nowhere. But eventually they found the clues that pointed them toward bin Laden’s courier, and that’s where the focused search began, leading them to the compound in Abbottabad, Pakistan.

We have learned from the Snowden leaks and official statements that the U.S. intelligence community, led by the NSA, has found some ingenious and technically legal ways to gather up huge amounts of data that they might need some day to catch terrorists—or better yet, to stop them before they conduct attacks. In other words, intelligence agencies have been collecting big haystacks of data, just in case they need it. And when they want to use it, such as to see what other phone numbers are connected to a number they obtained from a terrorist suspect, they try to use data mining tools to find the needle in that haystack.
How important is that big data? Some critics argue that such vast collection programs are unlikely to be useful, either because the NSA will never be able to make sense of it all, or because these programs are likely to only catch crooks with Yahoo email accounts, or those who are foolish enough to type into Google, “How do I make a bomb?” Others argue the opposite case, that all of this big data—such as the telephone numbers we dial—can enable the intelligence community to pry into the personal lives of millions of Americans.

The truth is probably somewhere in the middle, even assuming intelligence agencies are able to develop data mining tools that allow them to make sense of this flood of information. Amid all the discussion about big data, metadata, and data mining, it’s important to realize that it’s not big data that stops terrorist plots or prevents other bad things from happening. For that, little data is critical: the little pieces of information, usually the actions and behaviors of individuals, that gives something away. Big data is important, and the intelligence community can learn an awful lot about all of us through analyzing our metadata. But terrorist attacks don’t get prevented by computer algorithms, and people don’t get arrested—at least we hope they don’t—on the basis of analysis of their metadata.

Our government hasn’t been able to do a very good job of explaining to the public what it has been doing, partly because intelligence agencies are often unable to talk about their successes for fear of revealing their sources and methods. That’s why officials have said that a number of plots and attacks have been foiled, but they haven’t provided much specific information about those cases that wasn’t already in the public record.

Research I am currently conducting for the National Consortium for the Study of Terrorism and Responses to Terrorism (START), together with my colleagues Martha Crenshaw and Margaret Wilson, can shed some light on how this NSA data may be used. We are studying unsuccessful terrorist plots, in hopes of finding out what tools and techniques are the most useful in preventing attacks.

One finding supports the NSA’s argument that the data they are collecting can be useful in preventing future attacks. Opponents have suggested that the NSA data might only be useful in tracking down terrorists after the fact; because those haystacks of information are not apparently being looked at in real time, they are unlikely to help prevent future attacks. But the history of terrorist plots and attacks within the United States since 9/11 shows that most plots take a long time to develop. Even terrorist actions involving only one or two people typically take months or even years to plan and attempt. This is good news, because it gives law enforcement time to discover what’s going on, and it also gives the NSA time to search those haystacks it’s been collecting.

But another one of our findings is that the most effective tools in preventing terrorist attacks are relatively simple, old fashioned police methods, such as the use of undercover officers, informants, and tips from the public. This is especially true for domestic plots and attacks: of the 109 failed plots within the United States since 9/11, more than 75 percent were foiled at least in part because of traditional law enforcement methods, and not—from what we can gather—from NSA surveillance. Thus it is not surprising that government officials have said most of the 50 or so plots that have been foiled by the NSA monitoring programs were overseas. In other countries we can’t necessarily rely on local authorities, and spying—whether conducted by the NSA or the CIA—is a critical tool for our national security. But
here in the U.S., the most important terrorism prevention tool remains the country’s 800,000 police officers, deputy sheriffs, and other local law enforcement officials, supported by members of the public who "see something and say something," calling authorities when something doesn’t look right.

These NSA programs do appear to be important for preventing terrorist attacks, and they make sense from an intelligence perspective. But their greatest value concerns threats overseas, and this is probably a good thing, because it means that if the programs are managed properly, and if our intelligence oversight mechanisms work as they should (which are admittedly big if’s), the NSA collection of big data will have relatively little impact on most Americans’ lives.

--------------------------------------------------------------------------------

1 Erik J. Dahl is an assistant professor of national security affairs at the Naval Postgraduate School in Monterey, California, where he teaches in the National Security Affairs Department and the Center for Homeland Defense and Security. His research and teaching focus on intelligence, terrorism, and international and homeland security, and he is the author of “Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond” (Georgetown University Press, October 2013). He retired from the U.S. Navy in 2002 after serving 21 years as an intelligence officer, and received his Ph.D. from the Fletcher School of Tufts University. The views presented here are those of the author, and do not necessarily represent the views of the Naval Postgraduate School or the U.S. government.

2 For earlier findings from this research see Erik J. Dahl, “The Plots that Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks against the United States,” Studies in Conflict and Terrorism 34, no. 8 (August 2011). I update this research in my new book Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond (Georgetown University Press, October 2013).