Leaked docs give new insight into NSA's searches (Update 2)

July 31 2013, by Raphael Satter

Demonstrators take part in a protest against the US National Security Agency (NSA) collecting German emails, online chats and phone calls and sharing some of it with the country's intelligence services in Berlin on July 27, 2013. A secret surveillance system known as XKeyscore allows US intelligence to monitor "nearly everything a typical user does on the Internet," according to leaked documents.

Documents published by the Guardian newspaper are providing new insight into the National Security Agency's surveillance of world data,

giving an over-the-shoulder look at the programs and techniques U.S. intelligence analysts use to exploit the hundreds of billions of records they gather each year.

Dozens of training slides published Wednesday divulge details about XKeyscore, one of a family of NSA programs that leaker Edward Snowden says has given America the ability to spy on "the vast majority of human communications."

Some of the slides appear to carry screenshots showing what analysts would see as they trawled the intercepted conversations and include sample search queries such as "Show me all encrypted word documents from Iran" or "Show me all the word documents that reference Osama Bin Laden."

One question-and-answer slide asks what to do if a terror cell isn't associated with any particular search term. The answer: Look for "anomalous events," which the NSA defines as "someone whose language is out of place for the region they are in" or, rather more vaguely, "someone searching the web for suspicious stuff."

In an indication of the program's importance, one slide says that XKeyscore has led to the capture of more than 300 terrorists. In a statement, the NSA said that figure only included captures up to the year 2008, and pushed back against any suggestion of illegal or arbitrary collection of data.

"These types of programs allow us to collect the information that enables us to perform our missions successfully—to defend the nation and to protect U.S. and allied troops abroad," the statement said.

How and from where the program harvests its information isn't completely clear, nor is it obvious how XKeyscore fits in with other

recently revealed NSA activities, such as the PRISM program, which draws data from Silicon Valley firms.

"It's hard to tell what this is without some context," said security researcher Ashkan Soltani, who has been following the NSA revelations.

But hints as to the program's size and scope are scattered across the documents. One slide said XKeyscore was supported by 700 servers and 150 sites across the globe, and the volume of data available to analysts through XKeyscore appears to be vast.

The Guardian quoted another slide as saying that nearly 42 billion records had been captured by the system during a one-month period in 2012. So much content was being collected, the newspaper said, that it could be stored only for short periods of time—generally just a few days.

"At some sites, the amount of data we receive per day (20+ terabytes) can only be stored for as little as 24 hours," the paper quoted one document as saying.

The leaked documents also give new insight into how analysts determine that their target is a foreigner—a key issue thrown up in the debate over the American surveillance program. In a statement broadcast in June, Snowden warned he had the authority to spy on any American he pleased—"you, your accountant, to a federal judge, to even the President if I had a personal email."

The NSA has strongly denied that claim, and on Wednesday it repeated past assurances that it had "stringent oversight and compliance mechanisms built in at several levels" and that analysts were unable to "operate freely."

The new documents may provide fodder for both sides of the argument.

On the one hand, it appears that NSA analysts were required to fill out forms asserting that their target was a foreigner before they could pore over the intercepted data.

On the other hand, the forms published by the Guardian did not appear terribly exhaustive. One was a multiple-choice list explaining why a target was believed to be foreign (one option: "Phone number is registered in a country other than the US.") Another form, for reading intercepted emails, had a field for "justification," but the brief sample justification provided appeared to be only five words and refer vaguely to a "ct target" in "africa."

Like past stories on NSA surveillance, the Guardian's most recent article drew on documents supplied by Snowden to journalist Glenn Greenwald in Hong Kong, according to newspaper spokesman Gennady Kolker. They're the first to have been published in the Guardian since Snowden, who remains stuck at a Moscow airport, applied for temporary asylum in Russia on July 16.

It's not clear whether that may complicate the leaker's asylum bid.

Russian President Vladimir Putin said he'd be inclined to accept the bid on condition that Snowden agreed not to hurt U.S. interests—implying that the American would have to stop spilling U.S. secrets if he wanted safe harbor. But Snowden's Russian lawyer, Anatoly Kucherena, said Wednesday that the material for the article was provided to the media long before Snowden promised to stop leaking.

"He warned me that he had already sent to the press an array of revealing information and secret documents and, unfortunately, could not stop its publication," Kucherena was quoted as saying by the Interfax news

agency.