computer center

(S//SI//REL) Intro: Here in S2F, we've had great success using systems that buffer full-take audio collection for a nominal 30 days -- these systems have led to real breakthroughs in target discovery -- and we wanted to alert other analysts to their potential. Collectors: please take note of how beneficial these types of collectors can be to analysts, as compared to more traditional models.

(S//SI//REL) SOMALGET is a family of collection systems which greatly facilitate and make possible remarkable new ways of performing both target development[1] and target discovery.[2] Significant analytic breakthroughs and successes in both areas have been made by SID analysts in the two countries where SOMALGET accesses currently exist (i.e., [redacted] and the Bahamas).

(U) **How It Works:**

(S//SI//REL) SOMALGET collection systems ***forward full-take metadata in real time and buffer full-take audio for nominally 30 days.***[3] It makes possible the selection of audio content against the buffered data after the fact, in near real-time, or up to 30 days later. This ability is dubbed "*retrospective retrieval*." The power of retrospective retrieval in facilitating target development or discovery lies in its ability to permit the analyst to selectively retrieve audio content and immediately validate his/her tentative analytic conclusions derived from metadata.

- (TS//SI//REL) SOMALGET access to Bahamian GSM communications has led to the ***discovery of international narcotics traffickers and special-interest alien smugglers.*** This access -- together with our use of methods that take advantage of targets' behavioral patterns[4] -- have allowed our S2F analysts to gain a firm understanding of the targets' activities even when these contacts occurred prior to their discovery.

(U) **More to Come?**

(S//SI//REL) These successes, which depend on access to buffered audio files that may be associated with selectors not tasked to the collection asset in question, ***argue in favor of a collection methodology for telephony that may be viewed as analogous to XKEYSCORE. That is, we buffer certain calls that MAY be of foreign intelligence value for a sufficient period to permit a well-informed decision on whether to retrieve and return specific audio content.*** With proper engineering and coordination, there is little reason this capability cannot expand to other accesses (besides [redacted] and the Bahamas), provided compatible hardware and interfaces are developed and deployed.[5]

(U) Notes:

1. (U) Target development = the process by which an analyst can **extend his/her knowledge of a known target** by observing elements of metadata that relate to that target.

2. (U) Target discovery = the process whereby an analyst can **discover targets by observing metadata as it relates to behaviors** characteristic of his/her target set, regardless of whether or not the newly discovered selectors are related to known targets.

3. (S//SI//REL) The nominal "30 days storage" actually varies depending upon on space, power, and observed activity levels.

4. (TS//SI//REL) Observing that targets tend to use prepaid calling cards in an attempt to mask the destination of telephone calls, S2F focused on mobile identifiers in number ranges that represent newly activated accounts. We have also used SMS text messages to identify and retrieve audio of interest.

5. (S//SI//REL) Storage capacity is directly related to the amount of disk storage that can be deployed. When deployed against entire networks, as SOMALGET is, the back-end database and processing required for interactive search and retrieval of cuts also requires enterprise-class data warehousing and high-performance processing to manage the vast amount of data captured. Currently this warehouse dynamically manages roughly 5 billion call events, with the capacity to expand well beyond our current target communications. This retrospective retrieval infrastructure is web based and is already in place. As noted, with proper engineering and coordination, there is little reason this capability cannot expand to other accesses, provided compatible hardware and interfaces are developed and deployed.