___

(U) Data Acquisition Update

FROM: ███████████
SID's Deputy Director for Data Acquisition (S3)
Run Date: 08/20/2004

(U//FOUO) It's time that we brought you up-to-date with some recent and on-going activities affecting Data Acquisition. Today we'll concentrate on work meant to connect the great efforts underway in our line organizations and around the extended enterprise.

(TS//SI) A recent SID Today article is a great illustration of why this "glue logic" is vital. The article passed on kudos to a whole host of SIGINTers who were instrumental in the May 30th capture of an important terrorist named Umar Baziyani. It's a wonderful example of seamless interaction with the CT product line, field elements, and tactical units in Iraq, and we plan to tell this story in greater depth later. For now, here are a few themes that can be drawn from it and similar operations:

1. (TS//SI) Metadata collection and SIGINT Development drove the operation, making it possible to map logical communication data into physical locations, and ultimately to tip tactical units to target location and activity.

2. (TS//SI) Highly interactive use of diverse accesses was critical. Warranted collection pointed to target locations in cyberspace; computer network exploitation added informative tags to internet café data to allow collection at Menwith Hill.

3. (TS//SI) Tracking Iraqi internet users, and similar tough challenges, requires increasingly creative technical and operational strategies. In just this one operation, commercial relationships, endpoint operations, cryptanalytic exploitation using special purpose hardware, and midpoint collection all had to pull together to track a single individual.

(U//FOUO) It took heroic efforts by key individuals to make all of these things happen in this particular operation. That won't scale unless we learn the lessons offered by this and similar cases, and build the infrastructure and tools needed to make this work much, much easier. Here is a barebones outline of a few of the activities underway to support this:

(U//FOUO) A metadata strategy has been developed to unify the many strands of related activity already underway in the SIGINT system. We are very pleased to have ███████████ serving as the lead for this; she is already actively involved with many of you.

(TS//SI) Getting our diverse accesses tied together is a really tough challenge. Some seemingly small things can make a huge difference. For example, TRAFFICTHIEF is the cross-access tipping service at the core of this operation. Starting as a small project led by two entrepreneurial individuals, ███████████████████████████ it has grown into an essential service in constant use for counter-terrorism operations.

(S) The Network Analysis Center (NAC), one of three key SIGINT Development centers, provides cutting edge analysis of challenging target networks, providing the information needed to create effective access and exploitation strategies.

(S) The new Global Network Development Activity (GNDA) will create an environment for exploiting Special Source programs and a test-bed for learning how to use all of our accesses to identify, locate and collect a dynamic, mobile target set. GNDA is developing entity extraction techniques through metadata.

(S) On an even larger scale, we've established the Global Network Forum, a 5 Eyes construct to manage midpoint accesses on a community basis. Its first order of business is to bring coherence to our planning for and development of accesses to international communications, whether carried over the RF or not.

(U//FOUO) We are also working closely with ITIS and the Senior Acquisition Executive/Program Executive Office (SAE/PEO) to get the right IT services deployed around the world to support the cross-access communications needed to make all this work on the scale and at the speed required.

(U//FOUO) Ever since 9/11, Data Acquisition has hosted a forum (the Terrorist Pursuit Team) for exploration of new counter-terrorism requirements: we have the players explain the problems, send smart people away to create solutions, and then decide how/when/where to find the resources. It's a successful model, which we will shortly expand into a Requirements Process that will cover all challenges that aren't more properly dealt with at a higher (SID or corporate NSA) or lower (one of the Data Acquisition groups, or a field site, or ITIS) level.

(U//FOUO) We have also obtained the services of ███████████ from SID Systems Engineering, to advise us on systems engineering issues that come up as we try to add functionality and connectedness to an already complex system. ███ will also make sure that the improvements we make are done so in a way that will fit into NSA's transformational programs.

(U//FOUO) That's more than enough for now. If you are intrigued by any of these, check out the web pages. We'll come back to most of these in future messages.