(U) O Where, O Where Has My Target Gone?

FROM: [redacted]
Technical Director, Metadata Analysis Center (S2S1)
Run Date: 05/09/2005

Pinpointing the whereabouts of people using GSM cellular networks (S)

(C) Help us help you find your target in a GSM network! Do you have a recent PILOTHOUSE mapping survey hanging around your office? Has your telecommunication research yielded GSM network infrastructure information or email exchanges between network engineers? Have you been involved with a special collection effort that has yielded the layout of a cell network? If so, then we need your help!

(C) One of the most frequent requests for assistance that we receive here in the Metadata Analysis Cell (S2S1) concerns locating GSM cellular users as they roam within their home network or a network they are visiting. While we receive millions of metadata records EVERY DAY that tells us that users are in a particular cell or a particular location area or network, pinpointing that information to a physical point on a map is the challenge. I'd like to tell you what we've been trying to do to help analysts answer these location questions and what you can do to help.

(S) First, just a couple of definitions to make sure all are familiar with the terms that pervade this article!

- **IMSI** -- International Mobile Subscriber ID; and identifier used by the networks use to keep track of subscribers in their network.
- **Cellid** -- a 5-digit identifier used by the network to differentiate between cells in the network; a cell can be a small as a city block or in rural areas, for example, can cover up to a 35-km radius.
- **LAC** -- Location Area Code; a geographic area that covers a number of cells; like the cellid, it too has a 5-digit identifier to differentiate it within the network; it could be as small as a neighborhood or as large as a town or province.
- **VLR** -- Visitor Location Register; a database with a corresponding designator (known as a Global Title - GT) that identifies a large coverage area of a network; a network could use several VLRs to cover a major metropolitan area, or a single VLR to cover an entire country.
- **ASSOCIATION II** -- the tool/db through which you can access correlation and event data associated with Personal Communications Systems, to include GSM.

(U) Okay, that should do it for the acronyms/terms. There are plenty more where those came from but I'll try to stick to those for the purposes of this article!

(S) As I said above, we receive millions of location-related metadata records every day. All of these records are accessible in the ASSOCIATION database/tool ("go ASSOCIATION"). Depending upon where the intercept occurred, the information will reveal locations of subscribers, as denoted by their IMSIs usually, at the VLR, LAC and/or Cellid level. What can we do with this information? It depends. If all we want to know is what country or city a subscriber is in, we can do that without too much of a problem. For example, we know where many VLRs are located because of the information we pick up in SIGINT and collateral. We've centralized that information in the "VLR Look-up" which you can find by going to the Global Numbering Database ("go gndb") or by going directly to the VLR website . There, if you know a VLR, you can check to see what city that VLR covers or you can search by network and find all VLRs assigned to a particular network. I'm not saying we have the whole world covered but we do have a huge number of VLRs recorded in this search tool!

(S) What if you just have tracking information that centers on the LAC or cellid? Enter OCTSKYWARD ("go octskyward" or [redacted]).

(S) Currently OCTSKYWARD holds all logical information on geo-reference data. That means that you can tell if a certain cellid belongs to a certain LAC or whether a set of LACs are subordinate to a particular VLR. It even holds channel information. So again, if you just want to have an idea of the city in which a subscriber is operating, you can start with pulling the subscriber-related location information out of the ASSOCIATION tool, check the geo-related info in OCTSKYWARD, look up the related VLR and at least you know the city where the subscriber is operating. But that's really not enough in many cases, is it? Most people want to know what area of a city someone is in, and in the case of the work that GEO does, they want to be able to be even more specific. For quite some time we here in the Target Analysis Center, which includes the MAC and our sister division, the Target Development Services organization, have been working on refining and further developing these tools and their interactions so that you will actually be able to look on a map and see what area is covered by what cellid, LAC and/or VLR. Let me explain our plans and our progress.

(S) The MAC vision for OCTSKYWARD (which we have coordinated with GEO) is to provide a single repository for all SIGINT and collateral information relating to location data on GSM networks. Data points include cells (with ids, frequencies, channels and lat/long points), towers (BTS's with ids, freqs, height, azimuth, tilt and lat/long), VLRs, and any other points in the network. Once we get enough points, we'll be able to build polygons based on the combination of those points that belong to a particular cell to give an idea of cell coverage. This repository will also provide the capability to automatically connect to other tools and databases like ASSOCIATION, BELLVIEW (used for in-depth geospatial metadata analysis); THORNYHOSTILE (the corporate digital map and foundation geodata repository) and the GCHQ geo-reference database, so that an analyst will not only be able to layout the network on a map but will also be able to track targets of interest on a map with all the available information.

(S) Data sources for this type of information include: SS7 and billing data, SMS and GPRS messages, Overhead information (from DEEPSKY and GAMIRA processing), CIA documents, Network Engineering documents picked up in SIGINT, TAREX reporting, PILOTHOUSE and other mapping tools used by multiple collectors in the field, special (*supersecret!*) collection sources, and "Computable" information (that is, derived from analysis). And, if you're still with me after this lengthy explanation, here's where you can help! **WE NEED THE PHYSICAL GEOLOCATION INFORMATION ON GSM NETWORKS!** We'll take anything you have and we'll even make it easy for you to submit the information! If you go to OCTSKYWARD's home page, you'll see a line that says "Submit data to OCTSKYWARD." Click on the word "submit" and you will be taken to a page that allows you to download a file from your computer. Please make sure you include appropriate details on the source and classification of the information you're giving us.

(C) I think I've covered everything! If you have questions or suggestions, feel free to contact the following MAC analysts:

- [redacted] [redacted] nsa),
- [redacted] ([redacted]@nsa),
- [redacted] ([redacted]@nsa) or
- me, [redacted] [redacted]@nsa)!

"(U//FOUO) SIDtoday articles may not be republished or reposted outside NSANet without the consent of S0121 (DL sid_comms)."