(U) Countering Improvised Explosive Devices in Iraq

FROM: (C) [redacted] SSG Representative at CSG Baghdad, and
[redacted] SSG Operations Orchestration
Run Date: 01/31/2005

New exploitation of High-Powered Cordless Phone Base Stations raises hopes that attackers can be neutralized (S//SI)

(S//REL TO MCFI) The most potent weapon used by the insurgents in Iraq is the improvised explosive device (IED). Because IEDs are often triggered from a distance with no discernable enemy visible, these attacks are extremely frustrating to Coalition troops. In 2004, 822 American servicemen were either killed or wounded by IEDs.

(S//SI) Building on analysis done by Meade Operations Center's HPCP Analysis Cell (also known as the HAC) and teaming with INSCOM's SIGINT Technical Development Activity (STDA), TAREX* operators in theater developed a technique to quickly recover the security codes of High-Powered Cordless Phones (HPCP) handsets. This procedure has reduced the time needed to decode the HPCP security codes from weeks to a matter of hours, and in doing so, has opened a new avenue to pursue IED triggermen and take the fight to them.

(S//REL TO MCFI) Many IED triggers within Iraq are HPCP handsets controlled from a common base station. Recent HPCP models allow for the programming of as many as fifty handsets per base station, allowing insurgents to use one base station as a trigger for numerous IEDs-a real challenge to the SIGINT System.

(S//SI) Locating the IED triggermen is the first hard challenge with this technology. Finding the base station's location is critical to determining the location of the triggermen, and identifying the point of initiation. For SIGINT, this means trying to identify the security code or the "Base Station Identification" (BSID) and locating that equipment for targeting. Handsets used as triggers for the IEDs are often recovered; however, until recently, it was not possible to quickly identify the BSID from these captured handsets.

(S//SI) The TAREX-Baghdad team realized the value of acquiring the BSID quickly to support Geospatial analysis as well as assist with collection/tasking processes. They took on the challenge of trying to use existing collection and processing equipment (PROPHET, SALVAGE, and ALASKA) to extract the security codes, but without success. At this point, TAREX decided to employ their laptop computers to record the digital wave files directly, using the "Sound Recorder" program. Hooking the XPLORER test receiver directly into the laptop's microphone jack, then tuning to the handset's 228.74 megahertz broadcast frequency, the TAREX staff was able to broadcast and record a series of on-off sequences. Since audible beeps were heard only when keying the handset transmitter on and off, these segments were most likely the security code. TAREX then sent this recorded file to INSCOM STDA and the HAC. Several days later, the HAC (Mr. [redacted]) informed TAREX that the files were of sufficient quality to allow a breakout of the security codes they contained.

(TS//SI) As a result of TAREX's ability to send the recorded wave files, the HAC developed and standardized a MARTES Software method for processing these new input files. These MARTES methods can easily determine the keying rate, coding scheme, center frequency, signal fielding, service signal identification, mode/function and-when possible-the BSID of the captured phone (either handset or base station).

(TS//SI) To take this success one step further, when an intercepted signal is known and the security code (BSID) is recovered, the HAC forwards an immediate turn-around report to the TAREX report originator, as well as collection and analysis resources (Overhead, Airborne, and Ground-based assets) for special emphasis targeting. If the service signal is unknown, as was

the case recently, a new signal report (HILITE) is issued, the structure is outlined on the HAC web site, and developers can create a processing algorithm for the OOK HPCP service signal.

(TS//SI) With the ability to quickly identify the BSIDs directly from the handsets, the base stations -- and hence the IED triggermen -- can be targeted. As a result of the vital work conducted by operators of the TAREX-Baghdad team, INSCOM STDA, and the HAC, a principal component in many IEDs can now be targeted and hopefully, the IED makers neutralized. The effects of this work will be counted in the lives saved.

(C) The following contributed to this article:

- [redacted] IMPACT Science and Technology
- SSG [redacted] USA, TAREX Representive to MNF/C-I Baghdad
- [redacted] Functional Engineer/Analyst, IFC/IDC Baghdad

---

*Note:
(C) TAREX, or Target Exploitation, is a unique collection program chartered under USSID 173 to collect information and documentation of interest to the U.S. Cryptologic System.
