(S//SI) NSA-Georgia Project Serves as Model for Digital Network Intelligence Operations

FROM: Chris Stegmaier
Chief, Iran Digital Network Cell (GS2E4)
Run Date: 09/12/2006

(TS//SI) Project shows that three different skill sets must be brought together when working DNI targets...

(TS//SI) NSA/CSS Georgia's Iran Digital Network Cell recently completed a successful, nine-month project tracking the network upgrade at a high-interest facility in Tehran, the [redacted]. Upon completion of the project, an after-action review determined that the [redacted] project **succeeded because of the presence of linguistic ability, target knowledge, and computer skills.** The combination of these three factors in a small cohort of analysts working Digital Network Intelligence (DNI) makes the difference between success, marginality, or failure.

(U//FOUO) Each of the three factors poses specific problems when absent, but these problems can be mitigated by choosing a variety of workaround solutions. Managers and supervisors should strive to assemble DNI teams that have all three factors or partner with organizations that can provide support when one of the three factors is not available. This article outlines the challenges presented when one of the three factors is missing and presents ways to overcome these challenges.

(U) Case 1: Language Ability and Target Knowledge

(S) The limiting factor in this case is the ***absence of computer skills.*** While the analysts know the target and can process native language traffic, the potential exists for them to miss key intelligence about the target's computer systems and their capabilities. This could be as simple as the difference between Windows and UNIX systems or as complex as recognizing filenames and directories that contain information about firewalls and system vulnerabilities.

(S) To compensate for the absence of computer skills in this case, a number of online National Cryptologic School courses are available through Vuport (" go vuport ") and platform training in the form of networking classes like NETA-3001 (go neta3001). This training offers introductory to in-depth instruction on the technology and terminology that our targets use every day. The analysts working the target do not have to be computer experts, but they do need a basic knowledge of what possibilities exist with advanced technology.

(S) A good source of information is Squirrel Accumulator* (" go nuts "), a collection of digital network analysis tools put together by the Protocol Exploitation Branch (S31212). It serves as an excellent repository for DNI analysis, especially when the target analyst is not familiar with computer and networking technology.

(U) Case 2: Language Ability and Computer Skills

(S) The limiting factor in this case is the ***absence of target knowledge.*** Operational and developmental DNI efforts in which computer-savvy analysts and linguists are assigned can potentially fail and leave managers wondering what went wrong. In many situations, failure results when the analysts do not know the nuances of their target. Leaving those key pieces of information out of the intelligence processing equation makes it very difficult to succeed.

(U//FOUO) A quick means to solve the target knowledge problem is regular visits or meetings with the target subject matter experts. Even in organizations where the analysts work in close proximity, regular meetings about developmental or operational goals can spark intuitive thought in the DNI analysts and also provide ready resources for questions about unexpected issues in traffic.

(U) Case 3: Target Knowledge and Computer Skills

(S) The last, and possibly the worst, case scenario is when analysts with target knowledge and computer skills are assigned to work an operational or developmental target ***without linguistic ability.*** Knowing the target and understanding how computer applications and systems work will help the analysts to be somewhat effective, but the killing factor is that they are unable to read the target traffic. Targets whose primary traffic is international will be easier to work because the language of choice is generally broken English. Even so, targets internal to one country or language set will be very tough, if not impossible, to penetrate.

(S) Various options are available to analysts in a situation where linguist resources are very few and far between. One is CYBERTRANS , but it is limited in its ability to fully translate documents. At best, it can give the target analyst an idea about a piece of traffic to then send off for a full translation. A better option is to partner with some linguistic resource, either embedding borrowed linguists or working virtually with a team of linguists off-site. Knowing the target will allow the analyst to guide the linguists and provide them the key terms and concepts they will need to prosecute the traffic forwarded to them.

(U) Looking Ahead

(U//FOUO) There is probably little argument that the majority of target sets worked within the Extended Enterprise will be headlong in information technology (IT) solutions in the very near future, if they are not already relying heavily on advanced IT infrastructures. Having recognized that our targets are going in that direction, we need a solution that mirrors and counters that trend, whether it has to do with digital representation and translation of native texts, new target aspects dealing with technology and computers, or historical facts and figures about target sets that lend themselves to current development and processing endeavors.

(U//FOUO) That solution, whether in the developmental or operational spaces, is to combine analysts whose backgrounds and abilities represent each of the three factors needed to be successful: linguistic ability, target knowledge, and computer skills.

---

*(U) Note: See an earlier article about Squirrel Accumulator.

(U//FOUO) Do you have a comment on this topic? Post your thoughts on the SID *today* blog .

(U) See also other recent articles from the Cryptologic Centers:

- (S//SI) NSA/CSS Texas Supplies Key Reporting About Cuba for Congressional Mandated Memo
- (S//SI) Watching for -- and Predicting -- the North Korean Missile Test Flight (Hawaii)
- (S//REL) TechSIGINT Watch Desks Renamed (Colorado)
