(S//SI) SIGINT Forensics: A Look Inside Terrorists' Computers

FROM: Dr. Adele Merritt
SIGINT Forensics Lab
Run Date: 09/22/2003

(U//FOUO) Recently, the Royal Canadian Mounted Police arrested 19 suspected Al Qaeda members. The New York Times reported that the authorities "need to sift through 30 computer hard drives" and it "could take weeks if not months" to finish gathering evidence. Ever since the War on Terrorism started, government agencies throughout the world have been gathering computer media while pursuing and capturing suspected terrorist and Al Qaeda members. Ever wonder who looks at this data?

(S//SI) The SIGINT Forensics Lab was established in September 2001. The Lab's mission is to analyze seized computer media in support of SIGINT operations. This makes the Lab unique from other computer forensics efforts that exist throughout the U.S. Government. Utilizing commercial, open source, and in-house developed tools, the Lab harvests communications information such as phone numbers and e-mail addresses in an effort to provide actionable SIGINT leads to NSA offices. Because the lead information is pulled from computer data, the Lab is also usually able to pass along useful context information to assist customers in assessing the significance of the lead. Residing in Cryptanalysis and Exploitation Services (CES), the Lab is also well-positioned to identify and facilitate the exploitation of encryption and steganography found in target computer data.

(S//SI) One other unique service provided by the SIGINT Forensics Lab is the identification of direct and indirect communication links from looking across data from numerous target computers collected via SIGINT, HUMINT, and law enforcement efforts. This problem is more challenging than other metadata chaining efforts due to the variability of the communications data format and locations within computer media. However, the Lab has been able to overcome this problem and find countless communication connections between target computers. These discoveries have led to the identification of new targets for the SIGINT system to pursue, as well as providing a better understanding of how targets communicate via computers.

(S) In addition to providing SIGINT support, the lab also provides technical assistance to external organizations through facilitating responses to requests for decryption of computer data, as well as providing computer communication profiles for targets. On occasion, the lab has also been able to provide non-communications forensics work. For instance, in November 2002, pictures of American trains found on a terrorist hard drive prompted intelligence reports and a FBI-issued alert warning that Al Qaeda operatives may be planning an attack against US railroads. Time Magazine reported in their November 4, 2002 issue, "photos of American passenger and cargo trains as well as rail crossings" were found on a terrorist hard drive. The SIGINT Forensics Lab examined the photos and accompanying computer files to determine that the train photos were taken from a 1980's commercially produced clip art CD. NSA was able to provide this information to the various elements of the U.S. Government who had committed resources to following this specific threat.

(U//FOUO) If you are interested in learning more about the SIGINT Forensics Lab, please contact us at [redacted].

DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON: 20320108