(U//FOUO) TEC Successfully Installs BOTANICREALTY at LADYLOVE (USJ-799)

(TS//SI//REL) In response to a request from S2B, MSOC System Development and Signals Development Lab personnel collaborated with the TEC to deploy a solution to collect a ▓▓▓▓ video network. When first detected, the video was unencrypted. The video then became encrypted over a period of two months. The current demodulation solution from the TEC is called BOTANICREALTY. Originally, SALTYDOGS was used to find carrier acquisitions and discover signal characteristics. This provided the frequency range, carrier rates, and a rough time up and time down for channel activity.

(TS//SI//REL) In mid-April, the TEC installed BOTANICREALTY (formerly known as UNCANNY) at LADYLOVE in the hopes of locating, identifying, and collecting ▓▓▓ ▓▓▓▓▓▓▓▓▓▓ clear and encrypted video signals found on the ▓▓▓ of ▓▓▓▓▓▓▓▓▓▓. The collection of these signals, in support of ▓▓▓ ▓▓▓▓▓▓▓ is important to the S2B ▓▓▓▓▓▓▓▓▓▓▓▓▓, various special projects at the CIA, and in general product reporting ▓▓▓▓▓▓▓▓.

(TS//SI//REL) Within minutes of the system coming on line, BOTANICREALTY successfully collected its first signal matching the parameters of the encrypted (HIGH PRIDE) video ▓▓ signals. The hub control channels are session encrypted while the outstations are bulk encrypted video. Since proving the ability to automatically process these signals of interest at LADYLOVE, over 1000 collects, totaling hundreds of hours of raw data, have been made and forwarded to cryptanalytic personnel in CES for further investigation.

(U//FOUO) Joint SIGINT Activity Annual Report for 2007

(S//SI//REL) The Joint SIGINT Activity (JSA) experienced notable successes in its FORNSAT mission during 2007 for NSA and the German Federal Intelligence Service, or Bundesnachrichtendienst (BND). However, concurrent with the JSA mission changes, manpower requirements were re-evaluated and reductions to both civilian and contractor manning levels were approved with implementation to be carried out in FY08.

(S//SI//REL) The past year also saw an expansion of JSA's partnerships with SSO, TOPIs, and ESOC, with plans to expand these further and increase support on various operations in 2008. JSA will continue to build on its successes and improve its mission contribution in collection and SIGINT development to both NSA and BND.

(U//FOUO) Highlights for 2007:

(S//SI//REL) JSA engineers developed various analysis tools and an automated selector sanitizing tool. The selector sanitization tool can be used at other sites, including those working special projects.

(S//SI//REL) The expansion of site capabilities through the installation and integration of U.S. and German systems significantly improved collection and development of high-priority targets. New or improved capabilities include an automated survey system, VoIP processing and metadata collection capabilities, a high speed filtering system, GSM metadata collection capabilities, and new data flows to NSA for DNI, VoIP and GSM metadata.

(S//SI//REL) A closer relationship between ESOC, JSA and BND resulted in new exploitation of targets in Algeria as well as other African targets. New TROPICPUMA fax processing capabilities deployed in December immediately began to provide unique and valuable intelligence to ESOC and BND on ███████████████████

(S//SI//REL) The BND used JSA ███████ GSM collection to identify, track, alert, and ██ ██

(S//SI//REL) JSA continues to provide critical collection of the ████████████ ████████████████████ network, providing unique insights into ██████████████ ████████████████████

(S//SI//REL) NSA personnel continued to improve BND's skills through both classroom and on-the-job training allowing BND personnel to take on greater roles in DNI processing and analysis.

(S//SI//REL) Joint SIGINT Activity-Developed VoIPSum and AutoNorm Tools Used in Local Analysis, Create Agency-wide Interest

██

(S//SI//REL) JSA has developed and is now using two new number normalization tools – a VoIP Summarization (VoIPSum) tool and an Automated Normalization (AutoNorm) tool.

(S//SI//REL) Voice-over-IP (VoIP) traffic is prevalent at many collection sites, including JSA. Site engineers have developed a simple tool, called VoIPSum, to extract, parse, and organize VoIP metadata for analysis by Intelligence Analysts, Signals Analysts, and developers. VoIPSum provides the user with several outputs: a summary file of cities/countries on each case notation seen in its run, also viewable by web browser; a

file containing URIs (Uniform Resource Indicators) and their associated IP addresses; a file of normalized numbers and location information; and a file of normalization suggestions for non-normalized numbers, generated with help from AutoNorm.

(S//SI//REL) Generating normalization rules for NORMALRUN can be very difficult without adequate knowledge of a region's Country Code (CC), National Destination Code (NDC), Local Exchange Office Code (LEOC), and Subscriber Number (SN). JSA has found their in-house developed tool, AutoNorm, a great time saver for generating NORMALRUN rules. AutoNorm works by matching substring combinations of the raw number against the Global Numbering Database flat file. It provides several input options: generic, which tries to find an exact match; prelist, which appends a given set of digits to domestic calls before attempting matches; and sort, which sorts its output into groups that share the same digits stripped or pre-pended.

(S//SI//REL) These two tools have been used by JSA analysts to aid in generating reports and number normalizations and target research. Additionally, representatives from the NAC, Misawa, SSG, S2C, and SSO have expressed interest in receiving and using VoIPSum and AutoNorm.

(S//SI//REL) VoIPSum and AutoNorm are now available for download! For more information, including user manuals, output examples, and a downloadable tarball, please visit JSA's website. You may also contact the POCs listed above.

(S//SI//REL) Joint SIGINT Activity Begins New SMS and Call Event Dataflows for NSA Analysts

(S//SI//REL) JSA initiated two new SMS dataflows for NSA analysts in April. These new dataflows are from USD-1079's AST128B and AST128C DNR collection platforms. The SMS data is flowing into DISHFIRE, and the corresponding call event data into FASCIA. A cursory look at dialing showed ███████████████████ Poland and others. Preliminary data shows that JSA is sending over 330,000 SMS events to DISHFIRE daily. So, let the hunt begin! One can isolate this new SMS data by querying in DISHFIRE on JSA's PDDG (IQ) and collection box (RA, L1). This SMS collection is being processed on multiple case notations from INTELSAT-902 (G2), YAMAL-202 (E9), and EUTELSAT-W6 (KL) with forward and reverse gateways with ██████ (primarily). However, we also have Tajikistan, Russia, Monaco, Lebanon and UAE gateways represented. As a reminder, JSA has been forwarding SMS data from its JUGGERNAUT GSM collection platform since 2007.

Der Zeitgeist
(C) Joint SIGINT Activity (JSA)