(U//FOUO) NBOVBM DSZQUBOBMZTJT GPSVN -- 8-12 NBZ 2006

FROM: [redacted]
Target Pursuit/Balkans, Russia and FSU (S31134)
Run Date: 06/09/2006

(S//SI) 5-EYES cryptanalysts compare notes at GCHQ conference.

(S//SI) Fish and chips, double-decker buses, narrow streets, 5:20 a.m. sunrises, and 9 p.m. sunsets were among the delights for 14 Office of Target Pursuit (S311) and Extended Enterprise analysts when they attended a GCHQ*-sponsored Manual Cryptanalysis Forum at Cheltenham, UK, during the week of May 8.

(S//SI) The Forum was a gathering of five-eyes community cryptanalysts and cryptolinguists for discussion of technical issues concerning the decryption of manual cryptosystems -- ciphers where it is possible to encrypt and decrypt without the aid of a machine or computer. ("NBOVBM DSZQUBOBMZTJT GPSVN -- 8-12 NBZ 2006": If you want to see the solution to title, please read to the end of the article.)

(U//FOUO) GCHQ

(U//FOUO) Departing from Hawaii, Georgia, Maryland, and Virginia, most of the NSA delegates arrived after an 8-hour airline flight and 2-hour bus trip on Sunday, 7 May. Fighting jet lag, they ventured forth into the heart of Cheltenham, walking to shopping areas and city parks still abloom with lilacs and tulips. Most of the group reconvened at the hotel and then went in search for dinner. We finally settled on a restaurant called Renovations, which was aptly named, as the menu was being changed that week and many of the choices were not available--they had sold the last shepherd's pie at lunch! Despite the non-smoking sign, the back room had a distinctly smoky atmosphere, but the food was good and the company most excellent, as we chatted about our backgrounds and families.

(S//SI) Monday morning's welcoming remarks by [redacted] Head of OPH Crypt Customer Delivery Service (OPH-CD), heralded the start of the week-long conference, which touched upon both the current and future status of manual cryptanalysis. Members of each five-eyes community then discussed manual cryptanalysis at their respective agencies.

(S//SI) Several challenges were echoed by the agencies: the need for language skills in a cryptanalysis office, difficulties with training, fluctuating volumes of collection, poor quality of intercept, diminishing numbers of experienced analysts, and difficulties in building the next generation of manual cryptanalysts. Throughout the rest of the conference, delegates presented detailed technical briefings on manual systems -- some simple and others extremely complex -- and software tools used to analyze and recover these systems, revealing the variety of cryptosystems still seen and skills and tools needed to solve them.

(S//SI) As a departure from briefings, Wednesday afternoon was a chance for participants to break into smaller groups. Several operational problems were presented for diagnosis or chart recovery, while other groups saw demonstrations of software tools used by GCHQ cryppies. This open time also gave some people a chance to work one-on-one with GCHQ analysts, providing a chance for sharing of analytical expertise.

(S) Finally, Friday's closing session centered on discussing challenges that all five agencies face. **Key points raised were:**

- the need for training at both a beginning and advanced level for cryptanalytic as well as cryptolinguistic skills;

- the need for making the most of our limited resources (cryptanalysts, linguists, and programmers) thus emphasizing the need to smartly share tools, resources, and problems; and
- the need to record the intellectual capital of those nearing retirement and develop skills and knowledge in the next generation of cryptanalysts and cryptolinguists.

Thirteen action items, most aiming to increase sharing of resources among the Second Party partners, were agreed upon and deadlines were set.

(U//FOUO) After work on Tuesday evening, NSA, CSE, DSD, and GCSB* analysts competed with their GCHQ counterparts in a British game of skittles -- where each player was given three balls (one had a decidedly flat side) to knock down 9 pins arranged in a diamond shape without touching the sides of the alley. Laughter and good-natured gibes accompanied many throws. Some new skittle players were amazed at how easy it was to miss all nine pins! Finally, on Thursday evening, the last night before our departure, GCHQ hosted dinner at a nearby pub. The analysts from all agencies enjoyed the excellent food and atmosphere in a private upper room with bared ceiling beams, wooden tables, and various sports' hats on the rafters.

(U//FOUO) All in all, the conference was a great success with SID analysts working hand in hand with their Second Party counterparts. The technical briefings and discussions highlighted strengths and raised concerns, while the after-hours activities gave everyone a chance to relax and interact. All agreed that future forums should be held to further develop sharing amongst the manual crypt community. (U//FOUO) NBOVBM DSZQUBOBMZTJT GPSVN -- 8-12 NBZ 2006 -- And the title's solution? Why, "MANUAL CRYPTANALYSIS FORUM -- 8-12 MAY 2006."

(U//FOUO) NSA attendees:

S3113 (Eurasia Pursuit)	S3114 (Terrorism, MENA and Regional Pursuit)
[redacted] NSA/CSS Hawaii (HS312)	[redacted], S31143
[redacted] S31134	[redacted], S31141
[redacted], S31133	[redacted] S31142
CTI1 [redacted], S31131	[redacted], S31141
[redacted] S31134	[redacted], S31142
[redacted] S31133	[redacted] S31141 (CADP intern)
[redacted] NSA/CSS Georgia S31133	

NCS: [redacted], E91

*(U) Notes:
GCHQ = the UK's Government Communications HQ
CSE = Canada's Communications Security Establishment
DSD = Australia's Defence Signals Directorate
GCSB = New Zealand's Government Communications Security Bureau

DYNAMIC PAGE -- HIGHEST POSSIBLE CLASSIFICATION IS
TOP SECRET // SI / TK // REL TO USA AUS CAN GBR NZL
DERIVED FROM: NSA/CSSM 1-52, DATED 08 JAN 2007 DECLASSIFY ON: 20320108