

SIGINT Talk Notes for LA2600; 1.3.2003

By xinc@strangerthanfriction.org

Pre-Notes Notes:

This collection of notes was used mainly to keep me on-track and to help me remember all those pesky dates and numbers that pop up whenever you talk about anything historical. As such, they're not all that informative by themselves – beyond giving a brief list of cool things to look up in the reader's spare time. Also, much of the talk itself was done from memory.

Feel free to contact me with any questions you might have and I'll do my best to answer them. That said, there's nothing more satisfying than doing something your-goddamn-self, and so I highly recommend anyone interested in the subject read the following:

- The Puzzle Palace, by James Bamford – Great exposé of the NSA. Slightly out of date, but very informative.
- Body of Secrets, by James Bamford – A follow-up to Puzzle Palace.
- Interception Capabilities 2000 document (<http://www.iwar.org.uk/sigint/resources/ic2000/ic2kreport.htm>), also mirrored along with this file.

We now return you to your normal program...

What is Signal Intelligence?

- The interception and exploitation of emissions within the electromagnetic spectrum.
- Includes COMINT, which is concerned exclusively with the actual communications carried by a particular signal.

Signal Mediums and Interception

- Submarine Cable (TransAT / TAT)
 - Capability
 - Submarine telephone cables provided the first major reliable high capacity international communications systems.
 - TATs 1-4 were limited to a few hundred simultaneous telephone channels.
 - TAT 5 & 6 had just under 5,000 channels, combined.
 - The most modern optical fiber systems carry up to 5 Gigabits per second (roughly 60,000 simultaneous telephone channels).
 - Tapping
 - Induction tapping trials against a Russian military submarine cable were run in 1971.
 - Induction tapping via submarine recording pod was in use from 1972 on. Capacity has increased over time and primarily submarine drones now handle data collection.
 - NSA and other Comint agencies have spent a great deal of money on research into tapping optical fibers, reportedly with little success.
 - The key means of access is by tampering with optoelectronic "repeaters" which boost signal levels over long distances.
 - Alternatively, but less comprehensively, one can tap the microwave communications en route to or from a TransAt terminal and receive a large percentage of the communications that were/will be on the wire.
 - Thoughts
 - If TransAt fibre cables have been tapped the capacity of the monitoring agency would have to be phenomenal.
 - Transporting that quantity of data back to a processing facility from a repeater (underwater) tap is nearly impossible, so initial processing would have to be done at the source to cull out irrelevant traffic.
- Microwave
 - Capacity

- Microwave radio was introduced in the 1950s to provide high capacity inter-city communications for telephone and, later, television.
 - Microwave radio relay stations utilize low power transmitters and parabolic dish antennae which are established in high places for maximum line-of-sight.
 - Because of the curvature of the earth, relay stations are generally required every 30-50km.
 - Microwave links carry the majority of Long Distance and cellular telephone traffic.
 - Tapping
 - Long distance microwave links often require relay stations to receive and re-transmit communications down the line. Each receiving station picks up only a small fraction of the original signal; the rest of which passes over the horizon and on into space, where satellites can collect it.
 - During the 1960s satellites began tapping Microwave links from space.
 - The best position for such satellites is not above the target, but up to 80 degrees of longitude away, i.e. just over the horizon.
- High Frequency
 - Capacity
 - Used primarily prior to 1960 for international communications.
 - High Frequency (HF) radio systems were used mainly for diplomatic and military purposes.
 - An important characteristic of HF radio signals is that they are reflected from the ionosphere and from the earth's surface, making their functional range thousands of miles.
 - Tapping
 - Because of this, they are relatively easy to intercept, requiring only a suitable area of land in, ideally, a "quiet" radio environment.
 - From 1945 until the early 1980s, both NSA and GCHQ operated HF radio interception systems tasked to collect European communications in Scotland.
 - The most advanced type of HF monitoring system deployed during this period was a circular antenna array known as AN/FLR-9. These arrays are more than 400 meters in diameter. They can simultaneously intercept and determine the bearing of signals from as many directions and on as many frequencies as may be desired.
 - Also:
 - HuffDuff tracking of submarines in WWII.

- SATCOM
 - Capacity
 - The majority of communications satellites (COMSATs) is operated by Intelsat (International Telecommunications Satellite organization).
 - The latest generation Intelsat communications satellite can handle the equivalent to 90,000 simultaneous calls.
 - Tapping
 - Easily tapped by placing a dish near the Earth terminal of the link.
 - Tangentially
 - Sugar Grove, West Virginia
 - Originally set up in the 50's to detect Soviet signals reflected off the moon's surface, which ultimately failed.
 - Exists in a nature preserve that has a 100 square-mile radio "quiet zone" around it. No radio or air traffic is allowed.
 - 60 miles from COMSAT's Earth Terminal
 - Is part of the Echelon system and most likely collects a large chunk of Commercial traffic entering and leaving the US.
 - Appears to target only domestic areas.
- Spy Satellites
 - DSP Code 949 and Code 647
 - Launched into a geo-stationary orbit, 22,300 miles above the equator.
 - Drifted 10° above and below the equator to pick up all off Soviet Russia and much of China.
 - Early warning for ICBM launches and nuclear detonation.
 - Later launches carried substantial SIGINT equipment for receiving radio and microwave transmissions.
 - Rhyolite/Aquacade
 - Purely SIGINT Successor to the DSP line.
 - Using a large parabolic antenna that unfolded in space, Rhyolite intercepted signals in the HF, VHF and UHF bands, as well as microwave transmissions.
 - Used as a primary form of verification of SALT (Strategic Arms Limitation) compliance - (until 1977 the Soviets didn't encode telemetry communications from their missiles, believing that satellites couldn't pick up the signal at large distances).

- Operated from a remote ground station in Pine Gap, Australia where captured data is burst-radioed back to earth.
 - Magnum/Orion
 - Newer versions of Rhyolite.
 - Their targets include telemetry, VHF, cellular phones, paging signals, and mobile data links like satellite phones.
 - Jumpseat/Trumpet
 - Operate in highly elliptical near-polar orbits, which lets them to "hover" for long periods over high northern latitudes.
 - They collect signals from transmitters in high northern latitudes, and also to intercept signals sent to Russian communications satellites in the same orbits.
 - General Info
 - Details of US space-based Sigint satellites launched after 1990 are rare, but collection infrastructure has continued to grow.
 - The main stations are at Buckley Field, Denver, Colorado; Pine Gap, Australia; Menwith Hill, England; and Bad Aibling, Germany.
 - The United States can direct space collection systems to intercept mobile communications signals and microwave city-to-city traffic anywhere on the planet.
 - Because of the geographical and processing difficulties of collecting messages simultaneously from all over the world it's likely that this capacity is directed at military targets and areas of national interest.
 - Based on a simple count of the number of antennae currently installed at each COMSAT interception or satellite SIGINT station, it appears that the UKUSA nations are currently operating at least 120 satellite based collection systems.
- Non-Communication Intell
 - Ferrets
 - Ferreting is a Cold War practice that is still used whenever a border area is likely to become a battleground.
 - In the Cold War, EC-130's loaded with directional-finding SIGINT gear, would fly up against – and often well across – enemy borders in hopes of triggering border defense radar systems.
 - By 'waking up' these radar stations and getting a solid fix on their locations, bombing plans could be made well in advance to immediately establish air superiority.

- In the 1950's there were numerous altercations between Soviet MIG's and the lumbering EC-130's, some of which resulted in bloodshed.
 - Traffic Analysis
 - TA deals primarily with the frequency, security level and likely recipients of signals.
 - TA is completely unconcerned with the contents of a signal, but rather how well it's encrypted, what geographic area it covers and where the signal originated.

Key SIGINT Organizations

- NSA
 - Created in 1952 to oversee all SIGINT operations in the US.
 - Slowly wrested control away from the Army and Navy.
 - The NSA, like the NRO, was originally a Black agency; meaning its creation and continued existence was a closely kept secret.
 - Still considers its operational mandate, written by Harry Truman, to be a national secret. This mandate, which describes the Agency's objectives and outlines its mission, is highly classified.
 - Domestic monitoring.
 - Trivia: The NSA bought the first Cray-1 for its operations in Fort Meade.
- GCHQ (Government Communications HQ)
 - Great Britain's counterpart to the NSA.
 - Under the UKUSA agreement, SIGINT and COMINT workload is often shared between the two agencies to avoid duplication of effort.
- ILETS (Intl Law Enforcement Telecommunications Seminar)
 - NSA-sponsored European "seminar" of communications and intelligence agencies on policymaking.
 - Claims to be for law enforcement, but is clearly aimed at keeping technical infrastructure easily monitored by intell agencies.
 - Largely dominated by NSA and FBI interests.
- UKUSA / Echelon
 - A 1947 treaty, known as the UKUSA agreement, brought together the SIGINT organizations of the United States, Britain, Canada, Australia, and New Zealand.
 - Defined spheres of influence, each country is assigned specific targets according to its potential for maximum intercept coverage.
 - The UKUSA nations also standardized their terminology, code words, intercept-handling procedures, and indoctrination oaths, for efficiency as well as security.
 - The computer stations around the globe are known as Echelon Dictionaries. These computers have the ability to automatically search through intercepted communications for keywords, and have existed since the early 1970s.

- The Echelon system was designed by NSA to interconnect all these computers and allow the stations to function as components of an integrated whole.
- NRO (National Reconnaissance Office)
 - The National Reconnaissance Office (NRO) is the single, national program to meet US government needs through space-borne reconnaissance.
 - Existence was classified until 1992.
 - The mission of the NRO is to ensure that the US has the technology and space-borne assets needed to acquire intelligence worldwide.
 - The NRO's assets collect intelligence to support such functions as indications and warning, monitoring of arms control agreements, military operations and exercises, and monitoring of natural disasters and other environmental issues.

SIGINT History

- Zimmerman Telegram
- The Black Chamber / MI-8
 - MI-8 worked on military and tactical intell in the 1920's.
 - The Black Chamber was created for peacetime diplomatic intell for political use. Shut down by the Hoover administration.
 - The Black Chamber broke the Japanese "Angooki Taipu A" (a.k.a. "Red") cipher, and compromised domestic telegrams over Western Union.
- Bletchley Park
 - Broke Enigma and Lorenz (Hitler's High Command cipher)
 - Developed the world's first programmable computer, Colossus.
- Navy Combat Intelligence Unit
 - Broke Japanese Fleet code JN25 allowing the Allies to track ship movements. Ultimately resulting in the taking of Midway.
- Major SIGINT Failures
 - NSA Defections
 - Bernon Mitchell and William Martin, 1960
 - Jack Dunlap (Army, NSA Courier)
 - Pearl Harbor
 - In the early hours of Dec 7, 1941 a the first thirteen parts of a fourteen-part encrypted message from Tokyo to Washington was intercepted. In Japanese, it instructed the Japanese Ambassador to issue a diplomatic reply to the last round of negotiations with the US.
 - Around 5:00 the final part of the message, as well as a second, shorter, message was intercepted.
 - The final part of the larger message indicated that Japan was breaking off negotiations with the US.

- The shorter message was in Japanese and required translation.
- The message was not translated until mid-morning, and contained instructions to the Japanese Ambassador to deliver his reply and break off negotiations at precisely 1:00 that afternoon.
- Within the next few hours, Japanese diplomatic intercepts showed that Tokyo had ordered the Japanese Embassy to destroy all codebooks and cipher equipment.
- By 11:00 AM the messages had been disseminated to the Washington Brass, who believed that Scrambler traffic may have been compromised and chose to send the warning to Hawaii through the War Department's Message Center.
- The message arrived at 7:33 AM, Hawaii Time, where a communications officer addressed it to Gen. Short, stuck it in an envelope and put it in the outbox for courier deliveries.
- 22 minutes later the attack on Pearl Harbor had begun.
- The message was delivered and read at 2:40 PM, over 15 hours after the attack was known about.