From AFIO's The Intelligencer
Journal of U.S. Intelligence Studies
Volume 18 • Number 3 • $15 single copy price Summer/Fall 2011
© 2011 AFIO - Association of Former Intelligence Officers, All Rights Reserved.

The Intelligencer
Journal of U.S. Intelligence Studies
Top Secret America: Working Together Getting Results

Association of Former Intelligence Officers
6723 Whittier Avenue, Suite 200
McLean, Virginia 22101
Web: www.afio.com, E-mail: afio@afio.com

A Guide to Teaching Signals Intelligence

by Lawrence D. Dietz

If you ever made a call on a cell phone, or sent a text message, or posted on a blog, you have no doubt wondered if anyone else was listening in on your communications. You watch crime thrillers only to learn that the federal government finally was able to arrest organized crime gangsters by tapping their phones. What you may not have known is that these are examples of how Signals Intelligence (SIGINT) can be employed.

DEFINITION

According to the National Security Agency (NSA), "SIGINT... encompasses any intelligence... collected over the electromagnetic spectrum. SIGINT derives intelligence from transmissions associated with communications, radars, and weapons systems... It complements other forms of intelligence....[1]

Prior to proposing some approaches for instructors to teach about SIGINT, it is useful to consider and define the components of SIGINT. Most generally accepted definitions say that SIGINT is composed of:

- Communications Intelligence (COMINT), which means deriving intelligence from communications such as radios or telephones.
- Electronic Intelligence (ELINT), which is deriving intelligence from non-communications emitters, such as radar.
- Foreign Instrument Signals (FIS or FISINT) derived from foreign telemetry signals, such as from satellites.
- The newest component is Computer Network Exploitation (CNE), which encompasses exploiting computer networks and the Internet for useful intelligence.

APPROACHES TO TEACHING SIGINT

Three alternative and complementary approaches are feasible for the teaching of SIGINT – the historical, the technical, and via practical exercises.

Historical Approach. Intercepting the secrets of one's enemies has been a proven tactic for thousands of years. SIGINT often depends on breaking an enemy's codes. Consequently, the study of SIGINT is not complete without the study of cryptography. Cryptography is the coding and decoding of secret messages.[2]

There are several famous, and some not so famous, instances of when SIGINT turned the tide of war or public opinion. One is the Zimmermann Telegram of January 1917, ably chronicled in Barbara Tuchman's book (see Readings for Instructors). The Zimmermann Telegram was a major reason President Wilson acquiesced to entering World War I. In an intercepted diplomatic note, the Germans and the Japanese promised Mexico it could regain some of its territory 'stolen' by the United States in the War of 1846-48 if Mexico would join Germany in war against the US.

Another historical incident that is good to study is the January 1968 capture of the US Navy's SIGINT ship *Pueblo* by the North Koreans and the subsequent imprisonment of that crew. Students should explore the relationships between those entrusted with the secret codes and the role of the ship's captain, who was not. The *Pueblo* can also be used to debate how much effort should be given to protecting SIGINT sources, which often are fragile and therefore sensitive.

An interesting topic is the controversy of whether or not FDR had foreknowledge that the Japanese were going to attack Pearl Harbor because the US had broken the Japanese Purple Code used to encrypt its diplomatic traffic. (See Wohlstetter in Readings for Instructors.)

[1] Source: *http://www.nsa.gov/sigint/index.shtml* It is important to point out that SIGINT is just one of several intelligence disciplines. Another is Human Intelligence (HUMINT) familiar to most people thanks to James Bond and others of his ilk. Imagery Intelligence or IMINT, which can be thought of as Google Earth where pictures of areas and buildings taken from satellites, combined with other data, are used to develop a profile of a target. Open source intelligence (OSINT), such as everything available in the public library, is another. Lastly, Measurement and Signatures intelligence (MASINT) is best compared to the forensic tests shown in the CSI television series. In practice, intelligence analysts use all the "Int's" in concert as it is accepted practice not to rely on a single source, but to confirm information through several sources.

[2] Source: *http://www.wordcentral.com/cgi-bin/student?book=Student&va=cryptography*

An unusual scenario that combines history, Native American culture, and SIGINT is the story of the Navajo Code Talkers of World War II. In those days radio transmissions were sent in the clear, meaning they weren't encrypted and therefore heard by anyone on the same frequency. In order to befuddle the Japanese, the US Marine Corps employed Navajo speakers who used their native language with which the Japanese were totally unfamiliar.

Technical Approach. A technical approach is best suited for students who excel in math and logic. Under this approach an instructor shows how basic code systems work. There are extensive resources available. For example the National Security Agency (NSA) has cryptograms on line, which can be found at: *http://www.nsa.gov/kids/games/games00002.shtml*.

Instructors can develop basic handouts using substitution codes where one letter is substituted for another. Other simple techniques are described by the University of Illinois (Chicago) at *http://cryptoclub.math.uic.edu/indexmain.html*. These include the Caesar (shift) Cipher, Affine Cipher, Vigenere Cipher, Multiplicative Cipher, using numbers for letters, and the Substitution Cipher. This resource also introduces the concept of frequency analysis as a tool used to break substitution codes. Frequency analysis is based on the fact that some letters, like vowels — especially "e," are used frequently while other letters are used less frequently. Consider breaking your class into two groups. One would be using the code to communicate while the other would be trying to crack the code. Or you could divide the class into teams with a prize for the team that cracks the code first.

Another option is to develop an alphabet of symbols and use that alphabet to encode and decode simple messages.

Practical Exercises. There are several practical exercises that can be used to teach about SIGINT.

"Radio Silence" In the first phase of this exercise, students refrain from using their cell phones, tablets, and computers for a fixed time period. No cell calls, no texting, no emails. To be effective, the time frame has to be long enough to be more than a minor inconvenience. While radio silence prevents the interception of messages by unauthorized persons, the associated inability to communicate has other effects. These are interesting to explore.

In the subsequent phase of this exercise, the instructor explains the concept of 'sneaker-net,' whereby students put their e-mails or messages on a thumb drive and another student sends his communications out for them. This is the method employed for years by Osama bin Laden (OBL) as a means to avoid detection by SIGINT. His computer was not connected to the Internet. Rather, he wrote his e-mails and messages and created his audio and video presentations and loaded them on a portable drive. One of his trusted couriers then took the drive to another location where it was plugged into the Internet and the traffic sent.

Current Event Analysis Students are encouraged to analyze a major current event, such as the conflict in Libya. They have to assess how the parties involved are communicating and design a plan to intercept and analyze those communications. Students can be given a copy of the US Army Field Manual 2.0 on Intelligence, available at: *http://www.fas.org/irp/doddir/army/fm2-0.pdf*. Depending on the nature of the class, this exercise can be supplemented with maps and students asked to 'plot' key locations of people and/or places and indicate those that might be fruitful sources of intelligence. Instructors could expand the scope of the exercise by encouraging the use of Google Earth as means of providing Imagery Intelligence (IMINT) as well.

CONCLUSION

Signals Intelligence has had a profound impact on conflicts and diplomacy throughout history. Today's reliance on electronic communications over smart phones and tablets and the ubiquitous nature of the Internet means that SIGINT will remain a major source of intelligence in the future.

READINGS FOR INSTRUCTORS

James Bamford has written extensively on NSA and signals intelligence. His 1982 *The Puzzle Palace: Inside America's Most Secret Intelligence Organization* (Penguin Group) was at that time a controversial exposé. His later books were *Body of Secrets* (2001, Anchor Books) and *The Shadow Factory: The NSA from 9/11 to Eavesdropping on America* (2009, Anchor Books). A recent comprehensive history and examination of NSA is by Matthew Aid, *Secret Sentry: the Untold History of the National Security Agency* (2010, Bloomsbury Press).

Other recommended books include Barbara Tuchman, *The Zimmermann Telegram* (1958, Ballantine Books); Simon Singh, *The Code Book: The Science of Secrecy* *from Ancient Egypt to Quantum Cryptology* (1999, Anchor Books); and Mitchell B. Lerner, *The Pueblo Incident: A spy Ship and the Failure of American Foreign Policy* (2002, Modern War Studies, University of Kansas Press). *The Zimmermann Telegram* is an easy read and might seem to be more of a thriller than a historical commentary. Singh's book is an excellent primer for anyone who is interested in cryptography.

Two widely acclaimed books, fundamental for students of SIGINT, are David Kahn's massive *The Codebreakers: The Comprehensive History of Secret Communications from Ancient Times to he Internet* (1967, Scribner) and Roberta Wohlstetter's seminal analysis of the failure of warning at Pearl Harbor, *Pearl Harbor: Warning and Decision* (1962, Stanford University Press). *The Codebreakers* is a classic, but due to its length and technical content, not for the timid.

Several websites are valuable for teaching about SIGINT. Most titles are descriptive enough.

- *www.nsa.gov* — The NSA website is quite authoritative. A visit to the National Cryptologic Museum next to NSA at Fort Meade, MD, is also worthwhile.
- *http://www.nsa.gov/about/_files/cryptologic_heritage/publications/coldwar/venona_story.pdf* — Venona was the codeword associated with the breaking of the Soviet codes used by its spies in the United States during and just after World War II.
- *http://www.crows.org/* —This is the site of the trade association of electronic warfare and information operations vendors and professionals. It takes its name from the "Ravens," who were the mascots of radar operators during WWII. The Old Crows provide a wealth of information on Electronic Warfare, Computer Network Operations and have also become a respected source of resources for Information Operations (IO).
- *http://www.usspueblo.org/* — for materials on the Pueblo incident.
- COMINT and the Battle of Midway: *http://ibiblio.org/hyperwar/PTO/Magic/COMINT-Midway.html* — (a site of the National Archives and Records Administration).
- Pearl Harbor Revisited; Navy Communications 1924–1941; *http://www.history.navy.mil/books/comint/ComInt-Biblio.html* — (US Navy, Naval Historical Center)
- 1990 Army War College Paper on the History of COMINT; *http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA237861&Location=U2&doc=GetTRDoc.pdf*
- 1996 Presentation about Ultra at Bletchley Park by Sir Harry Hinsley, the official historian of British Intelligence in World War II. Ultra was the codeword associated with the breaking of the Nazi codes during World War II. *http://www.cl.cam.ac.uk/research/security/Historical/hinsley.html*
- *http://vivausafss.org/Kivett.htm* — An on-line record of experiences by a former member of the Air Force's SIGINT organization.
- *Breakdown: How America's Intelligence Failures Led to September 11*, by Bill Gertz, Regnery, Washington, D.C., published August 25, 2002, *http://www.crows.org/* (Gertz is an investigative journalist with *Washington Times* newspaper.)
- Intelligence Failures in Viet Nam; *http://academic.brooklyn.cuny.edu/history/johnson/65vn-5.htm*
- NSA Releases History of Cold War Intelligence: *http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB260/index.htm*
- A Brief Look At ELINT: *http://ftp.fas.org/irp/nsa/almanac-elint.pdf*
- Army Security Agency (ASA) COMSEC site: *http://www.davehatfield.com/davehatfield/ASACOMSEC.html*
- Article on space-based SIGINT and satellites of many countries is at *http://en.citizendium.org/wiki/SIGINT_space-based_platforms*

Lawrence Dietz is chief legal officer of TAL Global and has over 30 years of military and commercial intelligence and security experience. As an Adjunct Professor for American Military University, he teaches about intelligence and security. He retired as a Colonel in the U.S. Army Reserve. His degrees include BS in Business Administration, Northeastern University; MBA (with distinction), Babson College; JD, Suffolk University Law School; LLM in European Law, University of Leicester, United Kingdom; and MS in Strategic Studies, US Army War College. He is the author of a blog on Psychological Operations (PSYOP) at *http://psyopregiment.blogspot.com*.

> **The best field operative**
> **is he who makes**
> **the smallest amount of lying**
> **go the longest way.**
>
> **— Samuel Butler**
> **[amended quote]**