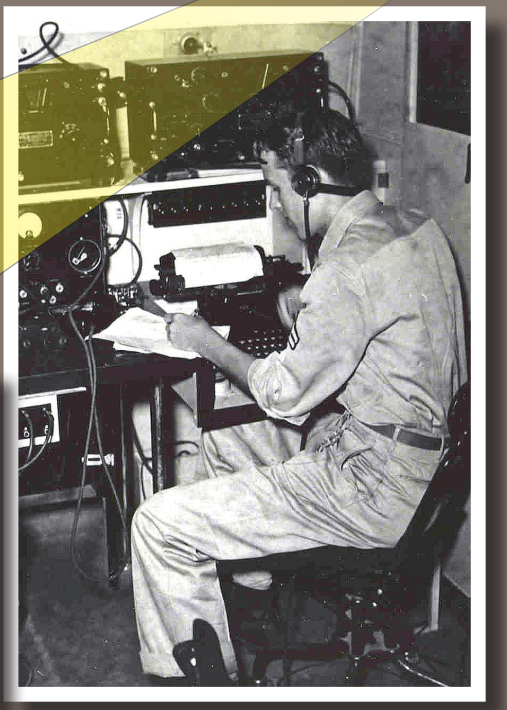
The History of Traffic Analysis: World War I–Vietnam



This publication presents a historical perspective for informational and educational purposes, is the result of independent research, and does not necessarily reflect a position of NSA/CSS or any other U.S. government entity.

This publication is distributed free by the National Security Agency. If you would like additional copies, please submit your request to:

Center for Cryptologic History
National Security Agency
9800 Savage Road, Suite 6886
Fort George G. Meade, MD 20755

Front cover: (l) General Heinz Guderian in armored command vehicle with an Engima machine in use, May 1940. *German Federal Archive;* (r) U.S. Army operator, WWII
Back: Sample military radio network, *NSA Office of Training Services, 1964*

The History of Traffic Analysis: World War I–Vietnam

Donald A. Borrmann,
William T. Kvetkas, Charles V. Brown,
Michael J. Flatley, and Robert Hunt

Center for Cryptologic History
National Security Agency
2013

Signals intelligence (SIGINT) is a major segment of the intelligence discipline, and communications intelligence (COMINT) is a subset of SIGINT. In turn, "traffic analysis" (T/A) is a significant part of COMINT while also useful in other aspects of SIGINT. This brochure defines and explains traffic analysis when used in this context, as part of the broader discipline of signals intelligence.[1] The brochure describes the elements of T/A and explains how T/A has been used for several purposes including to produce intelligence information, to aid cryptanalysis, and to support the collection of additional data. It then presents examples of intelligence contributions made by T/A during World War I, World War II, and the Cold War, including the Korean War and the Vietnam War.

A key purpose of this brochure is to improve the public's and intelligence professionals' understanding of T/A as an intelligence discipline. Further, it is intended that this will be a living document, to be amplified and expanded as the necessary research is completed, especially in light of new real-world examples of traffic analysis at work. In its present form, the report also can be used for historical reference and could even serve as a basis for developing museum displays.

Definition

The word *traffic* to a communicator or cryptologist referred to communications passed between a sender and an intended recipient. Thus, the study of traffic by unintended recipients was called traffic analysis.

T/A has been the study of "external" features of target communications. It also can be used against noncommunications electronic emissions and telemetry signals. It examined all aspects of communications transmissions excluding code or cipher message content, which was the purview of cryptanalysis (C/A). Traffic analysts studied signals' characteristics, including radio frequency usage, callsigns, (a series of letters and/or numbers assigned to a specific radio station), transmission schedules, locations of transmitters, the routings and volumes of message traffic, informal "chatter" between the targets' radio operators and the unique characteristics exhibited by manual Morse operators, referred to as their "fists."

T/A and C/A historically have been the major technical approaches to COMINT, and information derived from traffic analysis and cryptanalysis can be combined to gain knowledge about the senders and receivers. This knowledge was provided to customers in "end-product" reports.[2]

The Elements of Traffic Analysis

Historically, the elements of communications subject to traffic analysis were among the following:

Callsigns—Usually a brief series of letters and/or numbers assigned to a specific radio station by a government authority. The radio operator transmitted a callsign to identify the station when making contact with other radio stations. Some callsigns were permanent, while others changed periodically according to a pre-arranged plan to confuse monitoring by unintended listeners.

If the unintended listeners (COMINT units) solved the system by which the callsigns were generated and/or assigned, they could then predict the new callsigns used by individual radio stations following the periodic changes.

Frequencies—Organizations using radio communications were allotted various blocks of the radio frequency spectrum. Within these blocks, organizations selected frequencies which worked best for them. For example, in the high frequency (HF) range (3-30 MHz, which provided the bulk of the long-distance communications capability), frequency usage typically was divided between daytime and nighttime ranges, with the higher range used in the daytime for clearer reception. Radio signal propagation at nighttime usually required less power and could be heard well at the lower frequencies because of changes in atmospherics.

Military organizations, if given the capability/option, might rotate their use of individual frequencies among the stations of a network in an effort to foil COMINT units' interception and identification of individual stations. Frequency rotations were designed in advance, with stations in a network each being assigned an individual starting frequency, from which they proceeded through periodic

rotations in a prearranged manner. To be most effective in countering the COMINT unit's attempt to listen to them, military organizations would simultaneously change callsigns and frequencies. When that was not done, it usually was an easier task for the traffic analyst to equate the new callsigns to old frequencies and vice versa.

Schedules—Military radio station networks usually operated according to prearranged schedules for making contacts and sending messages. The recovery of these schedules allowed the COMINT unit to allocate its monitoring resources most efficiently, without wasting time listening for an inactive station or network. It maximized the COMINT unit's collection of messages from the network, messages that might be readable and of possible intelligence interest.

Additionally, if a station or network changed its callsigns and frequencies, but not its contact schedules, it might be possible to use communications schedules to identify stations and gain insight into the new callsign and frequency allocations, which could lead quickly to full recovery of the network and permit continued exploitation.

Address Systems—In addition to callsigns, radio stations often used message address systems to route messages to particular addressees or military units, several of which might be served by a single radio station. An example would be a radio station at an army post that housed infantry units, armored units, and a helicopter unit. Messages intended for any of these units typically would be accompanied by a message serial number, an indication of the urgency of it (message precedence), and an expression of the size of the message in some numerical form (so the recipient would know if he has received a complete message), and usually encrypted designators that specify the originator of the message as well as the specific addressees. If the address system could be solved by the traffic analysts at the COMINT unit, often with help from other information sources, unit identifications could be revealed. That "order of battle" information (usually describing a military unit's identification, organization, strength, and location) could then be compiled and maintained.

Operator Chatter—Idle chatter between radio operators generally was unencrypted and in the native language of the country where the stations were located. If, for example, the radio signal was transmitted in international Morse code, three-letter brevity codes (called "Q" and/or "Z" signals) might be used simply to shorten the transmissions in much the same way that cell phone users send text messages today. (For example, "CUL" stands for "see you later.") Chatter collected from careless radio operators often contained useful information that might not otherwise be known to the COMINT unit. Callsign, frequency, or contact schedule information might be disclosed, thus making the intercept operator's job a bit easier. Security lapses in operator chatter could contain plaintext military unit designators and/or their locations–a "gold mine": for example, "I don't have time to send you those requisitions. The 509th is about to deploy."

Some operators had distinctive transmission patterns that could be recognized even after a communications change that resulted in new callsigns, operating frequencies, and contact schedules. Further, often the type of chatter was service unique. For instance, ground forces would sign off one way and air forces another. With slim leads like those, the traffic analyst could begin to recover the new signal procedures, then identify the individual stations, and finally reconstruct the entire network. In the words of one former traffic analyst: "The traffic analyst used all of the tools described and was a miner of the repetitive idiosyncratic. Find that little piece that stands out and is different and sustains continuity through repetition."[3] Although sometimes T/A information can be deduced from a few messages, generally the larger the volume of communications, the more that can be inferred.[4]

Location and Characteristics of the Transmitter—Radio direction finding (RDF) attempts to determine the azimuth (line of bearing between the source of the signal and the receiving station) of a propagated radio signal. If the azimuth of some signal can be determined from multiple locations, then perhaps the location of the transmitter can be derived, that is, obtain a "fix" on the transmitter's location. At times even a single azimuth can be helpful. RDF was particularly useful in locating and following the

movements of military units. Further, individual transmitters have unique technical characteristics which, if detected, can be useful to the traffic analyst.

The Role of Traffic Analysis

Production of Intelligence

The first step in intelligence production was to determine what the customers' requirements for information were and how they could be satisfied by SIGINT, including T/A. Then collection managers identified the targets to be collected and assigned the specific tasks to be accomplished to stations, often based upon the station's technical capabilities and its geographic access to the target signals.

Diplomatic, army, navy, air force, terrorist, commercial, and other foreign communications have been subject to traffic analysis. The structure of the military communications networks reflected the underlying structure of the military organizations they served. For example, a "net control" station and its "outstations" may portray a division and its regiments. T/A involves the study of the target's radio communications features, thereby helping to identify and locate the communication units and keep track of their signal activity and location over a period of time. All of these actions helped produce information known as "order of battle," which is critical to understanding enemy capabilities.

The value of any intelligence product, however, depended in part upon how effectively the recipient used the data. Throughout history, many of the so-called "intelligence failures" were incorrectly labeled. In all too many instances good intelligence had been forwarded to the user/customer only to have it ignored or rejected. This is as true of T/A as of any element of intelligence production.

Support to Cryptanalysis

T/A supported C/A by providing current information on the identity, location, and relationships of the originators and recipients of the messages, all of which offered help to the cryptanalysts in solving codes and ciphers.

One British author observed during World War II that "Only if the cryptanalyst were in close contact with those responsible for enemy interception and for Traffic Analysis could the cryptanalytical obstacles be surmounted with minimum delay."[5]

Guiding the Interception of Communications

T/A was used to assist intercept operators by providing current data on radio frequencies, callsigns, and transmission schedules used by the targets. In return, the intercept operators assisted the traffic analyst by their recognition of unique identifying characteristics of the target radio operators and their equipment, somewhat similar to recognizing the voice of a telephone caller.

A significant challenge was maintaining a current database on all prospective targets. Having current technical data available allowed the intercept operator to access the desired communications without first spending weeks or months building background information on the target communications. Given the changing nature of communications, the building and maintaining of technical data were an important and never-ending process.

Countering Deception

The target forces took many measures to make it difficult to intercept and exploit their communications. Measures they used included constantly changing their radio frequencies, callsigns, and communications transmission schedules and reducing the length of time they were on the air. They also encrypted addresses and operator chatter or sent false (or "dummy") traffic; they even rapidly switched from one mode of communications to another.

A challenge to traffic analysts was to determine when the target communications were being fabricated in an effort to mis-

lead. Callsigns, frequencies, and other elements of radio transmissions might be altered to indicate that military units were neither the units they seemed to be nor were they located where they appeared to be. A good example of this type of deception was used by the Allies in WWII creating the illusion of an Allied army that did not exist. The ruse was supported by establishing a communications network across from the Pas de Calais just before the Normandy invasion.

Summary

A hypothetical analogy using postal mail may clarify the concept of T/A in more familiar terms. In the case of postal mail, the content of the envelope would be the purview of cryptanalysis, whereas the study of the address, the return address, and the date stamp would be akin to traffic analysis. Study of these external features could reveal identification of banks, stockbrokers, credit unions, employers, doctors, dentists, friends, relatives, etc., and how often and when mail contact is maintained with these recipients. For example, T/A in this context might reveal that an individual had been diagnosed as seriously ill based on communications with doctors and insurance companies, or that the person is under financial stress based on the volume of letters from collection agencies and banks.

History

Traffic analysis has been of key importance in providing current information to U. S. military commanders on the identity, location, and movement of opposing enemy forces at the tactical and strategic levels. Although some use was made of the discipline as early as the American Civil War, information derived from traffic analysis was critical in influencing and winning many ground, sea, and air battles of World Wars I and II, Korea, Vietnam, Iraq, and other conflicts. T/A also has been useful in supporting diplomatic initiatives, and, especially during the Cold War, it supported counterintelligence, counterterrorism, and counternarcotics efforts, as well as the country's response to numerous international crises.

World War I

When the American Expeditionary Force (AEF) entered WWI in 1917, it was not schooled in the use of traffic analysis. British and French intelligence services provided the AEF personnel a "crash

Illustration 1. German troops and officers manning a wireless field telegraph station, WWI

course" in the art of traffic analysis. The AEF sought "to describe the enemy's forces, to determine the locations of his units, discover his intentions, and where and when he would carry them out."[6] T/A was one of the primary sources of intelligence contributing to the satisfaction of these operational requirements.

Military intelligence improved markedly during WWI, and the sources and methods developed there continued to produce information for decades to come. The static front with its miles of trenches diminished the value of cavalry and espionage as sources. The advent of reconnaissance information from airplanes and more particularly T/A of enemy communications filled the intelligence gap by providing accurate and timely information.[7]

Army and Air Corps

There were three main means of electronic communications used by ground forces in the front battle lines of WWI. One was radio; another was telegraph on wires; and the other was called a "power buzzer," a device that sent communications for short distances by using the ground as a conductor. Each was susceptible to being intercepted by the opposition, and traffic analysis was possible on intercept from these sources. It was mainly the advent of radio, however, that brought traffic analysis into the fore.

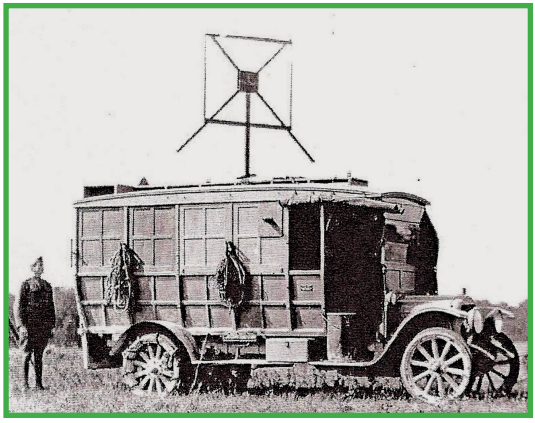


Illustration 2. U.S. radio direction finding vehicle, WWI. *CCH print #11, 1A, Potter 870-11*

During 1917 and 1918, T/A may well have been the single greatest source of operational intelligence available to every army on the Western Front.[8] For instance, it has been estimated that T/A, during that period, determined the location of 50-60 percent of the German divisions and military groupings on the British front.[9]

Radio direction finding (RDF), called "goniometry" at that time, also provided critical information on enemy locations (see Illustration 2 showing a direction finding vehicle). One officer described its use in the intelligence process as follows: "Just as naturalists can reconstruct from a few bones a prehistoric monster, which they had never seen, so the goniometric experts are able to gain an amazingly accurate idea of the organization of an army by locating its stations, for the lines of radio communication, which spread fan-wise from army headquarters, form a sort of skeleton, as it were, of the army's organization, the location of the various stations and their distance from headquarters indicating quite accurately the position of the corps, divisions, brigades, regiments, and battalions."[10]

Another prominent target of traffic analysis intelligence during WWI was communications supporting the fledgling aircraft activity. Just as with infantry and artillery, the employment of aircraft required radio communications between headquarters and the aero-

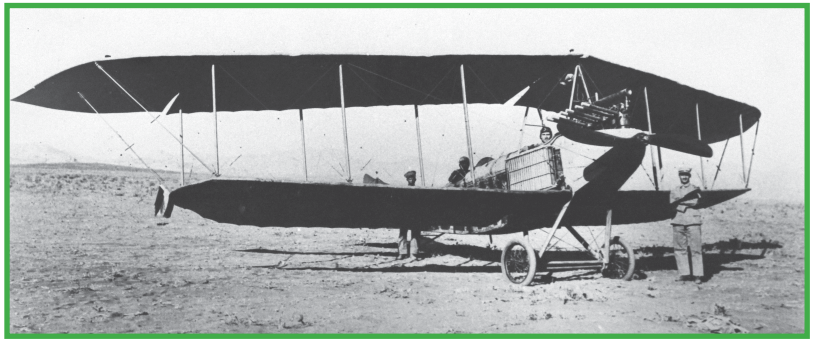


Illustration 3. German spotter aircraft "Roland" used for reconnaissance early in World War I

dromes, and those transmissions were susceptible to interception and exploitation.

One particularly useful application of T/A information was employed against German spotter aircraft. The trench warfare on the front became a battle of attrition, and artillery was a key element in this aspect of the war. Artillery fire was directed in large part through the use of aircraft flying over the battlefield, which would locate high-priority targets, direct artillery fire at them, and assist in calibrating the accuracy of that fire. The British, in particular, used T/A to predict the spotter aircraft flights and, with great effect, direct British intercept aircraft to destroy or disrupt the German flights. These efforts significantly decreased the effectiveness of German artillery.[11] Further, in those instances when the German aircraft got through, the Allied units that were to be targeted by the artillery barrage were warned of possible impending artillery attacks based upon the activity of the aircraft. This warning gave the targeted units some opportunity to take cover and evade fire.

T/A also supported electronic deception, which was practiced during WWI. An army would deliberately send false signals to mislead the enemy into thinking that military units had moved (or not moved). One prominent example was when the British generated a message transmission pattern that led the Germans to believe that the crack Australian and Canadian units remained on the line in Flanders. Under signals silence these units moved to Amiens and participated in an attack that crushed the unsuspecting Germans.[12]

Navy: The Battle of Jutland, May 1916

Early in World War I the British fleet was the dominant force on the high seas. The Germans, on the other hand, were in the process of developing a respectable surface navy. In the spring of 1916, Admiral von Scheer, the new commander-in-chief of the German High Seas Fleet, planned to entice the British Grand Fleet into a sea battle during which he hoped to engage the British fleet in segments and inflict serious losses upon the British without incurring devastating German losses. Meanwhile, the British wanted to counter any German moves, attempting to keep them at bay and inflict whatever

damage to the German fleet that they could, without incurring a significant degradation of their own fleet, which they needed to keep intact for the defense of the home islands. One problem the British Navy had at this point was the regular navy's lack of confidence in the Naval Intelligence arm (Room 40) to support the operational commands in offensive tactical maneuvers. The Room 40 analysts were not permitted to be involved in anything but defensive operations, and were unable to directly communicate with fleet components. Even though the naval intelligence analysts had built a good working knowledge of the organization and operations of the German Fleet, they were not permitted until 1917 to provide any direct support to the British Navy for operational activities.

On 30 May 1916, the two main segments of the British fleet which were in port at Scapa Flow under Admiral John Jellicoe and at Rosyth under Vice Admiral David Beatty, were advised, based on decrypted signals and traffic analysis, that von Scheer intended to put to sea early the next day.[13] That evening, Jellicoe ordered both elements of the Grand Fleet out to sea. Early on the 31st, German battle cruisers left Wilhelmshaven to decoy the British Fleet into the North Sea, with the rest of von Scheer's High Seas Fleet to follow. It so happened that although von Sheer's intelligence had alerted him to the deployment of the British Fleet, he decided to proceed as planned. The two components of the British Fleet led by Jellicoe and Beatty, after setting sail on the 31st, were planning to trap the German Fleet based on their earlier intelligence warnings. Unfortunately, the British naval operation was disrupted when the Director of Naval Operations injected himself between the intelligence analysts and the combat commanders.

On the morning of May 31, after the British Fleet had departed Scapa Flow and Rosyth, Rear Adm. Thomas Jackson, the regular navy DNO, made an early and rare visit to his operations center, where he asked the naval intelligence analysts a traffic analysis question. Having seen a report based on T/A that located the callsign DK in port at Wilhelmshaven, Thomas inquired of the meaning of that callsign. With no details provided, the analysts replied that DK was Admiral von Scheer's personal callsign. Without waiting for clarifi-

cation or checking further to find that Admiral von Scheer used a different callsign when deploying, while the DK callsign remained at Fleet Headquarters to disguise the Fleet Commander's movements, Jackson left the ops center to alert Jellicoe and Beatty of his conclusion that the German Fleet was still in port. Shortly after noon on the 31st, the two British commanders received the following cable: "At 12 Noon today, our directional stations place the German fleet flagship ((at its base)) in the Jade. Consider it possible that lack of air reconnaissance may have delayed their start." Admiral Jellicoe, on receiving this wire, delayed his movement toward the German Fleet, leaving V/Admiral Beatty nearly 70 miles out in front of Jellicoe, where he quickly met the entire German Fleet. Although caught by surprise after the misleading information provided in error, Beatty, though losing two cruisers and suffering serious damage to his flagship, through a brilliant maneuver, lured the German Fleet into the path of the entire British Fleet. Beatty and Jellicoe, with the combined British fleet, then forced the Germans back to port, with nei-

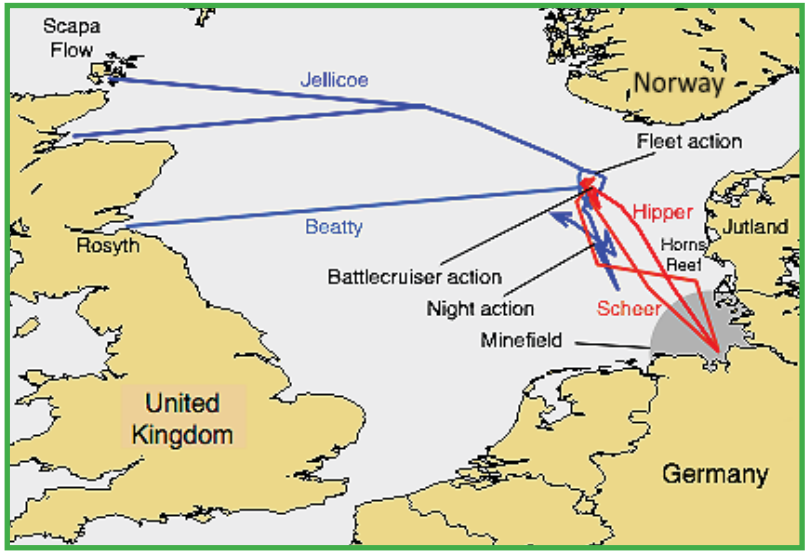


Illustration 4. The Battle of Jutland, May 1916

ther side sustaining unacceptable damage. Jellicoe, however, missed a splendid opportunity to decimate the German Fleet on its return to port by not using his intelligence fully and by his timidity, stoked by his desire to preserve the British fleet. Even worse, Jellicoe had apparently become jaded regarding the quality of his intelligence and although receiving accurate information on the direction of Scheer's return route to port, he refused to rely upon it, causing him to miss the opportunity to inflict serious damage to the German fleet. This situation represents a classic instance where solid traffic analysis was misunderstood, misused, and not allowed to provide a potential naval victory which might have altered the outcome of not only a naval operation, but perhaps the war itself.

Illustration 5. Lt. Donald A. Borrmann in India, 1945. *Borrmann personal files*

World War II

China, Burma, India: The CBI Theater

One of the authors of this report, Donald A. Borrmann, who served as a T/A Officer in India and China during WWII, furnished this information concerning the CBI.

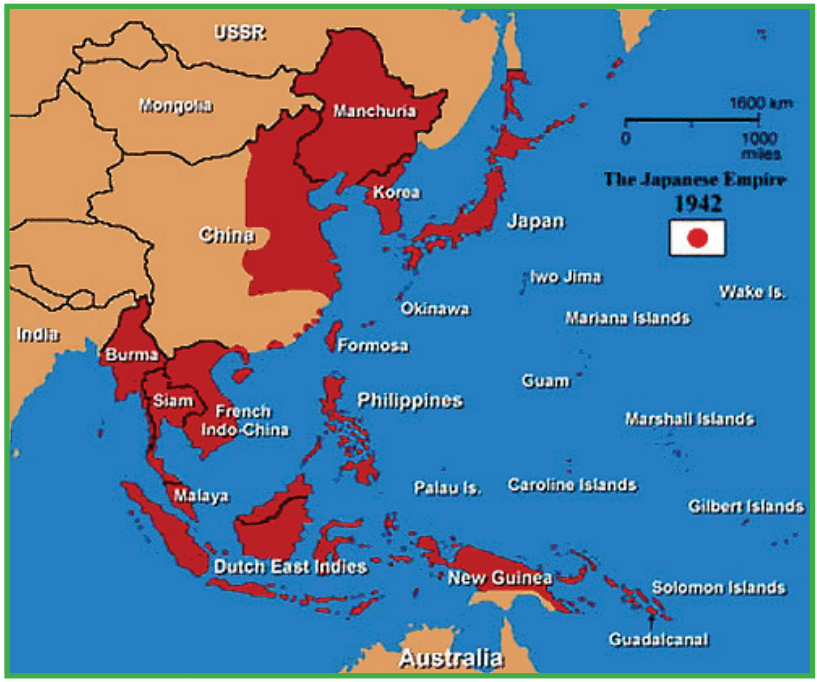


Illustration 6. The China/Burma/India theater, WWII

The CBI Theater was important to the Allies in WWII but did not involve the numbers of U. S. troops that fought in Europe and the Pacific.

The U. S. strategic objectives were to maintain the Chinese Nationalist government's ability to engage significant Japanese forces in China, to protect India from invasion, and to re-take Burma from the Japanese.

The CBI Theater Headquarters at New Delhi, India, included a unit of the Signals Intelligence Service (SIS) headed by Col. Leonard Bickwit. I know that the Allied effort to re-take Burma was given support from signals intelligence, including T/A, but I cannot furnish specifics because my own assignment involved Japanese forces in China, and the need-to-know security policy was very much in force during

the war. Additionally, due to the nature of the fighting in Burma, with Allied irregular forces implanted in Japanese-occupied areas, valuable intelligence also was provided by human sources (HUMINT).

Concerning Japanese forces in China, I can document a specific example of the value of T/A as follows: By early 1945 the Japanese army's 'Ichi Go' offensive in China had succeeded in occupying the most forward bases (including Liuchow and Kweilin) of the U.S. Army 14th Air Force, which included some of the former members of the famous Flying Tigers unit. At that time the U.S. Army G-2 in New Delhi informed Col. Bickwit that he was receiving valuable signals intelligence on these Japanese forces in China and wished to know more about how it was produced. The source was T/A, so Col. Bickwit took me to brief the G-2 on how, through T/A on Japanese army communications, it was possible to continue to identify the Japanese army units involved and their changing locations. The elements addressed in the briefing included: analyzing the radio callsigns and address systems, the communications relationships, radio network structure and message flows, and also included radio direction finding. Despite this evidence of intelligence value, circumstances were such that there was no resultant change on the battlefield in this area of China. The intelligence was provided to U.S. Army 14th Air Force and to U.S. Army advisory group personnel attached to the Chinese Nationalist army, which contributed mostly defensive resistance to the Japanese. The Japanese were not defeated in China, but their forces there did surrender at war's end.

The Pacific Theater

During WWII, COMINT, including T/A, played a vital role in the Pacific Ocean naval battles occurring as U. S. forces were "island hopping" westward to secure bases necessary to support later attacks on the Japanese home islands and to prevent further expansion of Japanese forces closer to Hawaii and Australia. Successful cryptanal-

ysis of Japanese naval cipher messages was often temporarily unavailable due to Japanese cipher changes. Throughout these periods, T/A was relied on to maintain continuity on the identity of the Japanese military and naval units and their location and movements through message externals and RDF.

In 1942 there was a great disparity in favor of Japan in the number of battleships, aircraft carriers, and cruisers available to each opposing force. During the spring of 1942, prior to the naval battle in the Coral Sea, the presence and movement of Japanese naval forces into the Solomon Islands area was revealed through T/A, including RDF.[14] Less than a month later in June 1942, prior to the battle of Midway Island, T/A contributed to identifying the presence of a

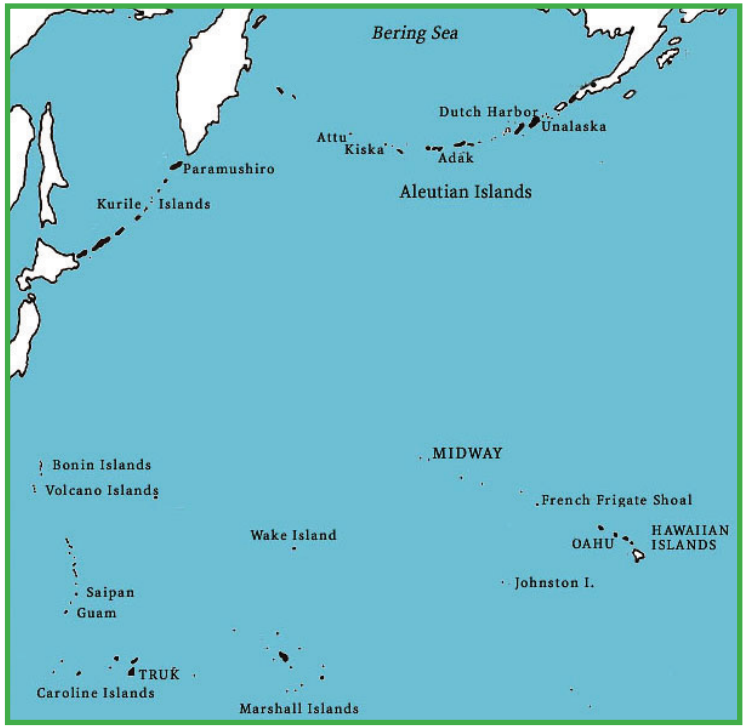


Illustration 7. The Central Pacific and Midway Island.
Frederick Parker, A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians, *CCH*

Japanese air group in the Marshall Islands, and more importantly, T/A confirmed that the entire Japanese combined fleet was en route to Midway.[15] The Japanese attack on Midway Island on June 4, 1942, resulted in a vital U.S. victory.

From August through December 1942, the Solomon Islands campaign included many engagements and actions between naval surface and submarine units and land and carrier-based aircraft. These included the U.S. landings on Tulagi and Guadalcanal islands and continuing Japanese efforts to land troop reinforcements by sea (the "Tokyo Express") on Guadalcanal (through the channel known as "the Slot"). T/A made critical contributions during this period. Prior to the U.S. landings, T/A noted a marked increase in Japanese activity in the Solomons and provided identities of the Japanese naval units involved and not involved, all of which were of great value to U.S. preparations and reactions. After the U.S. landings in August 1942, T/A was able to give many advance warnings of the numerous

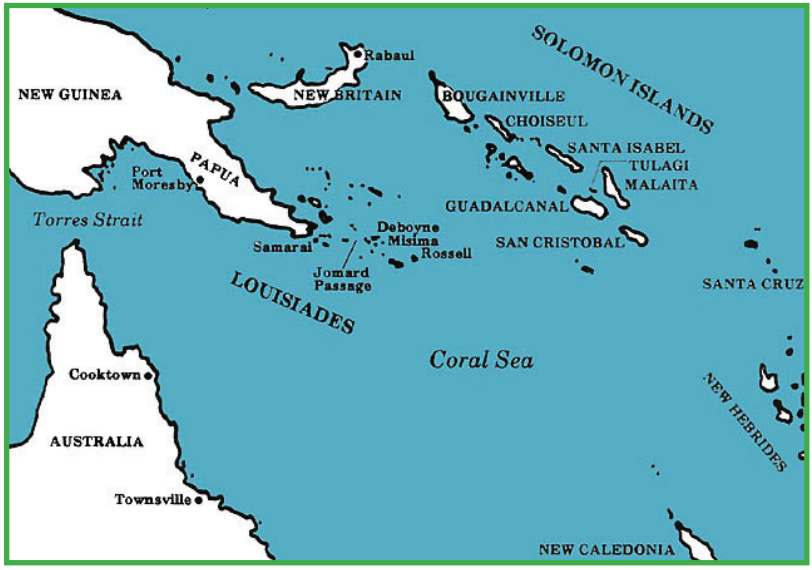


Illustration 8. The Solomon Islands, Coral Sea, and Southwest Pacific. *Frederick Parker,* A Priceless Advantage: U.S. Navy Communications Intelligence and the Battles of Coral Sea, Midway, and the Aleutians, *CCH*

nighttime "Tokyo Express" runs. Based on this information, the U.S. launched strikes, causing significant losses of Japanese ships, aircraft and troops, and forcing the eventual Japanese decision to withdraw their forces from Guadalcanal in February 1943. A quote from this period states: "The problem of attaining surprise and at the same time keeping track of enemy movements was immensely complicated by the fact that the Japanese on August 1 made a drastic change in their naval operation code, JN25, evidently scrambling the code groups." That evening the keeper of the CinCPac Command Summary wrote: "We must depend almost entirely on traffic analysis to deduce the enemy deployment."[16]

The Southwest Pacific Theater

General MacArthur became commander of the Southwest Pacific Theater after his arrival in Australia from Corregidor. SIGINT capabilities were provided in this area by Central Bureau Brisbane (CBB, a joint U.S. and Australian organization) and by the U.S. Navy's Fleet Radio Unit Melbourne (FRUMEL). These organizations provided important support as MacArthur's forces moved against the Japanese in New Guinea, bypassing and isolating Japanese units in many locations, and eventually retaking the Philippine Islands in conjunction with the U.S. Navy (also see Illustration 6).

A description of intelligence support provided by these units to MacArthur appears in an NSA history document, which states: "Traffic analysis activities were the first step in compiling an accurate Japanese order of battle. There were many instances during the war when traffic analysis was MacArthur's only source of signals intelligence because codes were unreadable at the time. One instance was the Japanese attack on Port Moresby, New Guinea, in July 1942. Another time traffic analysis had to fill the void was when the Japanese army changed their codes on 8 April 1944, as MacArthur was planning the Hollandia invasion, which was to begin on 22 April 1944."[17]

Generally T/A was able to provide accurate prediction of attacks, identify Japanese units involved, and describe Japanese troop deployments. One such instance included increased activity at Wewak in August 1943 and movement of a Japanese headquarters from Rabaul

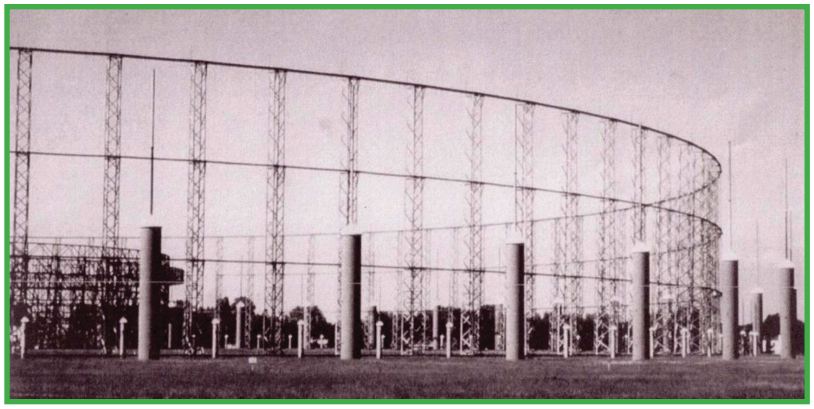


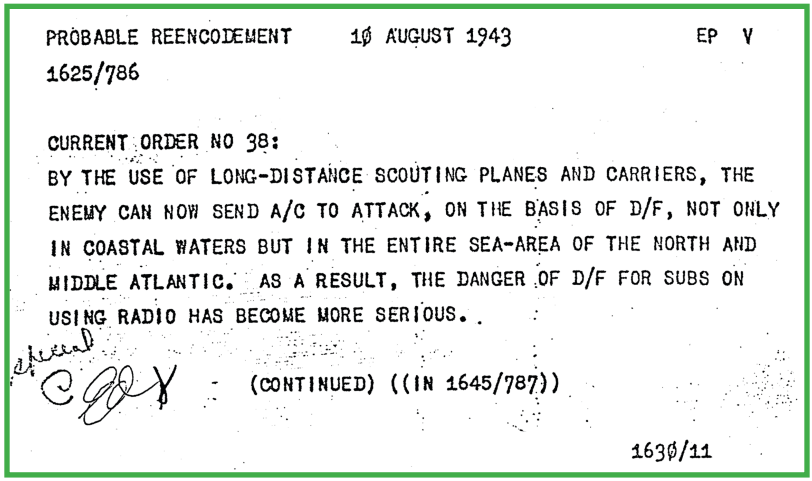
Illustration 9. Large circularly disposed antenna array used for radio direction finding and intercept. *John P. Finnegan,* The Military Intelligence Story: A Photo History, *1994, 61*

to Wewak, enabling the U.S. Army Air Force to destroy some 200 Japanese aircraft within two days. T/A forecast the Japanese intention to reinforce the island of Morotai in 1944 and the intended move of a major Japanese army headquarters from Manila to Saigon in November 1944 (later confirmed by a decrypted message).

The Battle of the North Atlantic

The German U-boat campaign against Allied shipping in the North Atlantic early in WWII was very successful in its initial stages. An average of about 500,000 shipping tons per month were lost to the U-boats between January and September 1942, and there was a serious and real concern that Great Britain would not survive if this trend continued.[18] The Allies initiated a variety of actions to stem the losses inflicted by the U-boats and to ensure that a steady flow of critical supplies safely reached the British Isles.

These actions resulted in a complete turn-around of fortunes in the North Atlantic, and German Admiral Donitz, commander of the U-boat fleet, was forced to change the focus of his efforts away from that area. Radio Direction Finding was one of the principal tools employed in this successfully coordinated approach, along with decryption of messages (ULTRA), radar, sonar, T/A and the



PROBABLE REENCODEMENT 1Ø AUGUST 1943 EP V
1625/786

CURRENT ORDER NO 38:
BY THE USE OF LONG-DISTANCE SCOUTING PLANES AND CARRIERS, THE ENEMY CAN NOW SEND A/C TO ATTACK, ON THE BASIS OF D/F, NOT ONLY IN COASTAL WATERS BUT IN THE ENTIRE SEA-AREA OF THE NORTH AND MIDDLE ATLANTIC. AS A RESULT, THE DANGER OF D/F FOR SUBS ON USING RADIO HAS BECOME MORE SERIOUS.

(CONTINUED) ((IN 1645/787))

1630/11

Illustration 10. German Enigma message referring to D/F.
National Cryptologic Museum library

increased range of land-based aircraft. Every one of these efforts contributed significantly, but, in combination, it made individual efforts extremely difficult to distinguish. This complex atmosphere had the salutary effect of "covering" the singular contributions of individual efforts and especially of the super-sensitive ULTRA source. It also prevented Admiral Donitz from determining exactly what was contributing to the high German losses.

Two distinct aspects of RDF were used in the North Atlantic. One was land based and the other mobile. Land-based H/F D/F operations, sometimes referred to as "Huff Duff," often employed large antennas. (Illustration 9 shows a more recent version of an antenna called a circularly disposed antenna array or CDAA which was used for radio intercept as well as D/F. These were so large they were referred to as "elephant cages." By contrast, illustration 2 shows a WWI land-based mobile D/F operation). D/F information from land-based sites was more strategic and was used to re-route convoys to avoid U-boat activity. Land-based D/F also was used to locate German resupply operations where supply submarines, referred to as "milch cows," were replenishing fuel and other supplies on board the attack submarines.

Most of the mobile RDF in the North Atlantic was shipborne D/F and was used extensively in tactical operations. On occasion a location or "fix" could be obtained by using cross bearings from multiple sources and then convoy escorts or even aircraft in the area could be vectored to the target. There are other occasions where an escort ship would get a line bearing from its own D/F unit and follow the line until it spotted the submarine, then initiated an attack. Line bearings from mobile naval D/F units normally were a maximum of thirty miles in length; therefore, the surface ship would expect to find the target along the prescribed line and within thirty miles. Again, although it is difficult to tally exactly the results of D/F because of the variety of information also available from other sources, it is safe to say that D/F made significant contributions to the successful prosecution of the Battle of the North Atlantic. Illustration 10 shows the German awareness of their vulnerability to D/F.

The European Theater

The U.S. Third Army. The U.S. Third Army posted one of the most impressive records among U.S. forces participating in the European campaign. The Third Army had moved from the U.S. to England in December 1943, but did not take part directly in the Normandy invasion. It moved to the continent shortly after the initial wave of troops and equipment had landed.

Meanwhile, LTG George S. Patton, one of the most prominent U.S. generals of WWII and highly respected and feared by the Germans, had incurred the anger of his superiors in 1943. As a disciplinary measure, he had been relegated to a diversionary role just prior to the invasion of the continent. He was placed in charge of a largely phantom army stationed across the English Channel from Pas de Calais in an attempt to reinforce the Germans' erroneous belief that the Allies would invade directly across the Channel. In combination with other imaginative deception operations, the ruse worked perfectly and then General Patton, known for his aggressive strategy, was assigned as commander of the Third Army.

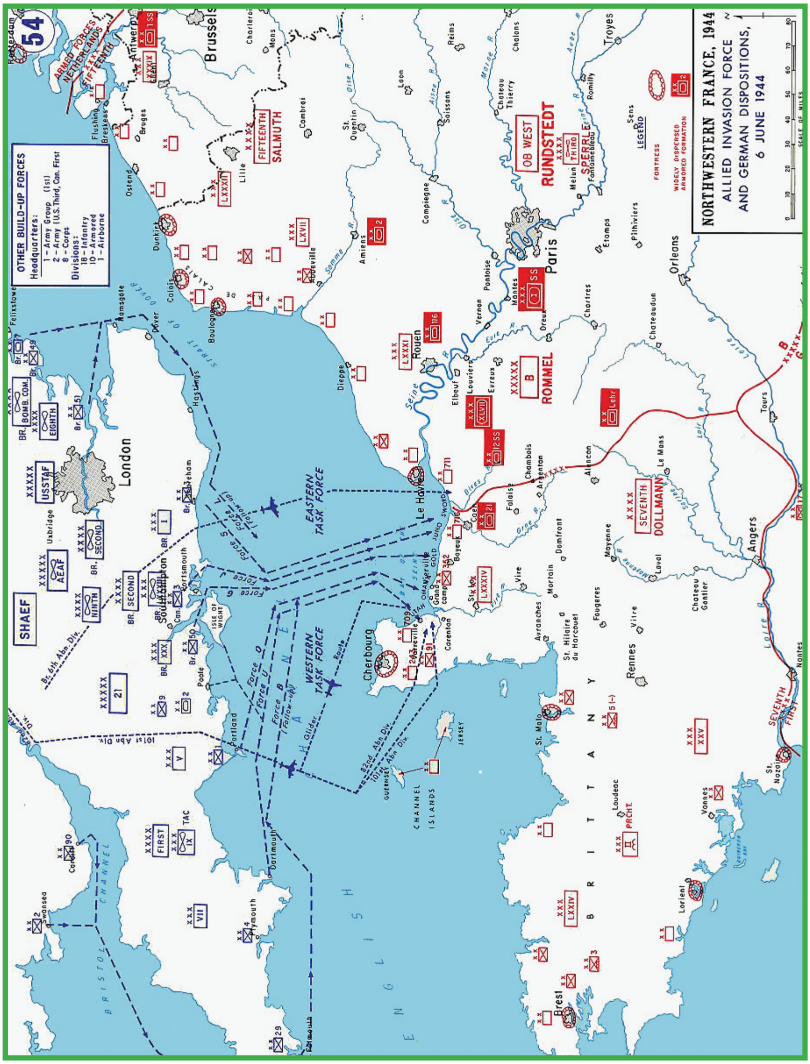


Illustration 11. Allied Normandy invasion force

Providing intelligence to an army with such mobility was a challenge. The 3253/4/5 Signals Service Companies were established in April and May 1944 for that purpose. These units trained in England and then were attached to the various Third Army Corps; the 3253rd deployed to Omaha Beach in France, arriving on July 12, 1944. The intelligence

Illustration 12. Location of the Third Army near Falaise, France

units provided information to the various elements of the Third Army throughout its movements through France and into Germany.[19]

T/A, and its incorporation of RDF, was a critical source of the intelligence information provided to the Third Army. The two were so closely interdependent that arrangements were made to perform the tasks together where a traffic analyst usually plotted the RDF bearings.[20]

The principal source of information derived from T/A came from German armored units. Even before the Third Army deployed to France, it was found that the German 21 Panzer Division was committed to the Caen area of France. Later, on 31 July 1944, the HQ of the 2 SS Panzer Division was located at Montbray, and they needed ammunition. Information also was provided on infantry deployments. The German 268th Infantry Division was located in the Guingamp area directly in the path of the U.S. VIII Corps. All of this information gave the Third Army an indication of what they were about to face.

As the Third Army moved east through France in August 1944, there was an Allied operation to trap German units in the Falaise area known as the "Falaise pocket." Third Army intelligence, mainly through T/A, was following the locations of many German armored units, and all were determined to be on the left flank and not on the Third Army front, thereby allowing Patton to move forward expeditiously. Six Panzer units were deployed on Patton's left: the 116, 2 SS, 9 SS, 130, 17 SS, 10 SS, and two other elements. These units were described as "the real backbone of the German Army."[21] Through 15 August 1944, constant monitoring of these units indicated no movement to the Third Army front, allowing Patton to move forward in an attempt to close the pocket. General Patton is known to have chided his competitors for not moving fast enough to successfully close the gap.

Later in August, the 2 SS Panzer and the 130 Panzer moved eastward through the gap in the Falaise pocket. T/A then detected the 130 Panzer moving north beyond Paris well away from the Third Army, thereby removing it as an immediate threat. T/A and RDF continued to provide the Third Army with information on the identification and movement of other German units opposing it and, on 30 August, identified and located the 3 Panzer Grenadier Division, which had just arrived from Italy to oppose the Third Army. It was the first of several German divisions to move in from Italy.

A wide variety of SIGINT continued to be provided throughout September, including daily reports on the enemy order of battle, reor-

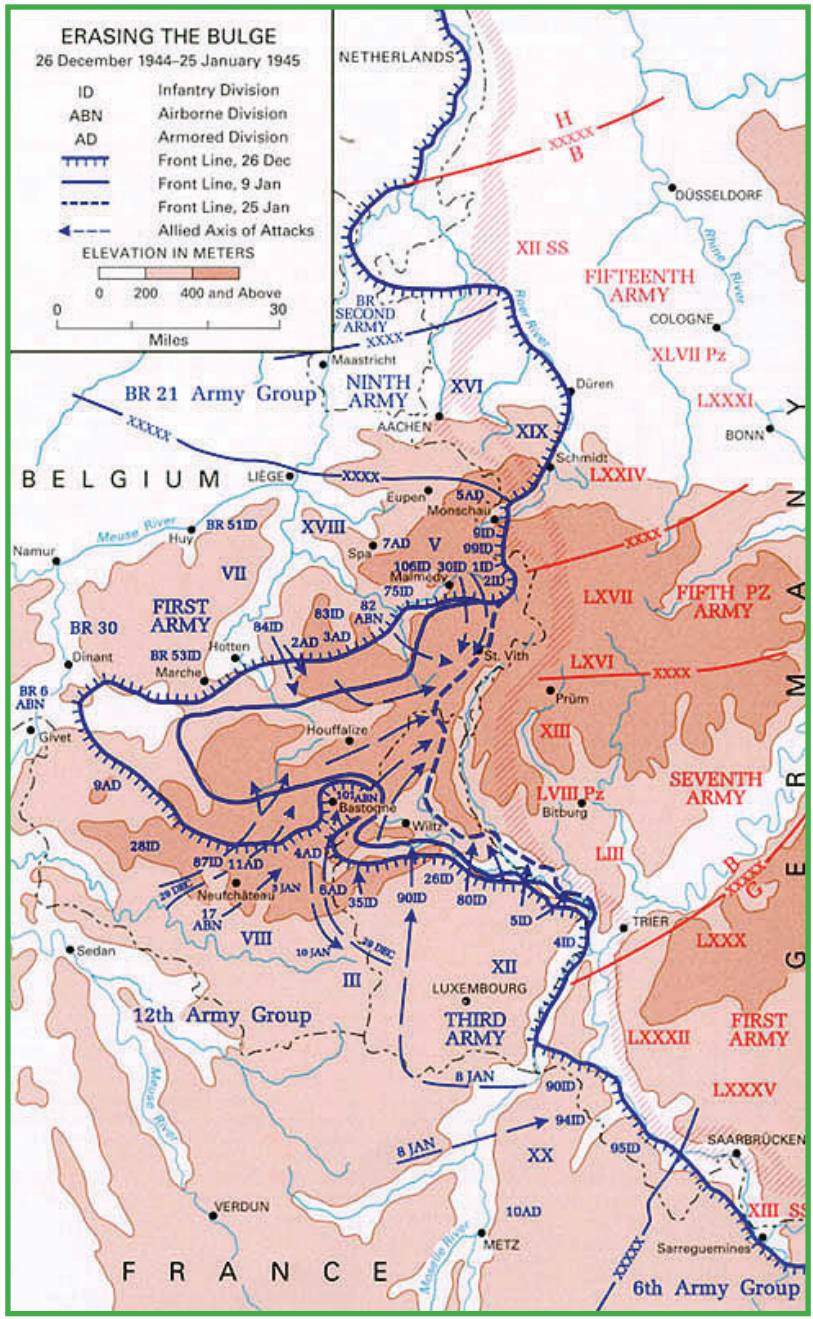


Illustration 13. The Third Army at the Battle of the Bulge

ganization of units, movements and location of units including withdrawal and reinforcements. Then in October and November there was a reduction of German activity. Further, the Germans instituted an extensive change in their communications procedures. Both of these factors resulted in a significant reduction in the production of intelligence. Meanwhile, however, analysis indicated a general move back to the "static Moselle front,"[22] and one message said that the 130 Panzer was to move north to an assembly area.

Activity on the Third Army front remained quiet until late December 1944 when the "Von Runstedt" offensive took place, more commonly known as "the Battle of the Bulge." The 130 Panzer became active in the area of Bastogne, and shortly thereafter many other German units appeared in that sector. The 3 Panzer was located there on 30 December.

As the recovery of the German communications systems progressed, by January 1945 information from T/A increased significantly in volume and quality. Five Panzer divisions were located in new locations, and the 3 Panzer was located retreating east from the Bulge, as were the 130 Panzer and the 2 SS Panzer, in spite of rumors that the latter had gone to the Russian front. The 21 Panzer and the 17 SS Panzer moved south, and there was an almost complete withdrawal of German armor from the Third Army front. Meanwhile, painstaking analysis of procedural characteristics and good RDF determined that the 130 Panzer was located in an assembly area at Bitburg.

Valuable information was provided to General Patton, assisting him in the difficult process of crossing the Rhine. The German resistance was in a general state of disarray, but fragmented reports on miscellaneous German units pressed into defense were available to the Third Army. Reports were issued on the status of Rhine bridges around Mainz and on the bridge at Remagen.[23] Information on German vehicles heading toward the bridges at Mainz was sent to the U.S. Army Air Force, which reacted adroitly and destroyed the vehicles.

In February 1945 T/A reflected the general disintegration of the German forces. On the other hand, the Allied front was converging

Illustration 14. Narvik, Norway, 1940

with the Russian front, and interception of communications from German units on both fronts became common. Having this access to information was fortuitous in one respect as the German units from the Russian front could quickly turn and attack the Third Army. In this regard, the Third Army continued to receive locations of the 9 SS Panzer, the 21 Panzer, and the 10 SS Panzer even though at that time they were facing the Russian front.

In summary, the Third Army received intelligence of inestimable value during its entire campaign across Europe. Although some information was provided by reading low-level codes, photography, prisoners' interrogation, and scouts, the preponderance of accurate and timely information was provided by T/A in combination with RDF.

The Army Air Corps

The German Air Force produced a large amount of tactical traffic in the course of training, and this allowed T/A to accurately estimate the current operational strength and disposition of Germany's bombers and reconnaissance units.[24]

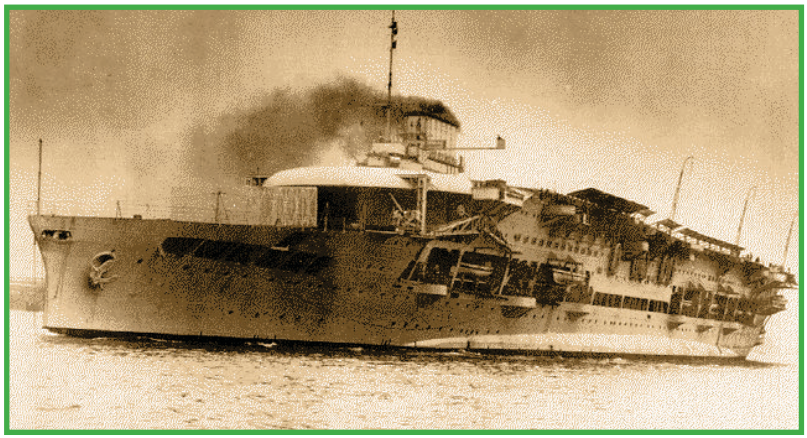


Illustration 15. The HMS *Glorious*

The British Evacuation of Norway

Early in World War II, the British position in Norway became untenable, and they decided to remove their forces.

The operation to accomplish this task took place in Narvik, Norway. It was supported by the aircraft carrier HMS *Glorious*, which evacuated pilots and planes. British T/A produced indications that German naval units were transiting into the North Sea and in all likelihood were prepared to engage in hostilities. These reports, some as early as two weeks before the engagement, were sent to the British Admiralty which, having little understanding of T/A, dismissed the reports as unproven and failed to send the warning to the *Glorious*. In fact, the German battle cruisers *Scharnhorst* and *Gneisenau* were moving into the North Sea and about to engage the *Glorious*. Had the *Glorious* received the warning, she might well have sent out defensive patrols and even attacked the German cruisers with her torpedo planes. The captain of the *Glorious*, however, not having received the intelligence reports, was totally surprised by the German presence. This fact, added to several incompetent moves on his part, led to his ship being sunk before he could get a message off to his headquarters that he was under attack. Ironically, the British learned of the disaster

by reading German messages reporting the sinking of the *Glorious*. This painful lesson clearly illustrated the value of T/A and the consequences of not using it properly.[25] The British did give much greater credence to COMINT after this unfortunate incident.[26]

German Use of Traffic Analysis

The Germans used COMINT extensively in WWII, and they were fully aware of its value. Their efforts in WWII were based upon their WWI experience, which led them to make a strategic decision at the outset of WWII to emphasize efforts against low-level and medium-grade cipher systems rather than dedicating scarce resources on the slim possibility of exploiting high-grade ciphers. The Germans were quite successful in attacking medium- and low-grade cipher systems.[27] Further, their attempts to produce information through T/A, along with RDF and reading operator chatter and other low-level clear text traffic, yielded the major source of their tactical intelligence information during the war.[28] Some examples follow.

The Germans had mounted an offensive in the Crimea on the Black Sea and were moving against the port at Sevastopol. The Soviets levied counterattacks against the Germans, but the Germans had intercepted wire communications, allowing them to save two of their patrols from annihilation. The same source on another day gave warning to the Germans of two Soviet attacks on their position. Both were repulsed, and after the second attack, they counterattacked with an artillery barrage.[29]

In another case the Soviets attempted to spoof the Germans, but one experienced German intercept operator detected the ruse. A Soviet army unit was moving to Stalingrad and left a communications group at its original position. The unit maintained its communications pattern, indicating to the Germans that the Soviet unit remained in its original location; however, one of the communications operators, who moved with the Soviet army, made the mistake of transmitting from his new location. The astute German intercept operator recognized the Russian communicator and warned the German command that the Soviet unit was actually moving toward Stalingrad. The Germans took appropriate defensive measures.[30]

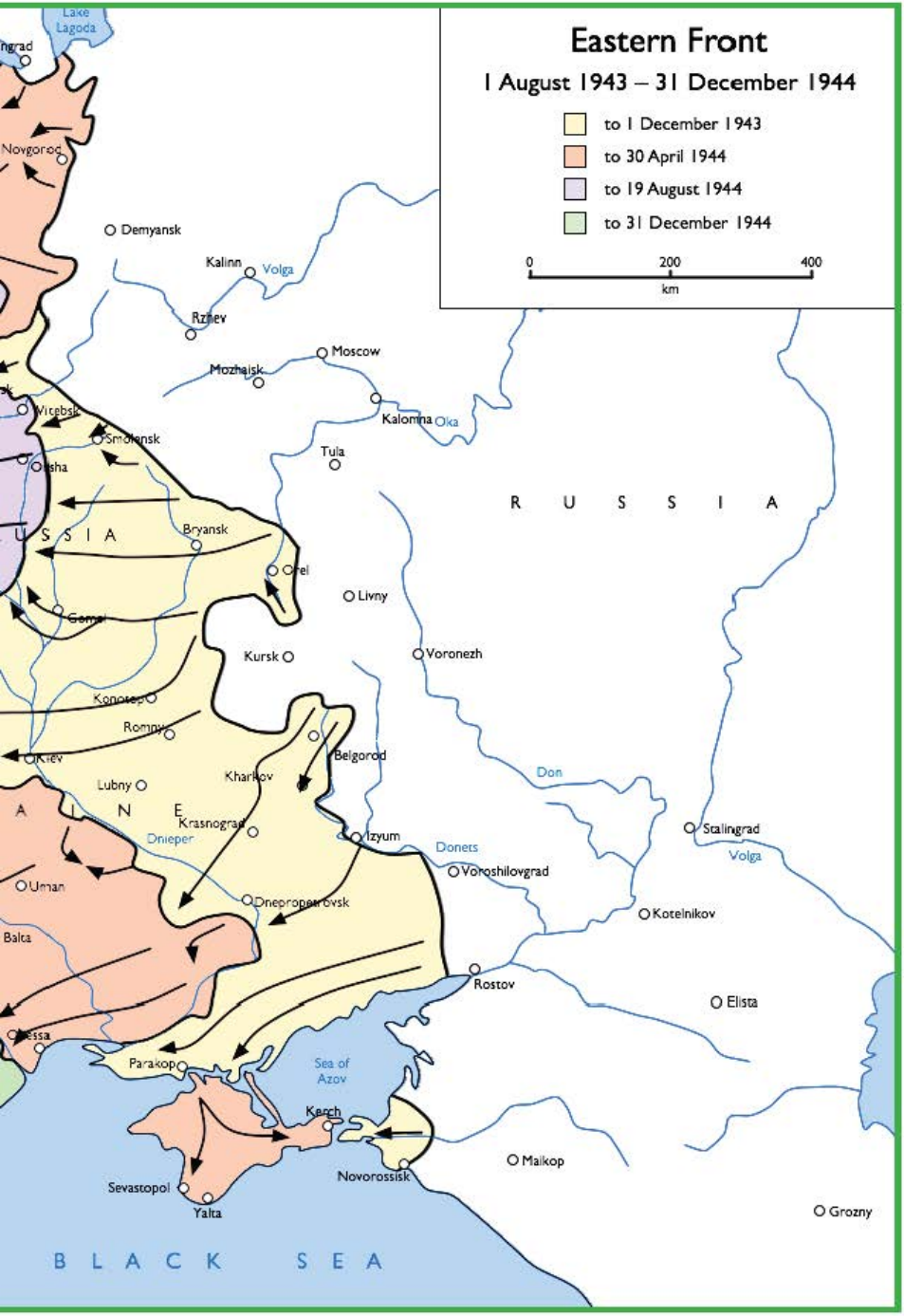
Another source of information accessed by the Germans was obtained by monitoring British exercise activity. A prevailing assumption was that the way a military unit exercises indicates how it will fight. The Germans copied communications associated with British amphibious landing exercises and determined what the British were planning. The information gleaned included the size of the proposed landing area, the number of units the British would commit in the initial assault, and how deep they planned to penetrate on the first day.[31]

The Germans used T/A to provide tactical information to their troops in France after D-Day in Normandy. They identified and located many American units including the 1st U.S. Army with four corps and fifteen divisions, the VIII Corps, the 101st and 82nd Airborne Divisions, and the 90th Infantry Division. Further, the Germans followed the movement of the U.S. XIX Corps, predicting that the Corps would attack in the identified location. The Germans took actions based on this information and significantly slowed the American advances.[32]

Also in Normandy, German troops received information from communications sources that warned them of Allied bombing runs. The Germans intercepted British requests for air support and were able to determine areas/targets and times of the planned strikes. Consequently the Germans were often able to move their units away from the target areas with a great saving of lives and equipment.[33]

Early in WWII German field commanders did not hold T/A in high regard, but as the war pressed on they considered it their best source of intelligence information. For instance, the G2 of the 40 Panzer stated, in referring to the usefulness of the T/A product, the corps "always knew almost exactly the enemy situation, location and strength. This knowledge contributed considerably to the complete annihilation of the Popoff armored army." Other commanders stated that T/A was "the most important means for clarifying the enemy picture," "the most important of the sources," and "the most copious and the best source of intelligence." [34]


Illustration 16. German campaign on the Eastern Front
Leningrad
Stockholm
SWEDEN
Tallinn
ESTONIA
Novgorod
Gulf of Riga
Riga
LATVIA
Copenhagen
BALTIC
LITHUANIA
Dvina
Rostock
Königsberg
Tilsit
Kaunas
Vilna
Danzig
EAST PRUSSIA
Stettin
Niemen
Minsk
Berlin
Poznan
Vistula
Białystok
GERMANY
Warsaw
Brest
Pripet
Dresden
Oder
Breslau
POLAND
Elbe
Prague
Lublin
Krakow
Lvov
CZECHOSLOVAKIA
Vienna
AUSTRIA
Budapest
HUNGARY
Szeged
Zagreb
YUGOSLAVIA
RUMANIA
Belgrade
Ploesti
Bucharest
Sarajevo
Danube
ADRIATIC
BULGARIA


Eastern Front
1 August 1943 – 31 December 1944
to 1 December 1943
to 30 April 1944
to 19 August 1944
to 31 December 1944
0
200
400
km
Lake Lagoda
Novgorod
Demyansk
Kalinin
Volga
Rzhev
Moscow
Mozhaisk
Vitebsk
Smolensk
Kalomna
Oka
Tula
Orsha
R U S S I A
Bryansk
Orel
Livny
Gomel
Kursk
Voronezh
Konotop
Romny
Kiev
Belgorod
Don
Lubny
Kharkov
Krasnograd
Dnieper
Izyum
Donets
Voroshilovgrad
Stalingrad
Volga
Uman
Dnepropetrovsk
Kotelnikov
Balta
Rostov
Elista
Parakop
Sea of Azov
Kerch
Maikop
Novorossisk
Sevastopol
Yalta
Grozny
B L A C K S E A

Operation QUICKSILVER: Deception Covering the Landing in Normandy

One great challenge of WWII was keeping secret the planned Allied landing sites in Europe. Hitler and the Germans, for a number of reasons, had a firm belief that the location of the landing would be on the French coast at Pas-de-Calais, the shortest distance across the English Channel. The Allies prepared a scheme, called FORTITUDE, to convince the Germans that they were accurate in their belief that Pas-de-Calais was the location and, further, to lead them into believing that the real landing in Normandy was merely a diversion. The scheme was so successful that the Germans believed Pas-de-Calais was to be the main landing place even after the Normandy landings began, still convinced that Normandy was a diversionary move.

A variety of actions in the plan were taken to trick the Germans into keeping their forces where they were and not moving them to Normandy. Most of the German units causing Allies concern were near Pas-de-Calais, but some were as far north as Norway. Although the overall plan was called FORTITUDE, the deception aspect was called QUICKSILVER, and it had subsets for each aspect of the plan. Some of these actions included:

- Stationing ground units, later intended for deployment to Normandy, across from Pas-de-Calais
- Developing fictitious military units and "stationing" them in various parts of the British Isles
- Bombing German units in the Pas-de-Calais area
- Placing dummy gliders, tanks, and trucks along the coast
- Maintaining offensive submarine activity as far north as Norway
- Concentrating shipping and landing craft activity in northern harbors
- Use of double agents to convey false information

"The most important of the deception measures, however, was wireless."[35] The wireless part of the plan was called QUICKSILVER

II, and it entailed establishing and operating a realistic communications structure to service the fictitious units. Further, the communications activity would appear to "support" the preparations for a major invasion at Calais. This posed a daunting challenge since the Germans relied heavily upon T/A and were very competent practitioners of the art. With this background, the Germans might very well have been able to detect the ruse if it were not executed convincingly.

The task of implementing the plan was given to the U.S. Army. In one instance the Army set up a simulation of the HQ 1st U.S. Army Group in England when, in fact, that unit was moving to France under the guise of the 12th Army Group. The 1st U.S. Army Group was shown as consisting of the fictitious 14th U.S. Army and the real 4th British Army in a fictitious location.[36] The Germans believed they still faced a formidable force across the Channel from Pas-de-Calais.

In other diversionary actions, General Patton, whom the Germans believed would lead the invasion, was stationed across the English Channel from Calais. Patton addressed ladies' luncheons and other public gatherings to affirm his presence in that area. He is said to have described his actions as "playing Sarah Bernhardt" (a great actress of the time). In another move, Patton had met an old acquaintance, General James Gavin, in a London hotel, and upon leaving a large crowded room he stopped, turned around and shouted to Gavin, "I'll see you in Calais." Most in the room were horrified with this breach of security when, in fact, it was part of the ruse, and Patton took some personal delight in acting that he was carelessly revealing too much.[37]

Korean War

Air Force

Intercepts of Soviet-built MiG fighter aircraft radio traffic confirmed the long-held suspicion that Russians were controlling the air defense of North Korea and Manchuria, not the Chinese or the North Koreans: "…we were actually monitoring the Soviet Air Force fighting the American Air Force, and we were listening to the Soviet pilots being directed by Soviet ground controllers to fight American pilots. We were fighting our own little war with the Soviets."[38] That information, from

Illustration 17. MiG Alley in North Korea

pilots' and ground controllers' plain language conversations and T/A on callsigns and procedures, gave the policy makers firm information upon which to make a decision of enormous proportions—whether to confront the Soviets with a distinct possibility of starting WWIII or to let the respective air forces continue the fighting under false pretenses. Obviously the U.S. policy makers chose the latter course of action.

Vietnam War

Army—Infiltration from North to South Vietnam, 1964-1973

One of the great controversies during the Vietnam war involved the number of communist troops infiltrating into South Vietnam from the North. As early as 1964 there was a wide and strident dif-

ference of opinion between Military Assistance Command, Vietnam (MACV), in Saigon and the Joint Chiefs of Staff in Washington. At that time Saigon wanted to prove that the war was being won and proceeded to "prove" that the threat from North Vietnam was being met by inflicting casualties. Headquarters in Washington, however, stated that the number of enemy troops coming south was much greater than MACV was estimating. Another point of major disagreement was whether the troops coming south were only South Vietnamese repatriates or regular North Vietnamese troops.

As the controversy continued in 1964, T/A with RDF provided significant information. Traffic analysts were studying some communications from the People's Army of Vietnam (PAVN) and followed the transit of their 325th Division from southern North Vietnam into the northern highlands of South Vietnam. This arrival of a regular infantry division represented a major escalation in the North Vietnamese involvement in the south, a development many military and political factions found hard to accept.

Another less precise yet important contribution of T/A to the infiltration dilemma was derived by assessing the volume of messages on a civil network in North Vietnam used by new recruits to send messages home as they left for the trek south. It had been determined that it took about four months for a soldier to make the trip from north to south. When the volume of messages surged in the north, arrival of more troops in the south could be anticipated within four months.

The big breakthrough in the production of SIGINT on this target came in late 1967/early 1968 when analysts gained access to low-powered North Vietnamese communications serving their General Directorate of Rear Services (GDRS). The GDRS was responsible for managing a system designed to move troops and materials out of North Vietnam and, either through the demilitarized zone (DMZ) or through Laos, into South Vietnam. The move south went through a number of way stations, known as Trams, which normally were located a day's walk from each other. These Trams often were run by families, but they had radios and did communicate. Messages from the Trams had four-digit indicators. The first digit identified the

individual's destination in South Vietnam, and the next three digits identified the soldier's unit. These texts contained information on the size of the units moving on the trail, the ratio of officers to enlisted, the need for fuel, numbers of sick and wounded, etc. This information essentially resolved the dispute between MACV and Washington on the subject of the numbers and timing of troop movements to South Vietnam.[39]

The Battle of Dak To

In October of 1967 the 330th Radio Research Battalion was located on a hill in Vietnam's western highlands. The unit, protected by sandbags, barbed wire, and watch towers, was listening to Vietnamese transmitters in the immediate area. At the time the Army personnel manning the station had a sense of foreboding based mainly on the "feel" of recent Communist radio activity but without definable evidence.

A civilian from NSA had just arrived at the unit to support its efforts. When he arrived at the location, he found a group of bright dedicated soldiers working diligently 24/7 under extremely challenging physical circumstances. The target was difficult; the Communists used daily changing callsigns, frequencies, and schedules. Further, they were using low-power transmitters, making intercept difficult.

A chat with the chief traffic analyst was the first step in developing a broad assessment of the situation. The first observation was that "the whole ball of wax was coming apart." Specifically a new North Vietnamese command station appeared which talked to Hanoi, was more active than anyone else around, contacted the highest North Vietnamese echelon in South Vietnam, operated at night when other Vietnamese transmitters were down, and had just moved 77 kilometers to a new location. Then the 330th unit's chief linguist stated that many Communist elements were moving and realigning with other elements throughout the area. All of this activity indicated that an attack was in the offing, but one key element still was missing: the Vietnamese Communists had not given any indications that they had reconnoitered the area—normally a prerequisite to an attack.

Illustration 18. U.S. troops fighting near Dak To, South Vietnam

Throughout October, message activity showed that the North Vietnamese 1st Division was preparing for urgent operations, and they expressed concern that their activities would be detected by the U.S. Then on 23 October the missing piece fell into place; the expected North Vietnamese precombat reconnaissance had begun, indicating preparations for an attack. Based on the frequencies, callsigns, schedules, and a direction finding location of the North Vietnamese Military Intelligence link, U.S. analysts determined the attack would be somewhere in the Dak To area.

Further details followed quickly. On 25 October the 32nd Regiment was located in the Dak To area after having traveled 100 kilometers. On 27 October the 66th moved there, and on 30 October the 174th arrived. Translations of clear text messages also yielded useful information including instructions on conducting reconnaissance

and the details of a new simplified signals plan. The North Vietnamese regularly instituted a new simplified signals plan just before beginning combat operations. Then one Vietnamese unit advised a subordinate to maintain secrecy before it was time to strike.

A report was issued by the 330th based upon all of the information it had gathered. In summary, the report advised that a major tactical thrust was in the offing, probably between 30 October and 4 November with the target in the Dak To area.

Additional evidence came in on the day after the report was issued. An unmistakable pattern of communications was observed. Division headquarters established communications with combat units, reconnaissance began, combat units took positions, the simplified communications plan was instituted, and a tactical command post took control of combat units.

Based on the reports, U.S. forces took immediate action and disrupted the North Vietnamese execution of significant portions of their plan. B-57 air strikes were launched, and two U.S. battalions landed on two strategic hilltop positions. The battle of Dak To continued through late November and proved to be one of the largest battles of the war, but the U.S. had gained an important tactical advantage by disrupting the Vietnamese plan of attack. The overall North Vietnamese objective of this campaign was the destruction of two U. S. brigades. Although the fighting was fierce, their objective was denied. [40]

Air Force—Raid on Son Tay Prison

A number of U.S. Air Force, Marine, and Navy pilots were shot down during bombing raids and fighter combat in Vietnam. Many were captured and imprisoned in North Vietnam, some at a camp named Son Tay, located twenty miles northwest of Hanoi. With assurance that prisoners were being held at this camp, planning began in April 1970 to mount an operation to free the prisoners.

Preparations for SIGINT support to this raid began in August 1970. Brigadier General Manor, commander of the operation,

Illustration 19. Mock-Up of Son Tay Prison, North Vietnam

requested information to aid a safe incursion of low-flying helicopters from Tahkli Air Base in Thailand to Son Tay and their egress. General Manor also wanted all information indicating a possible capability of the North Vietnamese to interfere with the operation. Analysts concluded that, if the raiders used the proposed route and did it at night, the North Vietnamese would have no capability to interfere.

SIGINT not only provided a key input to planning the raid but also provided critical information during the incursion. Extraordinary measures were taken to ensure that all collection and analytic assets were employed. Further, special rapid communications were set up to pass the information to those running the operation and to those in the Pentagon overseeing the activity. The select group in the Pentagon convened in the National Military Command Center and

included the secretary of defense, the chairman of the Joint Chiefs of Staff, and selected four and three-star generals. The NSA representative to the Pentagon also was there.

During the course of the raid the NSA Representative was briefing this group on the support being provided by SIGINT. Then an incident occurred illustrating just how important negative information can be. An officer entered the room and announced that General Manor had declared a MiG alert, indicating that North Vietnamese fighter aircraft could be threatening the operation. Everyone turned to the NSA Representative, who had just assured the group that there was no MiG threat. He based his judgment on analysis that had identified all night-qualified North Vietnamese pilots, where they were spending the night, and the absence of any activity from those airfields. Further, he had the best communications connections with the field, and he stayed with his position, reiterating "No MiGs". After a few more tense moments in the room, a courier entered the room with the news, "Cancel MiG alert".

Although the mission itself was well planned and executed and the SIGINT support to the military operation was excellent, tragically the mission failed, as the prisoners had been moved, undetected by U.S intelligence. There is some speculation that a Caucasian journalist had visited the camp a month earlier. This might have led the North Vietnamese to remove the prisoners from that location as a precautionary measure.[41]

The Cold War

The Early Stages

On Friday, 29 October 1948 (known by cryptologists as Black Friday), the Soviets executed a massive change of their code and cipher systems and communications procedures with devastating effect upon the U.S. efforts to produce COMINT. "Out of this devastation, Russian plaintext communications emerged as the principal source of intelligence on our primary Cold War adversary."[42] Outside of plaintext, one of the only other sources of information was T/A.[43]

That was the environment within which traffic analysts worked during the Cold War. With cryptanalysis being in a posture much reduced from the days of Enigma during WWII, T/A and plain language texts gained a more prominent role.

The Cold War presented a wide range of challenges for intelligence and in turn T/A. Foremost were the major "wars," the "police action" in Korea, and the Vietnam War (see above). In addition to these "wars," there was a series of crises, varying widely in nature. The Cuban missile crisis obviously was the most serious and best known. Other crises occurred in Eastern Europe and the Middle East, as well as those stemming from attacks on U.S. assets.

The Eastern European Satellites

The Soviets declared the Baltic states part of the Soviet Union, but most of the remaining countries of Eastern Europe were considered independent countries, albeit run by puppet regimes subservient to Moscow. They were known as Soviet Eastern European satellites.

The Soviets imposed their will on these countries but with great difficulty. The people never did embrace Soviet rule and repeatedly rose in opposition to the oppression.

Poland 1956

One major reaction against the Soviets occurred in Poland in 1956. Earlier, in 1953, the East Germans had rioted against the Communist regime, but those riots were suppressed without Soviet intervention. The label given to this Polish uprising was "The Poznan Riots." The set of challenges for intelligence was threefold: determine the nature of the uprising, report on the reaction of the Polish government, and observe the Soviets' response to the whole situation.

The Poznan Riots were relatively limited. Polish workers in Poznan rioted against the strict Communist regime, and the Polish Army stemmed the revolt but with significant loss of life. As a result, however, the Polish Communist Party did install a new president, who was a counterrevolutionary and bent upon reform. T/A and related information indicated that the Soviets were preparing to

Illustration 20. Soviet-dominated Eastern Europe

use force to oust the new president, Gomulka, but he hastily advised the Soviets that the political and military ties with Russia would be maintained. The Russians called off their troops.[44]

Hungary 1956

As the crisis in Poland was waning, on October 23, 1956, peaceful demonstrations in Budapest against the hard-line Hungarian Communist government turned violent. Whereas the uprisings in

East Germany in 1953 and in Poland in 1956 were riots, the Hungarian affair turned into a full-blown revolution. There were two distinct differences between this revolt and the earlier Polish riots. First, many Hungarian national military units sided with the rioters, providing a formidable albeit relatively small force contesting the Soviets. Second, Hungary has a border with a noncommunist state, Austria. These two factors increased the possibility of NATO and U.S. intervention or at least the provision of some assistance to the rebels. These factors made the need for good timely intelligence much more urgent.

Although there were human and open source assets producing information on the progress of the revolution, the information consisted mainly of descriptions of rioting in the streets in major towns. Understanding just what the Russian forces were up to and what the Hungarian military was doing, was based on T/A and low-level plain text transmissions as the Soviet high-grade cipher traffic remained unreadable.[45]

The riots started in Budapest but quickly spread to all major cities in Hungary. The Soviets had four divisions in Hungary, and they moved them rapidly to Budapest where they met fierce resistance from both the general populace and from many units of the Hungarian armed forces. The Soviets took significant casualties, but within a week they realigned their units within Hungary and moved in reinforcements from the western USSR. Intelligence, mainly derived from T/A, enabled analysts to follow the movement of Soviet units and the reactions within the Hungarian armed forces.[46]

Meanwhile thousands of Hungarian citizens took advantage of the drastically reduced security along the Austrian border to make their break for freedom. The flow continued for a few days until the Soviets regained control over all of the Hungarian armed forces and reestablished border security.

Czechoslovakia 1968

Each of the disturbances in the Soviet European satellites had its own defining characteristics. In Czechoslovakia, Alexander Dubček was elected president early in 1968. In short order he fired many of

the Communist hard-liners and started to institute social reforms, to the consternation of the Soviets. In response, Moscow started to muster its military forces and those of adjacent Communist satellite nations. "Within days of Dubček taking power, SIGINT detected the movement of eight Soviet combat divisions from their barracks in East Germany, Poland and the western districts of the Soviet Union to points around the periphery of Czechoslovakia. By the end of June, SIGINT and satellite reconnaissance revealed that the Soviets now had thirty-four combat divisions deployed along the Czech border, and that the Soviets were rapidly moving hundreds of combat aircraft to airfields within striking distance of targets inside Czechoslovakia."[47] The Soviet invasion started on August 20, 1968, and within days they were in control of the country. T/A provided most of the information on the military deployments.

Summary

Traffic analysis is an integral part of the broader category of signals intelligence. Although not as well known as cryptanalysis, it has been a major source of intelligence information over the years, and it has been employed against communications from at least as early as the American Civil War. This paper describes the elements of traffic analysis and offers examples of its contributions starting with WWI and through the intervening period until the end of the Cold War. The discipline undoubtedly will continue to be useful in the future regardless of the changing nature of communications. It is the hope of the authors that someone eventually will describe the changing nature of the discipline and present instances of its use in post-Cold War scenarios.

Acknowledgments

The authors are grateful for the contributions of a variety of experts and wish to convey their thanks to those people. Pertinent substantive inputs were offered by Dr. James Boone, Raymond Schmidt, and William Fromm, and they improved the document significantly. The brochure benefited from the editorial skills of Jenny Brown, and the guidance and research assistance of Rene Stein was outstanding. Useful comments were submitted by MG Thomas Flynn and Wayne

Stoffel. The team also benefited from the advice and counsel offered by Dr. David Hatch, Elizabeth Smoot, Barry Carleen, Lula Greenwood, Jennie Reinhardt, and others. We thank you all.

Notes

1. The term SIGINT (signals intelligence) includes three subordinate sources of information: COMINT (communications intelligence), ELINT (electronic intelligence), and FIS (foreign instrumentation signals). The function of radio direction finding (RDF) normally is included within the discipline of COMINT but is applicable in the other areas as well.

   While ELINT was collected and analyzed during WWII, the term SIGINT did not come into the lexicon until after the end of the war, and COMINT was known as "radio intelligence" until the middle of the 20th century. Traffic analysis (T/A) and cryptanalysis (C/A) were the two major components of COMINT, although exploitation of plaintext intercept, POW interrogations, captured documentation, open source publications (maps, transportation schedules) and the like were often helpful to both traffic analysts and cryptanalysts.

2. The authors of this brochure were engaged in traffic analysis during some portions of their careers in signals intelligence involving the various war periods listed subsequent to World War I. To facilitate the production of intelligence, NSA in 1965 formalized the technical career specialties such as T/A and C/A by establishing career panels to oversee training of personnel and their attainment of "professional" status. These panels developed specific training criteria, intern programs, rotating assignments, and formal examinations. Upon completion of the courses of study, an individual was certified as a professional in a specific field.

3. William Fromm, December 2012.

4. Raymond Schmidt, informal notes, January 2013.

5. F. H. Hinsley, *British Intelligence in the Second World War, Vol. I* (London: Stationery Office Books, 1988), 21.

6. John Ferris, *The British Army and Signals Intelligence During the First World War,* Alan Sutton for the Army Records Society (1992), 3.

7. Terrence J. Finnegan, Col. USAFR (Ret.), "Military Intelligence at the Front, 1914-1918," *Studies in Intelligence* 53, no. 4 (December 2009): 25-40.

8. William F. Friedman, *Solving German Codes in World War I* (Walnut Creek, CA: Aegean Park Press, 1979), 92.

9. Ibid., 12-16.

10. E. Alexander Powell, *The Army Behind the Army* (New York: Charles Scribner's Sons, 1919), 21.

11. Ibid., 13.

12. Ferris, 21.

13. This incident is described in detail in Christopher Andrew, *Her Majesty's Secret Service: The Making of the British Intelligence Community* (New York: Viking, 1986), 102-106; see also R. E. & T. N. Dupuy, eds., *The Encyclopedia of Military History From 3500 B.C. to the Present*, 1993, 1964, for warning to Jellicoe and Beatty of the sortie of the German High Seas Fleet on 30 May, based on "imprudent German radio chatter".

14. E. B. Porter, *Nimitz* (Annapolis, MD: Naval Institute Press, 1976), 69, 88, and Roland Lewin, *The American Magic* (Penguin Books, 1984), 93.

15. Lewin, 144, 155, 165, 166.

16. Porter, 179.

17. Sharon Maneki, *The Quiet Heroes of the Southwest Pacific Theater: An Oral History of the Men and Women of CBB and FRUMEL*, NSA Center for Cryptologic History (1996), Preface.

18. Kathleen Broome Williams, *Secret Weapon: U.S. High-Frequency Direction Finding in the Battle of the Atlantic* (Annapolis, MD: Naval Institute Press, 1996), 23.

19. Third Army Radio Intelligence History in the Campaign of Western Europe, Signals Intelligence Service of Headquarters Third U. S. Army (Undated [18 Sept. 1945]), 1.

20. Ibid., 11.

21. Ibid., 32.

22. Ibid., 41.

23. Ibid., 47, 48.

24. Hinsley, 53.

25. Ibid., 141.

26. Stephen Budiansky, *Battle of Wits: The Complete Story of Codebreaking in World War II* (New York: Touchstone, 2000), 46-49.

27. David Kahn, *Hitler's Spies: German Military Intelligence in World War II* (New York: Macmillan, 1978), 189-212.

28. Ibid., 200.

29. Ibid., 189.

30. Ibid., 203.

31. Ibid., 204.

32. Ibid., 207.

33. Ibid., 208.

34. Ibid., 210.

35. Albert Norman, *Operation Overlord, Design and Reality: The Allied Invasion of Western Europe* (Westport, CT: Greenwood Press, 1970), 127.

36. Ibid., 128.

37. William B. Breuer, *Hoodwinking Hitler: The Normandy Deception* (Westport, CT: Praeger Publishers, 1993), 113, 159-160.

38. Matthew M. Aid, *The Secret Sentry* (New York: Bloomsbury Press, 2009), 35.

39. From lecture delivered by Walter J. Abbott, NSA History Symposium, October 2009.

40. Sharon Maneki, *Proud and Bitter Memories: Personal Reflections of the Vietnam War*, NSA Center for Cryptologic History (2006), 37-42.

41. Thomas R. Johnson, *American Cryptology During the Cold War, 1945-1989,* NSA Center for Cryptologic History, 1995, Book 2, "Centralization Wins, 1960-1972" (1995), 576-578.

42. Jeannette Williams and Yolande Dickerson, *The Invisible Cryptologists: African-Americans, WWII to 1956*, NSA Center for Cryptologic History (2001), 19.

43. Matthew M. Aid, 21.

44. Ibid., 47.

45. Ibid., 47

46. Ibid., 49.

47. Ibid., 143.

Illustrations

Illustrations are from Wikimedia Commons unless otherwise noted.

Donald A. Borrmann attended the University of Michigan and in 1943, from the Army ROTC unit there, he was called to active duty as a second lieutenant in the Army Signal corps. He was assigned to the Army Security Agency; his tours included India, the China/Burma/India Theater, and the Philippines. In China, immediately after the Japanese surrender, he was assigned to TICOM duties, an effort to obtain codes, cipher machines, and information on "enemy" communications; he was present at the surrender of the Japanese 23rd Army. He continued his SIGINT career as a civilian, mostly with NSA. He served in London and Oslo, was assigned to the Office of Special Operations in the Office of the Secretary of Defense, and was the NSA representative on the first Intelligence Community Coordination Staff under the Director of Central Intelligence, Allen Dulles. Mr. Borrmann had several high-level managerial assignments at NSA and in 1965, when the agency formally established its technical career specialties, he began a seven-year term as the first chairman of the Traffic Analysis Career Panel as an additional duty. He retired from the agency in 1980.

William A. Kvetkas served at NSA for twenty-four years, two as a lieutenant in the U.S. Air Force and twenty-two as a civilian, during which time he was chief, U.S. Intelligence Board Branch, an assistant inspector general, chief of an analytic office, and chief, Office of Programs and Budget. He also served in Frankfurt, Germany. He joined CIA in 1976 and served as comptroller of the U.S. intelligence community and director, Program and Budget Office, Intelligence Community Staff. From 1979 to 1983, he was chairman, DCI SIGINT Committee. He was the recipient of NSA's Exceptional Civilian Service Award and the National Intelligence Distinguished Service Medal in 1980 and 1983. He was a deputy vice-president from 1991 to 1994 at Lockheed Missiles and Space and chairman of

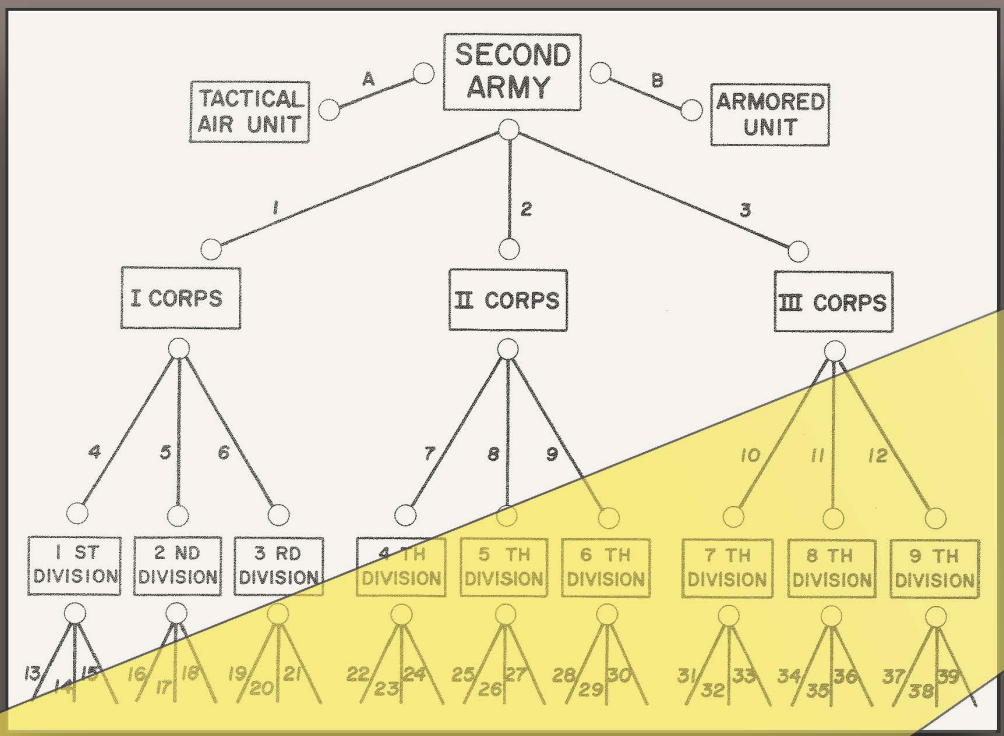
the board of the Association of Former Intelligence Officers 1997–2000. Mr. Kvetkas received a B.S. from Wharton School, University of Pennsylvania; a master's degree from George Washington University; and a law degree from Georgetown University. He is also a graduate of the National War College, the Federal Executive Institute, and the Harvard University Executive Program in National and International Security. He is a member of the DC Bar and is a CPA.

Charles V. Brown received an ROTC commission as a second lieutenant in the USAF upon his graduation from Ohio Wesleyan University in 1958. After receiving Air Force intelligence training at Sheppard AFB, he spent eleven years in the USAF with two tours at NSA, one at Shaw AFB, three years in Germany, and one year in Vietnam. In 1972 he converted to civilian status at NSA where he had operational and staff assignments in DDO, R/D, the National Cryptologic School, and the EEO Office. He retired from the USAF Reserve as a colonel in 1988 and from NSA in 1992. He returned to NSA full time from 2003-2005 to support the buildup for the Second Persian Gulf War. Later in 2005 he became a civilian volunteer in the Center for Cryptologic History until 2013 when he moved to Williamsburg, VA. He has an MA in international studies from American University and after retirement was active in supporting federal/state/local counternarcotics efforts. He was a noted clarinetist and author in the Dixieland jazz circles in the Baltimore/Washington area.

Michael J. Flatley joined the USAF in 1957 after finishing high school. He studied traffic analysis and was assigned to Shiroi AB in Japan, Okinawa, and then NSA at Ft. Meade where he converted to civilian status in 1961. He served as a traffic analyst and as a special research analyst in several

operations organizations after which he took a three year tour at an overseas SIGINT processing center. He went to Vietnam in 1967 where he served with the USAF 7th Air Force in Saigon. Upon his return to NSA, he was given middle management and staff level assignments until his retirement in 1994. Mr. Flatley had studied at the University of Maryland. Subsequent to his retirement from NSA, he worked on a project to supply intelligence information in support of federal/state/local counternarcotics efforts in the war on drugs.

Robert Hunt joined NSA after a tour of duty in the Philippines with the USAFSS and completion of a BA in history at the University of Maryland. He spent 25 years in Operations as a linguist, traffic analyst, cryptologist, staff assistant, and manager. He traveled extensively on TDY assignments and was stationed for four years in Germany. Receiving an agency fellowship, he completed his Master's degree at American University in intelligence research/lnternational relations and finished the coursework toward a doctorate. At the end of his agency career, he served as the deputy dean of a department in the National Cryptologic School, helping to develop and expand the instruction of cryptologic training in analysis and reporting, and computer-assisted training. After retiring in 1992, with 36 years of govemment service, he currently helps out as a staff assistant with the National Cryptologic Museum Foundation.


SECOND ARMY
A
B
TACTICAL AIR UNIT
ARMORED UNIT
1
2
3
I CORPS
II CORPS
III CORPS
4
5
6
7
8
9
10
11
12
1 ST DIVISION
2 ND DIVISION
3 RD DIVISION
4 TH DIVISION
5 TH DIVISION
6 TH DIVISION
7 TH DIVISION
8 TH DIVISION
9 TH DIVISION
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA