



Approved for Release by NSA on 09-27-2007, FOIA Case # 51633

(b) (3) - P.L. 86-36

Fabrication of Traffic—It Can and Did Happen

Can a radio-intercept operator fabricate traffic so effectively that he can fool experts? Can he create texts that are believable and go unnoticed—or at least be accepted—by linguists and analysts? Can he do this in a dozen or more instances without being observed or questioned at the site, or at higher echelons in the field? Can he fool an investigating team into believing he engaged in no wrongdoing when the traffic comes under scrutiny and question?

Yes, he can. And an operator did just that during the Vietnam war. He fabricated at least 17 messages—making up the texts, translating them into Vietnamese before encrypting them, and passing them to the local processors and to NSA as valid traffic. And he was successful for awhile, even fooling an investigating team when the traffic first came under suspicion. But the dogged determination of a group of experts proved to be his undoing.

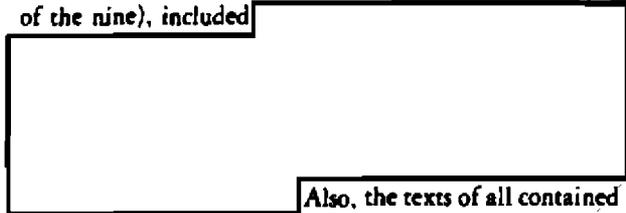
First Suspicions

Early in January 1969, nine messages intercepted in Vietnam attracted the attention of NSA analysts and linguists because they contained linguistic and textual peculiarities, inconsistencies, and inaccuracies to such a degree as to be suspect. Although some of the messages were intercepted as early as 18 December 1968, the

The authors wish to acknowledge the professional and technical assistance of Mr. Donald B. Oliver (V1) and Mr. Norman Wild (B4), who reviewed the article and made substantial contributions.

conclusions that they were suspect were not drawn until mid-January for a number of reasons, in particular because much of the traffic itself did not arrive on the desks of NSA analysts until shortly before that time. Also, analysts at NSA, and in the field as well, would not be expected to assume at first glance that the traffic coming their way would be fabricated; rather, they would be inclined to give the traffic a presumption of innocence, so the fabricator could—and in this case did—"win" the first round.

These suspicious versions were rife with irregularities, both in their formats and in the texts, and, indeed, in the varieties of the peculiarities themselves. Some, for example, were ostensibly passed on communications links that could not be identified as being valid. Others (eight of the nine), included



Also, the texts of all contained

The operator who actually fabricated the traffic was offered immunity from prosecution (1) to entice him to reveal all he knew about the matter, (2) to determine that he indeed worked alone, and (3) to help in identifying all bogus traffic. Consequently, subsequent revelations and admissions of wrongdoing did not result in court-martial, nor in any other kind of formal punishment. The operator involved, therefore, and others peripherally involved in one way or another, will not be referred to by name in the narrative. Nor is it considered pertinent or necessary to mention his branch or service—or locations or names of sites involved. Their mention would serve no useful purpose.

incorrect grammar, such as misplaced adjectives, and little known, archaic, or "dictionary only" words and phrases. And their word order appeared "to be more like English than Vietnamese."

Alerted by these problems, specialists at NSA quickly noted other peculiarities which were not part of the traffic itself; but which were equally suspicious. All messages, for example, were copied at a particular site in Vietnam; no other facilities anywhere in the theater—ground or airborne—had intercepted them. Wideband tapes were closely examined to determine if the transmissions might have been captured thereon. They were not. Additionally, all were copied by the same intercept operator, except for some which could not be equated to any operator, for they carried no personal operator identification (a factor that in itself was "unusual"). Nor did daily airborne or ground-based DF reflect any of the activity in question.

On the basis of these suspicions, fabrication of traffic was a strong probability, and the Director, NSA, was informed. He immediately took steps to investigate and resolve the matter. He notified the parent SCA in detail and requested an immediate investigation. He also initiated actions to insure, among other things, that no erroneous Comint might be in the hands of users, or if some had been published on the basis of this traffic, that recipients were cautioned accordingly until the matter could be fully investigated and resolved. In this regard, translations or reports that had been issued, in whole or part on the basis of these intercepts—by either the field or NSA—were isolated as quickly as possible, and identified to recipients as being questionable. (Later, after an initial investigation did not resolve the matter to his satisfaction, the Director ordered that the questionable product be cancelled.) At the same time, the field was alerted to be especially watchful for any additional intercepts that contained any of these peculiarities, and the Director ordered that NSA be notified immediately if any showed up. Also, he directed that, where practicable, field publication of translations of such intercept be delayed pending official Agency approval. And, as the matter evolved, the Director briefed the USIB concerning its progress and findings.

Initial Investigation

On 24 January 1969, a "preliminary" field investigation began. It was completed by 30 January. Its purpose was to determine the facts pertaining to the origin and validity of the messages involved, and to report results to appropriate authorities. A three-man board, whose members were picked from the SCA involved, conducted the investigation.

Fourteen persons were interviewed during the course of the investigation. Those interviewed included the operator himself, his commanding officer, the operations officer, traffic analysts, linguists, other intercept operators, two NSA employees working in the field at that time, and others.

Findings of this investigation, however, did not substantiate the alleged fabrication of traffic, nor did they lend credence to a possibility, suggested by some, that the enemy may have fabricated and transmitted the traffic as a deceptive measure. Also, the investigation did not support the belief, held by some, that the traffic may have been fabricated and sent by U.S. personnel who had access to transmitters. U.S. personnel having access to such radios were thoroughly questioned, and this possibility was discounted.

In particular, the report concluded that the nine messages under question did not, according to the findings of the investigation, contain inconsistencies or deviations from normal practice or patterns to a degree significant enough to warrant their being labeled as fabricated. Although the report noted that they did contain a number of questionable items, which were labeled as "unusual" when compared to traffic "during periods of relatively normal target activity," it concluded that most of these were not without precedent.

Nor were the texts of the messages themselves considered to be suspect. Although the board again concluded that some messages contained little known, archaic, or "dictionary only" words and expressions, as well as questionable items about troop strengths, personalities, use of jet aircraft, and the like, its conclusion was that these irregularities were not the result of concocted items, but, rather, they were "anomalies" originated by the enemy. Or, they were justified, again, by the "abnormal tactical situations at that time."

Other areas offered by analysts and linguists to support their beliefs that the traffic was fabricated were also carefully and minutely examined, and by and large also explained away or discounted during the course of the investigation by the board. For example, the fact that there had been no successful airborne DF of the suspect traffic (or any record of any having been attempted) was explained mainly by the times of intercept—this type of DF coverage having been discontinued because of historic target inactivity during these periods. (Such aircraft, in fact, were available for DF tipoff on only two such

occasions.) The point that the transmissions could not be found on the wideband tapes was also dismissed.

But in another area, ground-based DF, "minimum facilities" were manned during the times in question, and records at the intercept site showed that two schedules had actually been tipped off (though records at the DF site did not substantiate this). This "fact" was cited as evidence that the communications in question were real and not fabricated. (But the operator would later admit that he had rigged this aspect also, by "tipping off" the DF site himself, when actually there were no such target communications active. He did it, of course, in an attempt to further "validate" the bogus traffic.)

Another point, to the effect that intercepts were made when such target communications were usually inactive, was also explored. This, however, was explained by the "fact" that most suspect intercepts were pre-scheduled by the target during periods of normal activity, and these pre-planned schedules were actually consummated at other "odd" times.

Still another area of suspicion was probed by the examining board and also discounted. It concerned



This too, however, was explained by the "fact" that some suspect messages were of the "first-heard variety" and therefore "unique" in themselves. Others were dismissed as apparently "relayed by, rather than originated by," the transmitting entity.

Of all the above questionable items, the linguistic impossibilities were particularly compelling evidence that no native Vietnamese could have drafted such messages. An analogy to prove the point was hypothesized: Were you to observe a text ostensibly written by a native American which read "I have broken my goblets and cannot see," one might suspect the validity of the text even though in one context "goblets" and "glasses" are synonymous.

As far as the operator himself was concerned, he handled himself amazingly well during the investigation, and almost without exception, all others questioned gave him high marks as a conscientious worker. His abilities as an intercept operator also received high marks by peers and superiors alike. They were virtually unanimous in their praise of his outstanding abilities and accomplishments in this regard, and in the operator's dedication to his job, citing, in particular, his willingness to volunteer to work at times other than during his normal duty hours, mainly to intercept the odd-hour (or QRX) schedules previously mentioned. One such effort

in particular, when the operator volunteered to return to work on Christmas Eve to look for a QRX schedule, won special praise from his superiors, and the admiration of his fellow workers (and, as it later turned out, an opportunity for him to fabricate a message). Persons conducting the investigation were also thoroughly impressed with his over-all military credentials and bearing, and with his behavior while being questioned.

Thus, at the conclusion of this initial investigation, most of the peculiarities of the suspect traffic had been explained away or largely discounted to the satisfaction of the examining board, whose final report concluded that the "findings of the investigation do not substantiate the alleged fabrication . . ." Additionally, the report recommended that a product—which had been issued by NSA cautioning users against the validity of translations and reports issued on the basis of information in the suspect messages—be revised accordingly, and that NSA grant authority for the publication of additional products related to the questionable intercepts which were being held up pending results of the investigation.

Subsequent Investigation in Washington

The conclusions of this initial investigation did not, however, change the position of NSA. In fact, while the field investigation was being conducted, NSA continued to investigate the matter independently (with the knowledge of the SCA). As a result of this investigation, and, in his opinion, the inconclusive findings of the field investigation, the Director concluded that the subject messages were invalid, not originated by a Vietnamese, and constituted erroneous Sigint. (Many of the linguistic errors, in fact, could have had only one source—erroneous definitions from a Vietnamese-English dictionary widely used at NSA and in the field.) Consequently, the Director ordered the cancellation of all products which were derived from the suspect messages, noting at the same time that "the guilt or innocence of one or more . . . individuals is immaterial in regard to the validity of the Sigint," and that that matter could be dealt with in subsequent investigations. The Director also noted, in taking this action, that although a number of NSA's traffic analytic findings were "inconclusive and open to judgments, the weight of evidence (particularly linguistic) points conclusively to the fact that the messages are invalid." And in a final note, he proposed to the chief of the SCA that the matter be further investigated jointly, with mutual agreement on location and procedures, and with representatives of NSA present to assist in the resolution of substantive specifics.

(b) (1)
(b) (3) - 50 USC 403
(b) (3) - 18 USC 793
(b) (3) - P.L. 86-36

As a result, it was agreed that the matter would be jointly investigated in Washington, to resolve it one way or the other. It was requested of the parent service that such an investigation be authorized, and that the operator be brought back to participate in it. The services of a polygraph examiner were also requested to assist in the investigation. The parent service concurred in both requests, and the operator, and a linguist who had worked with him in Vietnam, were ordered back to Washington.

Shortly thereafter, the two men arrived in Washington for the investigation. Representatives of NSA and the SCA, and others, questioned them on 24 and 27 March 1969, and both men voluntarily submitted to the polygraph examination on 28 March.

During the session on 24 March, the operator stuck to the story he had used during the earlier investigation in the field. But after this effort, he later claimed he fully realized, for the first time, the seriousness of the matter, and the damage it could have caused the war effort. And after thinking it over that night, he decided to seek medical help. The next day he saw a doctor, who in turn scheduled him for a meeting with a psychiatrist on 26 March. And at the meeting with the psychiatrist, he admitted that "he had collected messages in Vietnam and he realized he falsified some." Shortly thereafter, he went voluntarily to the SCA representatives of the investigating team and stated that he wanted to change his story, writing a brief statement regarding his fabrication of traffic while in Vietnam.

Renewed questioning on the following day by the personnel who had conducted the 24 March interview, and the polygraph itself, were therefore anticlimactic. But they did reveal considerable detail about the matter, and, in the case of the polygraph, confirmed, among other things, that the operator had acted alone, and that the whole scheme was solely his idea from start to finish.

But some items were never explained to the full satisfaction of the persons involved in the investigation. The operator seemed to have difficulty remembering details, and, in fact, exactly how many messages he had fabricated. Nor could he say why he had done it in the first place, other than that he "guessed" to bolster his ego. Other questions were also left unanswered, to one degree or another, not the least of which was why he wasn't observed and questioned at the site, and why, in fact, no one at the site apparently became suspicious of his extracurricular activities—or, with one exception, of the irregularities in the traffic—even though the messages were fabricated in the operations area.

A number of revealing details did result from the investigation, though, showing, among other things, that there were clues available even before the initial

investigation which might have aroused the suspicions of those who worked for and with him.

It was determined, to the maximum extent possible, that the operator had fabricated his first message on 18 November 1968 (although nine unreadable messages that had been "intercepted" earlier in that month by the same operator were also probably fabricated, as NSA claimed and the operator "guessed" to be true). His last bogus message was apparently originated on 25 January, just before the initial investigation began.

In regard to the numbers of messages fabricated, his best recollection was that he had originated as many as 20, perhaps 25, giving as his reason for this belief that he had "copied" about 50 messages during the period under suspicion, and that he believed about half were fabricated. During this detailed questioning on 27 March, it was determined that 17 messages were actually fabricated, not counting the nine unreadable messages of early November. Several additional messages which the operator professed to have fabricated did not, in fact, look unreasonable, even with hindsight, for they were of such routine and stereotyped nature that their authenticity could not be confirmed or refuted, though they had not been seen on wideband. And even if they had been fabricated, as the operator maintained, the nature and brevity of the texts precluded their being injurious.

The operator was able to identify some of the fabricated messages by "flags" he had inserted into them, and others by terms and subject matter in the texts. But he could not explain why he had inserted these flags into the traffic, which would most certainly, and did, attract the attention of analysts and linguists. He could not in most cases justify their use, or explain why he had deviated from normal target procedures in such an obvious manner. (Some of these "odd" procedures he even attributed to "things he believed he had learned at school.") When it was suggested that he consciously or subconsciously added them to insure that he would later be caught, he admitted that this may have been the underlying reason.

Other areas probed were equally enlightening. When asked where he fabricated the messages, he replied that they were done in the operations area, and that he had not been questioned, other than in one instance, about their subject matter. This one exception concerned the troop strength of an enemy organization, which, in the opinion of an officer on duty at the time, was far too high and "couldn't therefore be correct." The operator admitted later that this questioning by the officer made him wary thereafter.

When asked what he needed to fabricate a message, he replied "merely a dictionary and a matrix, and minimum

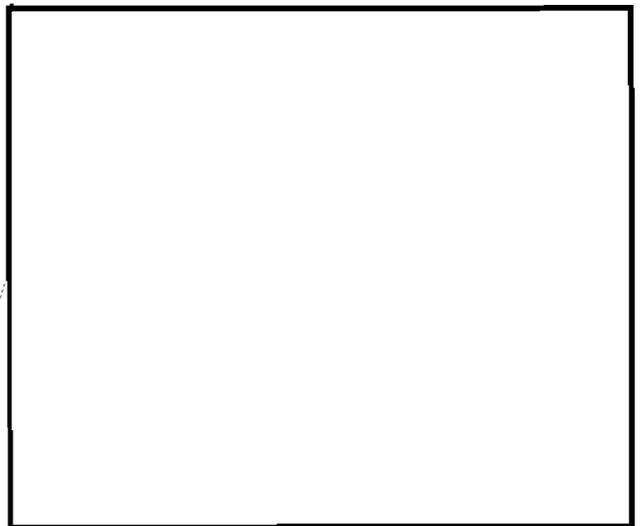
knowledge of the tactical situation." He further stated that, in using the dictionary, "all you would do is go down the English portion and take out a phrase you'd need and work up a message that way." He also claimed that it took between 30 and 40 minutes to make up a message from start to finish. The operator even initiated garbles into the fake messages, and collations to correct them as he normally did in valid traffic, to further "prove" their validity.

Also, in identifying some of the fabricated traffic during the investigation, he noted that "... traffic of the target wasn't as clear ..." as the copy he fabricated, noting in this regard that "you couldn't hear the target clearly," blaming the poor signal quality on inadequate antennas at the site and their less than optimum locations. He also commented that, in retrospect, this very fact "should have been questioned ... for just the clarity alone."

Equally perplexing was the operator's reason for engaging in the effort in the first place. When asked why he did it, he stated that he had difficulty understanding why he had done it. His only reason was that, as noted previously, he believed he had "a fervent desire to excel in his work." He said he had never excelled in anything he had ever done, and he apparently saw this as an opportunity to do so, while at the same time gaining some "glory" for his organization, for contents of the fabricated texts were far above the norm in importance. Apparently he did not realize at first—or admit to realizing—the seriousness of his actions until after the initial investigation began. And from then on he said that he could not force himself to tell the truth until after he was recalled to Washington for further questioning, at which time he "finally realized that he might be in serious trouble."

And with this the case ended, except for some final remarks about the expertise of NSA specialists involved in the matter. The chief of the SCA, for example, noted in a final comment to the Director that "NSA's discovering and development of possible fabrication in the mass of traffic handled is truly extraordinary." And the Director also voiced strong praise of the specialists who had originally uncovered the problem and doggedly stuck to their beliefs throughout, noting in his final report to the USIB:

This fabrication ... involved several cryptologic skills, but the quick action by NSA in detecting the possibility of this material being invalid, and in alerting the intelligence community of this possibility, greatly reduced any danger this hoax might have presented to our troops in the field ... To this I might add that, while this expertise is typical of what I expect from my analysts, it is still reassuring to have this expectation borne out in practice.



(b) (3) - P.L. 86-36