

DIARY

ANNEX N ENCLOSURE 3
TO COMMANDER'S DIARY
SEP 67

CONFIDENTIAL

HQ 104 Sig Sqn
NUI DAT
7 Sep 67

See Distribution List

VC/NVA ELECTRONIC WARFARE CAPABILITY

The contents of this paper relating to enemy action and capabilities have been extracted from a Combined Intelligence Centre Vietnam report ST 67-061 dated 1 Jul 67.

Introduction

1. The VC/NVA have been concerned with electronic warfare throughout the Vietnam conflict, but recently they have intensified their efforts. By taking advantage of breaches in Allied communication security they have been able to gain valuable intelligence data. The VC/NVA have effectively jammed friendly radio transmissions and have developed the ability to enter friendly nets and transmit false information.
2. Recent examples of VC/NVA electronic warfare attempts are:
 - a. Jamming. On 25 Feb 67, 4 Inf Div on Operation SAM HOUSTON had their command net jammed by Russian and oriental voices and march type music. Jamming using music has been reported in recent months by units of 1 ATF.
 - b. Imitative Deception.
 - (1) In Jan 67, III MAF reported six attempts in one week when VC/NVA entered aircraft nets and, speaking English, attempted to misroute strike aircraft.
 - (2) In Feb 67, members of an MACV Advising Team whilst in contact with the enemy requested artillery support from the fire direction centre. As the FDC was preparing the request, they received another call in clear and distinct English for the fire to be shifted. The MACV Team heard this request and on checking found that the new coordinates were their own position.
 - c. Intercept. A platoon leader of a VC anti-aircraft platoon reported that his signal platoon was composed entirely of English speaking personnel who monitored FAC nets daily. When the FAC aircraft called for strike aircraft, VC battalion commanders would be notified.

Equipment

3. As at 10 May 67, it was known that the VC/NVA had the following VHF FM radios in the III Corps area:

CONFIDENTIAL

CONFIDENTIAL

- 2 -

- a. AN/PRC - 9 (27 - 38.9 Mc/s) 3
- b. AN/PRC - 10 (38 - 54.9 Mc/s) 133
- c. AN/PRC - 25 (30 - 75.95 Mc/s) 11
- d. AN/PRC - 6 (47 - 55.4 Mc/s) 13

4. Since the VC/NVA do not rely on VHF radio for communications within regiments and units, it must be assumed that a considerable proportion of the VHF FM radios which they have captured are used for electronic warfare.

Jamming

5. An FM radio has a property known as "capture effect". The strongest signal at the receiver is "captured" and all the weaker signals on that frequency are ignored. Therefore, for jamming to be effective with an FM radio, the jamming signal must be stronger at the receiver than the desired signal.

6. The AN/PRC - 9 and AN/PRC - 10 radios have an output power of 1 watt while an AN/PRC - 25 set has an output power of 1.5 to 2 watts. Other things being equal (such as antennas used, suitability of transmitting sites), an enemy jamming station must be closer to the receiving station than the desired station. Within an infantry battalion or within the Task Force it could be expected that the enemy can achieve this situation without difficulty.

Imitative Deception

7. Imitative deception is a most difficult form of EW. The enemy operator must speak fluently the language used on the net and with an accent appropriate to the station being imitated. He must know the communication procedures used on the net he has entered and he must know the form in which instructions are given.

8. Although the VC/NVA has tried imitative deception on English speaking nets, no examples of success have been reported.

Intercept

9. It is virtually impossible to detect that a radio net is being intercepted. Of all EW techniques, intercept is the most widely used by the VC/NVA.

10. Inadequate knowledge of English is the biggest single factor likely to reduce the VC/NVA effectiveness of their intercept of our radio transmissions. However, the enemy has got English speaking operators some of whom are sufficiently skilled to attempt imitative deception. It must be assumed that there are at all times in our TAOR enemy operators who understand English sufficiently well to enable information extracted from our nets to be exploited.

11. Intercept exploits breaches of communication security. Most radio users are aware of the need to avoid obvious security breaches such as giving overnight locations in clear or discussing movements for the next day in clear. However it is interesting to note that a VC returnee said that intercept had exploited the following:

- a. Conversations between officers of different units.
- b. Discussions in clear about a preceding message which resulted in a decrypting difficulty.

CONFIDENTIAL

CONFIDENTIAL

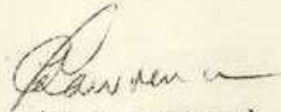
- 3 -

- c. Answering questions about information previously encrypted.
- d. The use of plain text mixed with encrypted text.

Conclusion

12. Various sources indicate that VC/NVA have increased their EW against the Allied forces. They are thoroughly familiar with our communication procedures and equipment. Some of their intercept units have English speaking personnel. They realise that EW, especially intercept, is a subtle yet highly effective means of gathering intelligence and causing confusion.

13. It is not known how much EW has aided the enemy but it must be concluded that if the VC/NVA are able to monitor our communications they have the potential to exploit any compromised information.



(G. J. LAWRENCE)
Major
Officer Commanding

Distribution

List C
HQ 1 ATF (12)
67 GL Sect
SO Sigs 2 AFV

CONFIDENTIAL