International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Protecting Existing Communication System of Bangladesh against Perceived Electronic Threats

Md. Mostafizur Rahman

Army IT Suppout Organization, Dhaka, Bangladesh

ABSTRACT

In the information age, commanders' decision making is excessively dependant on reliable and responsive communication system. Advanced technology is contributing towards this remarkably at the same time offering newer challenges to communication security. For Bangladesh to be effectively equipped with these modern equipments for secure communication will be difficult. Keeping this challenge in mind this paper makes an approach to identify the vulnerabilities of existing communication system and suggests protective measures against perceived electronic threats.

Key Words: Communication, protective, frequency, network, security, requirements.

INTRODUCTION

1. The Information Technology ministry is responsible for providing the backbone of Bangladesh communication systems in Bangladesh. Several diverse NTTN are designed to provide reliable, responsive and survivable communication supports to the dynamic forces on the battlefield with enough flexibility to meet the requirements of operational plan. Such communications are provided at three main levels. The backbone of Bangladesh communication includes a network of switches connected by multi-channel radio relays (RR) of very high frequency (VHF) / ultra high frequency (UHF) bands and an array of high frequency (HF) radios. Besides, the fighting and supporting arms units have integral signal elements to support command and control (C2). This communication is primarily based on VHF radios and field cables.

2. Today's battlefield is dynamic and lethal, and places demand on an integrated tactical communication system not experienced in the past. Communication systems must deliver to the commander the information he requires for decision-making quickly and in a form that facilitates the decision-making process. To do this, the tactical signal elements must provide reliable and responsive communication.

3. The electromagnetic spectrum will be our `Achilles heel' if we do not pay sufficient attention to protecting our use of the spectrum and at the same time recognize that we must take away the enemy's ability to see us and to control his forces." Unfortunately, reliability as well as survivability of the current tactical communication system in BANGLADESH in the event of a conflict is questionable now. The main reason for such speculation is that the tactical communication has never been tested for its vulnerability. Commands, staffs, communication managers and operators hardly believe that a threat exists and eavesdropping or a disruption could occur.

4. While studying the subject communication security (COMSEC), every practitioner would require a comprehensive knowledge on communication technologies and their application in the practicality. A secure tactical communication system demands an assessment of the EW capabilities of our potential enemy, which the system is likely to experience. Besides, it is also necessary to have an overview of own communication systems and their likely vulnerabilities to be exploited by perceived threats. It is also necessary to find some technical, tactical and training measures to pursue solution for the problems of COMSEC in Bangladesh. All these aspects of communication and COMSEC have been discussed in this paper.

A RECAPITULATION OF COMMUNICATION TECHNOLOGIES

5. The C2 of forces and weapon systems require an extensive exchange of information between headquarters (HQ), combat and combat support units and reconnaissance systems. Consequently, the main means of C2 in the combat zone (CZ) is radio and RR. From their type, location, structure, traffic flow and content it is possible to draw conclusions by potential adversaries as to the disposition, capabilities and intentions of the forces using them. There are whole varieties of communication serving many different purposes of the forces in a battlefield. Before any decisions can be taken concerning the need for security, choice of equipment, preference of technology, training requirements, regulatory requirements etc, the COMSEC practitioner must have an understanding of the behaviour or propagation of the radio waves emanating from the various communication systems. Such behaviour or propagations of communication systems are briefly illustrated in subsequent paragraphs.

6. Modes of Radio Propagations. There are three main modes by which radio can propagate:

a. Sky Wave. A wave transmitted from radios can travel 'along the ground' or bounce off the ionosphere. Waves that bounce off the ionosphere are known as 'Sky Wave'.

b. Surface Wave. Waves that travel through the air can either travel through the air or travel in contact with the earth's surface. The latter is known as 'Surface Wave'.

c. Space Wave. Waves travelling through the air is called space wave. This can travel pt to pt or line of sight and named direct space wave. The waves may be reflected off intermediate features and called 'Reflected space wave'.

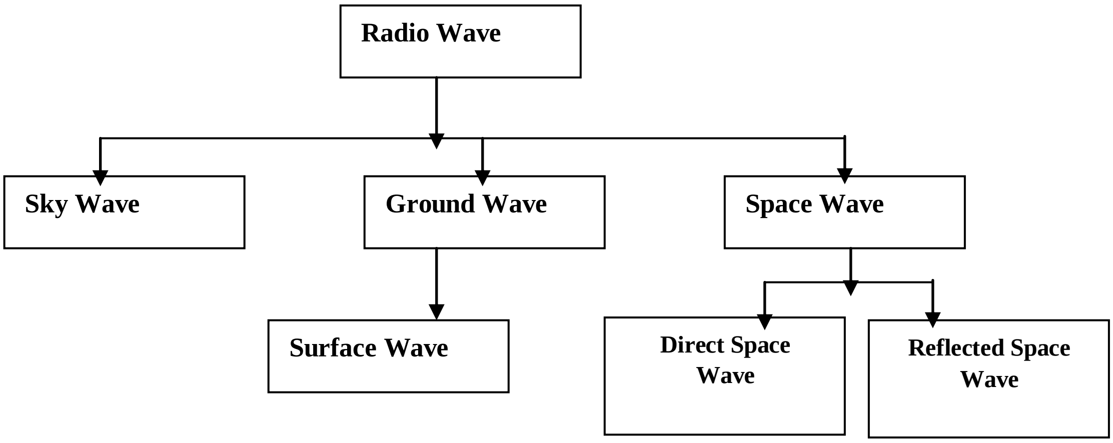

Figure1: Components of Radio Wave.

7. Frequency.In HF radios either surface or sky wave can easily be obtained. In VHF radios either surface or space wave is possible since ionosphere will not normally support VHF sky wave. At VHF and above only space wave is feasible It may be noted that all HF and VHF, the main combat net radio (CNR) bands, usually have two modes available as shown in below:

Waves	HF	VHF	UHF
Sky wave	√	-	-
Surface Wave	√	√	-
Space Wave	-	√	√

8. Nature of VHF/ UHF Radio Propagation. VHF and UHF radio communication are main means of C2 of combat and combat support forces. The radio waves of VHF (30-300 MHz) and UHF (300-3000 MHz) travel more or less along the line of optical sight. But frequency, power, antenna, earth's curvature, territory features etc limit their range. Without these limitations, VHF and UHF could cover a range of communication up to 1000 km or more.

a. VHF Radio. VHF is used for man-pack or vehicular purpose in the frequency range of 30-80 MHz at 25 or 50 KHz channel spacing. Its range varies between few hundred yards to about 50 Km depending on power, antenna and terrain features. Airborne systems can cover 100 Km or more.

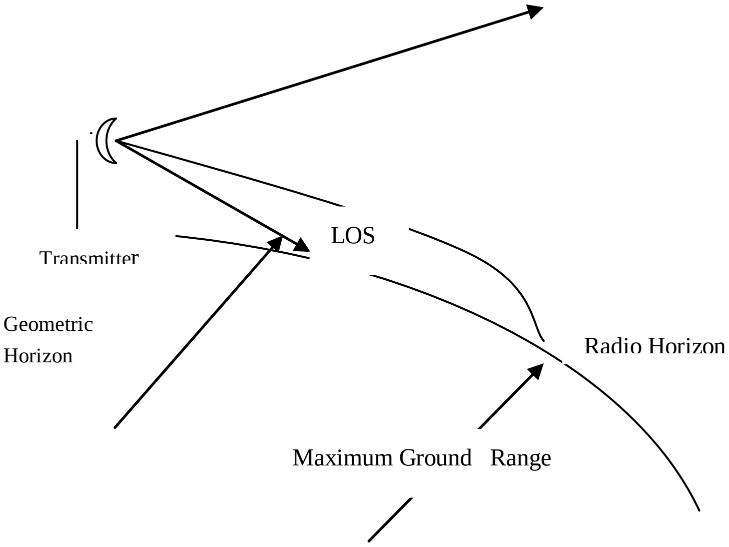

Figure 2: Modes of Propagation.

b. UHF Radio. UHF radios are used by aircrafts including helicopters for ground-to-air or air-to-air communication. It provides usual range of 70 Km between ground station and an aircraft at 300M heights.

9. Nature of HF Radio Propagation.

a. HF (2-30 MHz) communications are used at almost every level to cover larger distances. They are often used as backup to VHF or UHF means.

b. With whip antenna surface wave component of HF ranges approx 80 Km. It is devoid of obstruction and preferred for tactical communication.

c. At div or lower levels, own propagation is vulnerable to enemy's interception within 80 Km radius.

d. Sky wave goes beyond 100 Km and remains vulnerable to enemy interruption. Without security option the problem is more acute.

10. Nature of RR Communication.

a. Most tactical RR systems use VHF/UHF or even super high frequency (SHF) with highly directional antenna that forms lobes. The main lobe is directed towards the receiving station and requires quasi-optical line of sight (LOS).

b. RR produces weaker but exploitable side and back lobes, which are not necessary.

c. A single tactical link can be between 30-80 Km subject to the frequency, antenna, and terrain features etc.[1] Side and back lobes make the system vulnerable to enemy's eavesdropping and interception.

THREAT TO COMMUNICATION SECURITY

11. The nature of radio propagation proves their built-in vulnerabilities, which we have seen in the previous section. Hostile EW capabilities are usually tailored to exploit such weaknesses of C2 systems belonging to the opposing armies.

12. Threat to COMSEC. **Bangladesh** is a complex fighting machine. It is the command, control and communication (C3) that make this complex machine work. And without responsive communication there can be no C2. This is what is the importance of electromagnetic (EM) environment. Everyone from the commander to the radio operator must grasp the importance of secure communication and the great dangers that are present in the battlefields EM environment. To win, we must out-perform the enemy there. This is what is the nature of the threat to COMSEC and further details are as under:

a. ESM or EW Reconnaissance**.** ESM is a passive measure in an EW environment. It includes "the search, interception, identification and location of the equipment that radiates electromagnetic radiation[2]. For effective EW against our communication electronics, enemy requires to have knowledge of our equipment characteristics, capability, use and vulnerability to EW.

b. ECM or EW Attack**.** ECM is an active measure. It includes "all actions taken to reduce the enemy's effective use of the electromagnetic spectrum. The measures include jamming and electronic deception"[3].

(1) Jamming. Jamming is the measures taken by which own forces are denied the use of own C2 system effectively by an enemy using her electronic capabilities. Jamming is employed for the purpose of deliberately disrupting the use of electronic equipment and devices.

(2) Electronic Deception**.** The objective of deception is to mislead own forces and there-by creating a situation that is advantageous for the operation of enemy forces.

13. Signal Intelligence (Sigint). This is the attempt by a hostile force to continually maintain and update own database to include the technical characteristics of the communication equipments, own operating procedures and tactics. In combat, this database combined with current Radio Direction Finding (RDF) and other electronic information becomes the base for the refined intelligence analysis.

LIKELY ADVERSARIES OF BANGLADESH

14. Capabilities of Potential Enemies. Many EW techniques are rarely described or discussed outside of secret research laboratories, specialised books and journals, and the military units which put them into practice. The development in the field of EW techniques is always kept confined to the very essential few. The available military journals hardly address this issue. Thus, all information regarding our potential enemies is based mostly on intelligence report. However, the information that could be gathered on the EW capabilities of our neighbours are discussed below:

a. India. India's involvement in sigint activities has a long history, beginning some nine decades ago. Its sigint establishment is the second largest (after China) in Asia. Some of its facilities and operations are extremely sophisticated[4]. The overall EW capabilities of India are a combined effort of various organisations.[5].

b. The Indian maintains a very extensive sigint and EW capability, at strategic, operational and tactical levels. The bulk of the **India**'s sigint equipment at the tactical level was acquired from the Soviet Union in the 1970s. This includes both fixed HF and VHF direction finding (DF) systems and highly specialised truck-mounted DF and monitoring equipment.

c. Myanmar. Nothing significant could be gathered regarding Myanmar's EW capability. However, it is learnt that Myanmar has established sigint system that monitors all types of electronic signal coming in and going out of their country[6]. They mainly aim at destroying their enemy's use of electromagnetic spectrum facilities.

15. Assessment of Threat. Analysing the EW Environment and the Capabilities of Likely Enemies. It is certain that our communication is highly vulnerable to EW threat. Passive threat also exists at all times. Hostile ESM systems shall always keep an extra eye on our systems and sigint collection shall continue in peacetime. Possibilities of hostile ECM attack and deception cannot be ruled out at any stage. Active threat is mostly interference, jamming and destruction of communication equipment. This calls for the analysis of our present state of communication security.

ANALYSIS OF PRESENT STATE OF BANGLADESH COMMUNICATION

16. Levels of Communication. Communication in Bangladesh is provided at three levels. As per the principles of signal communication, AHQ is responsible for providing communication to all divisions and independent formations. These assignments are carried out by **Bangladesh** Telecommunication Regulation Commission on behalf of the ICT Ministry. At the second level, NTTN provide radio and fiber communication for the ICX and IGW. The smallest signal support element is brigade Signal Company, which is a composite sub-unit of signals that support communication to brigade down to battalions.

17. Means of Communication and Equipment. For providing radio and RR communication, different types of communication equipment are used by the Corps of Signals. Some of the relevant features of this equipment are discussed in the following sub-paragraphs:

a. Radio. Both HF and VHF radio equipment maintain radio communication. The power outputs of these sets are usually 15 to 20 watts. HF nets can cover a wider range of approximately a divisional area of 60 square kilometres. To cover even greater range specially for communicating with Headquarters (AHQ), 100 watts sets are used.

b. RR. RR communication is provided from AHQ to the divisional HQ and from the divisional HQ down to the brigade level. This is a highly directional, line of sight, Ultra High Frequency (UHF) communication system having the provision of handling huge voice and data traffic. The range coverage is about 25 to 30 kilometres depending on the terrain configuration, which may be extended up to 200 kilometres by placing relay stations in between.

18. Vulnerability. The **Bangladesh** in the field has a serious problem that cannot be readily cured. The radio net work, commander's voice channel and known to be his prime tool to control the battle may also be his weakness. The reason is twofold. There is not enough secure equipment for all voice channels, and secondly, poorly trained and inadequately supervised personnel often operate the equipment. The users, handicapped by either problem, or a mixture of both, unwittingly become the enemy's best ally.

a. State of Training. Whatever may be the state of equipment, due to lack of knowledge and efficiency of the operators as well as users regarding EW, the communication system becomes more vulnerable.

(1) Training and Efficiency on Equipment. The operators get formal training in the training centre and in the unit at different stages of their service. However, due to lack of resources and to some extent for lack of proper supervision at the unit, the operators face difficulty in learning the proper techniques and methods of establishing and maintaining communication.

(2) Training and Efficiency on EW. A survey was made on the operators and technicians of different ranks to assess their knowledge and attitude regarding EW. Unfortunately, the response was frustrating.

b. State Of Equipment. During peacetime, radio equipment is used extensively for different purposes. Besides trade training and exercises, the equipment is used as an alternative to telephone whenever the unit goes out for firing, route march or while performing other administrative duties. The use of the equipment, in all silly missions, shows little regard to the EW threat.

(1) Use of Electromagnetic Spectrum. An infantry battalion operates six to seven nets within a small area and uses that almost like telephone. There are approximately forty nets operate in a small divisional area. In the thick of the battle, almost all the nets become activated creating mutual interference and disruption of communication.

(2) During Normal Training. During normal training, efforts are made to explore maximum facilities of the equipment. Less care is taken to guard against passive EW threat. Due to extensive use and at times mishandling of different knobs of the equipment, the performance of the equipment reduces and even gets faulty.

(3) During Exercises. Radio and RR equipment are used lavishly during exercises. Control on the use of radio and monitoring of the nets is very limited. As such, the communication becomes more vulnerable to EW activities. For normal use, little care is taken to prepare and maintain the documents.

c. State of Procurement Management. Bangladesh has not yet been able to produce communication equipment. These equipments are procured either through the diplomatic missions abroad or through the local agents. Whatever options the suppliers provide, has no choice but select out of those.

d. EW Capabilities. No EW equipment has so far been procured by Bangladesh and as such doesn't have any offensive EW capabilities[7]. The proposal to set up an EW company has not yet been realised.

e. Limitations. Bangladesh being one of the under developed countries of the world, perhaps, cannot effort to have offensive EW capability. The economic constrain limits the choice of equipment for offensive EW.[8] However, any decision to this effect must be based on precise 'risk assessment', carefully considering the cost benefit of any project of protective measures against the risk involved.

APPROACH TOWARD PROTECTED COMMUNICATION

19. To reduce the vulnerability of own communication one will have to avoid detection by the enemy. Protection of communication should be given the required priority and for Bangladesh keeping the budgetary constraints in mind the policy for the procurement must be designed. Other important aspects needed to approach toward a protected communication system are discussed in succeeding paragraphs.

Technical Measures

20. Communication equipment offers several features that protect the transmission from hostile counter and support measures. Most of the features concern the technical expertise for efficient operation of the equipment and few are protection features based on equipment hardware. Some of the technical characteristics always come along with the radio equipment of the latest manufacturing, whereas, some involve additional accessories. However, few necessary technical measures may be described briefly below:

a. Steer able Null Antenna. Most of the tactical antennas used in Bangladesh are omni-directional. It is possible to save the antenna from a jamming signal coming from a particular source using this technique.

b. Directional Antenna. RR with directional antenna can suppress the side lobe and eliminate jamming.

c. Use of Reflectors. Unwanted signals can be screened from the antenna using reflectors. A steel building, weld mesh or chicken wire shall eliminate a jamming signal if placed correctly in relation with the antenna.

d. Squelch Tones. It is a fixed tone outside the voice or data band applied to the signal. For this reason, any unwanted signal not containing this squelch tone shall be eliminated at the receiver.

e. Modulation Type. There are different types of modulation such as AM, SSB, USD, LSB, CW, FM etc. Some modulations are more resistant to jamming than others. Like CW Morse is capable of working through jamming.

f. Cryptographic Protection. Using cryptographic protection it is possible to hide a network to a certain extent.

g. Frequency Hopping (FH). FH technique comes in many hops occurring at different speeds. FH radios hop between frequencies, dwelling on each for a short period. The hop set of frequencies may be a limited number, a band or the whole available band, with protected frequencies for other key users.

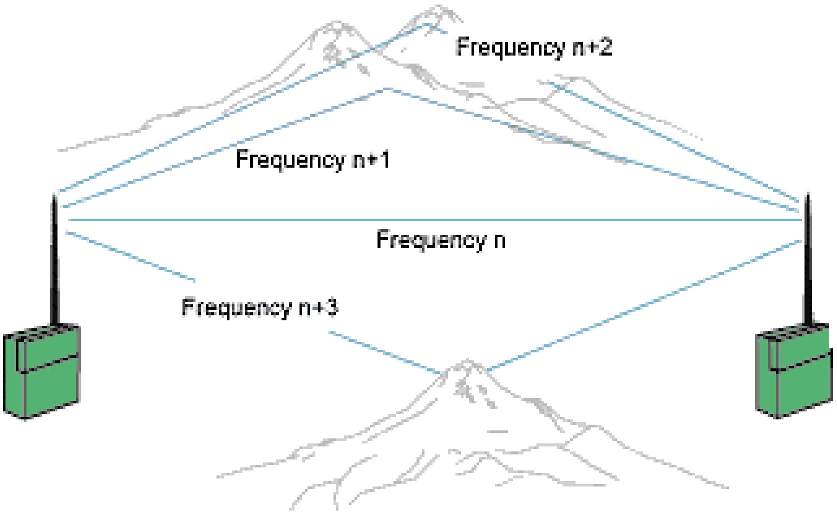

Figure 3: Depiction of FH functioning in MRR.

h. Spread Spectrum. This is another technique to defend radios against jamming. According to this, the signal is split in a pseudo random way and is transmitted with the energy spread across a wide bandwidth.

j. Free Channel Search. The set has a series of frequencies input and will search in a random fashion until it finds a free channel. It uses this frequency to open communication with the rest of the net using a specific code.

k. Burst Transmission. This is a suitable technique to be used on radio-based data circuits. Under a jamming situation radios are intelligent to find the lull, to compress the data to be transmitted and then quickly delivering at a very high speed.

p. War Reserve Mode. According to this technique the users reserve few of the transmission modes to be applied in case of war only. These are not used in peacetime. As a result, it will be difficult for the enemy to intercept this new mode of transmission and bring about effects of jamming.

Tactical Measures

21. These are the measures that concern the planning, application and deployment of the equipment and systems in the battlefield. Most part of securing own communication means using the equipment efficiently and appropriately, while guarding the same against all hostile interference. This is, in fact, the most important of the measures.

22. Siting of Radios and RR. Radios and RR should be sited, if possible, so that they are screened from the enemy. This reduces the possibility of interception and effective jamming. For each radio and RR planning the path profile analysis (PPA) technique to be followed.

23 Frequency Management. In a crowded EM environment frequency allocation is a problem. Poor frequency allocation creates chaos and limits the flexibility of communication planning under enemy EW attacks. Frequency allocation has to be held at higher levels and must have flexibility to allow the reallocation of frequencies to overcome jamming and interference.

24. Emission Control (EMCON). The EMCON state applies to all electronic emitters and is instituted in accordance with standard operating procedures (SOPs). It has two effects: the reduced or eliminated signature of friendly forces to enemy EW sensors and reduction of unwanted signals blocking out enemy transmission from friendly ESM sensors.

25. Masking. This is an active measure for protection that involves emplacement of a spot or barrage jammer in position where it can jam enemy ESM sensors. A spot jammer protects important net and barrage jammer protects a whole band.

26. Alternate Means. The means of communication should be diversified in order to enforce strict EMCON policies. Following are the available alternate means:

a. Tactical trunk system established through own RR and switches.

b. Existing telephone system.

c. Line communication.

d. Despatch riders.

e. Burst data transmission.

Training Related Measures

27. Training. Training of own personnel, to protect communication system is often neglected due to lack of interest and knowledge. During operational situation Bangladesh depends on radio due to absence or availability of poor alternatives. Therefore, operators as well as users randomly use radio considering them secure. It is important to re-emphasise the need for training of individuals and units on COMSEC as well as EPM.

28. Individual Training. The training must give the operators knowledge of the threat to their systems or equipment. This will range from threat briefings to intensive procedural training.

29. Unit Training. The defensive techniques must be designed to enable units and formations to reduce the effects of enemy EW and sigint in peace and war. It should cover all users and should not be limited to radio systems. Units should be trained on COMSEC mission during mission-oriented group training as well as during other collective exercises.

30. Training Modality.

a. Progressive Training. All the training standards, necessary for a well-protected communication system, may not be achieved in a day. Therefore, this training should be progressive.

b. Realistic. Nothing upsets soldiers' more than unrealistic training. The training should be planned considering own communication systems and equipment as well as their vulnerabilities. Besides, the threat situation may be depicted, as it is likely to be experienced considering our potential adversaries.

c. Operators Training. Training must plan for objectives/ goals for the operators. Communication systems should not be used for exercise control or NODUF purpose.

d. Use of Correct Procedures. Correct communication procedures like the voice procedures and communication drills are to be practised .

e. SOPs. All foreseeable communication incidents should be covered by SOPs. These must be rehearsed during training. However, SOPs shall include action on following circumstances:

(1) Action on Jamming.

(2) Action on Deception.

(3) Action on Procedural breach.

f. COMSEC. It encompasses many EW assets, codes to procedures etc. Breach of COMSEC may allow enemy exploitation across all nets through ESM and ECM systems. All breaches must be reported and it is very important for COMSEC.

g. Anti-Jamming Drills. Successful jamming delights an enemy and unsuccessful jamming attempt utterly frustrates them. Procedures must be practised and developed to work through jamming situation. Anti- jamming drills should be formulated for each type of radio equipment and regularly rehearsed.

h. Jamming During Training. This should be included and it must be realistic. Operators must be trained to recognise jamming and be able to execute correct drills. However, following points to be borne in mind while jamming during training:

(1) Jammers must be controlled and good alternate communication should be available.

(2) Operators must have a way of overcoming jamming such as alternate means, alternate frequencies etc.

(3) Over use of jamming may disrupt communication and thus frustrate own operators.

(4) Deception should also be introduced to allow operator to recognise jamming or deception.

CONCLUSIONS

31. EW technology has advanced quite a bit in the recent past and therefore; the threat could be very complex and enormous. As per the theory of EW, own C2 systems are likely to experience ESM activities during conflict. The purpose of this is very simple, reconnaissance of own means of communication to extract own information. Within the scope of this system, enemy shall search for the frequencies we shall be using, eavesdrop own clear texts, find direction of own transmission and locate the transmitters. After thorough analysis, the end product will be an electronic order of battle representing own forces. So far, the efforts have been passive. At this stage, enemy might consider if any offensive has to be launched on to the C2 systems identified.

32. Our potential adversaries have been reported to possess sophisticated EW equipment. In fact, they are already putting in sufficient experience in EW operations. India formerly used EW equipment from Russia. Recently, they are in a contract with a European manufacturer for EW equipment. The country has also developed own monitoring sub-systems. They have deployed sigint as well as tactical EW systems. However, little is known about EW capabilities of other countries in our neighbourhood.

33. Majority of risk to COMSEC originate from inefficient handling and employment of the equipment and systems. Therefore, tactical measures offer invaluable sources of solution to the problems of COMSEC. At first comes the planning of communication must be based on proper PPA. Masking technique should be observed while deploying the systems. Frequency management, allocation and assigning must be done systematically. EMCON policy needs to be defined accurately and adequately.

BIBLIOGRAPHY

Books

1. Arcongelis Mario de, Electronic Warfare: From the Battle of Tsushima to the Falklands and Lebanon Conflicts, UK: Blandford Press Ltd., 1985.

2. Ball Desmond, Signals Intelligence in India, Intelligence and National Security, Volume 10, Number 3, London, Frank Cass, 1995.

3. Dickson Paul, The Electronic Battlefield, USA, Indiana University Press, 1976.

4. Don E. Gordon, Electronic Warfare: Element of Strategy and Multiplier of Combat Power, New York: Pergamon Press, 1981.

5. Doug Richardson, Techniques and Equipment of Electronic Warfare, London: Salamander Book Ltd, 1985.

6. Laudon Kenneth C and Laudon Jane PI, Management Information System.

7. Neil Munro, Electronic Combat and Modern Warfare, London: Macmillan Academic and Professional Ltd, 1991.

8. Rice M A and A J Sammmes, Communications and Information system for Battlefield Command and Control, UK: Brassey Ltd, 1989.

9. Ross General Jimmy D, Winning the Information War, **Bangladesh**, February 1994.

Journals

10. Royal School of Signals, *Aerial Propagation, Precis 1*.

11. Royal School of Signals, *Aerial Propagation, Precis 2*.

12. Royal School of Signals, EW Handbook, Part 2.

13. Royal School of Signals, EW Handbook, Part 3.

14. Royal School of Signals, EW Handbook, Part 13.

15. School of Signals, Electronic Warfare, Jessore: 1997.