INDIAN DEFENCE RESEARCH AND TECHNOLOGY

Special Issue: Electronic Force Multipliers

Volume : V Issue : 1 March 2016

Jointly published by
Centre for Airborne Systems (CABS), DRDO
and
Institute of Defence Scientists & Technologists

INSTITUTE OF DEFENCE SCIENTISTS AND TECHNOLOGISTS

A SOLUTION PROVIDER IN DEFENCE R & D AND TECHNOLOGY

Aims & Objectives

To provide consultancy and technical expertise in the areas of Aeronautics, Armaments, Combat Engineering, Electronics, Life Sciences, Materials, MED, Missiles, Naval Systems.

Vision

The Vision of IDST is to make aware of the talents nurtured by DRDO and benefit from their capabilities in design, development and management of multifarious disciplines from the point of view of Defence, R&D and Technology

Mission

The Mission of IDST is to make available the expertise and knowledge of the vast pool of retired DRDO scientists, who are still in the prime of their intellectual capability, to the parent department as well as to any credible organization in need of such high quality of personnel

IDST HEADQUARTERS

DLRL Campus
Chandrayanagutta
Hyderabad – 500 005

Tel : +91 2444 0882
Fax : +91 2444 0375

Sri AK Chakrabarti
President

Phone : 040 24440882
Mobile : 0984 8613 713
Email : chakrabarti49@gmail.com

Sri BS Bansal
Secretary

Phone (Works) : 040 24440882
Mobile : 098 4979 8897
Email : bsbansal61@gmail.com
secretarygeneralidst@yahoo.in

IDST BRANCH OFFICES

Bangalore
ADE Campus
Chairman: C U Hari
Tel: +91 80 2528 3668

Hyderabad
DLRL Campus
Chairman: Harihar Singh
Tel: +91 40 2444 0375

Pune
ARDE Campus
Chairman: Dr.B R Gandhe
Tel: +91 20 2589 3341

Delhi
CFEES Campus
Chairman: J C Kapoor
Tel: +91 11 2390 7193

For more info contact any of the above or visit our website www.idst.co

CONTENTS

INDIAN DEFENCE RESEARCH & TECHNOLOGY

SPECIAL ISSUE: ELECTRONIC FORCE MULTIPLIERS

Indian Defence Research & Technology

Jointly Published by Centre for Airborne Systems, DRDO and Institute of Defence Scientists & Technologists

Designed and Printed at DESIDOC, DRDO, Metcalfe House, Delhi-110054

Foreword by Raksha Mantri

It is very important to educate the decision makers, the informed public and students on defence related technologies and trends. Towards this, the Journal being prepared by the Institute of Defence Scientists and Technologists (IDST) is a step in the right direction.

I note that this year the focus is on 'Electronic Force Multipliers', which is a very relevant and important topic.

I congratulate the IDST, Editors and Authors of the papers for the Journal and wish them all success.

डॉ. एस. क्रिस्टोफर
सचिव रक्षा अनुसंधान तथा विकास विभाग एवं महानिदेशक डी आर डी ओ

Dr. S. Christopher
Secretary Department of Defence R&D and DG DRDO

सत्यमेव जयते

स्वच्छ भारत
एक कदम स्वच्छता की ओर

भारत सरकार
रक्षा मंत्रालय
रक्षा अनुसंधान तथा विकास विभाग
डी आर डी ओ भवन, नई दिल्ली-110 011

Government of India
Ministry of Defence
Department of Defence Research & Development
DRDO Bhawan, New Delhi-110 011

From Special Editor's Desk

A Force multiplier is defined as a factor that dramatically increases the effectiveness of a group or an item. In modern day, electronics has emerged as the most potent force multiplier in all aspects of life. All around us, the all prevalent electronics equipment has resulted in a huge improvement and effectiveness on the capabilities of each and every human aspect.

In Defence also, Electronics plays a critical role in enhancing the effectiveness of each and every part of the equipment, system, weapon or soldier. The networked environment has further multiplied this effect. The availability of electronic force multiplier technologies and their effectiveness are decisive factors in modern warfare and is the subject for the current edition of Journal.

Till now, in India development of Electronics Force Multipliers have been carried out by DRDO/ISRO/BEL/HAL, etc. With the advent of Make in India there is a paradigm shift, where even private sector will be able to design/develop and sell these systems.

The aim of this Journal is to bring in the awareness to the uninitiated, technocrats, bureaucrats general public, students, etc., on the Electronic Force Multipliers in the defence and security arena.

I note that the topics selected and the papers, cover wide range of system/technologies, which affect the effectiveness of the security and warfare in modern times.

I congratulate IDST and Authors on excellent work and contribution and wish them all success.

(Dr S Christopher)

From IDST President's Desk

With the rapid advancement of technology and its numerous applications, military exercises are getting extremely challenging. Potential of emerging technologies in digital electronics, communication, special sensors, high energy ammunition and other areas have increased greatly for both defensive and offensive applications. Effectiveness of any weapon system can be increased manifolds if all its attributes are exploited, and for doing so, other technologies are to be applied intelligently, creating a strength, called the Force Multiplication. Electronics has emerged as leading force multiplier giving almost every system a new dimension in its manifestation and application.

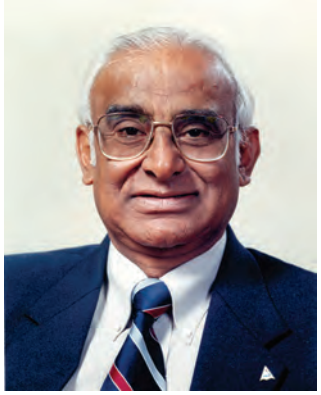
IDST, with its large pool of experts in all the areas of science and technology, can provide solutions to many military applications using electronics as a force multiplier. This issue of IDRT has brought out important applications exemplifying force mortification though various articles. I am sure our armed forces will get immensely benefited. The articles also will be highly useful for the researchers in the academies and the developers in the industries.

I appreciate the contribution of the authors and excellent effort of our editorial team to bring out this excellent compilation on the technologies which are of great importance to our armed forces.

A K Chakrabarti
President, IDST

CONGRATULATIONS

(yet another Diamond studded into his Crown)



Dr V K Aatre

Dr V K Aatre former SA to RM, Secretary Dept. of Defence R&D and DG DRDO, gave new impetus to R&D programmes of national importance such as development of Light Combat Aircraft (TEJAS), Electronic Warfare, Main Battle Tank (MBT) Arjun and Missiles. He was instrumental in the development of oceanographic ship 'Sagardhwani' for oceanographic research and set the DHWANI, a keynote for research in the field of Under Water System SONARS and Torpedoes in the country. He has been at the hub of the development of complex and sophisticated integrated electronic warfare systems for the Indian Defence Services and this special issue on Electronic Force Multipliers is an appropriate tribute to his achievements.

He is the recipient of many awards earlier such as DRDO Scientist of the Year Award (1986), VASVIK Award for Electronics Science and Technology (1990), IETE Ram Lal Wadhwa Gold Medal for Electronics and Telecommunications (1993) and Padma Bhushan Award (2000)

He has been a highly acknowledged member of many professional bodies, academic institutions and headed various committees for devising Policies and Programs of national importance.

In recognition of his sustained efforts and involvement in guiding the nation’s march towards many frontier technologies and make in India policy of the Government, **Padma Vibhushan** award has been conferred on him.

Associate Editorial by Director, CABS

IDST has been bringing out Journals on Specific topic with a view to educate general public, students on specialised area of defence related technologies. So far special issue Journals have been released on the following topics – Materials, Naval Sciences and Airworthiness Certification.

This edition of journal is dedicated to Electronic Force Multipliers. A relevant but a difficult topic to handle. Hence a careful selection of articles to cover force multipliers in the area of air/ground/sea based system has been presented. Also presented are the force multiplier effects of electronic warfare. The Cyber warfare is a hot emerging area having the potential to destabilize the enemy without any blood spill. Hence it was but natural that a paper on the same be included

All in all, there are fourteen papers bringing out the critical force multipliers, that are either emerging as potent force multiplier of modern battle field or continue to impact the outcome in the battle field

I hope the readers will benefit out of these topics.

M S Easwaran, OS
Director, CABS

Cyber Systems as Force Multiplier in the Battlefield

Saibal Kumar Pal

Scientist 'G'
Scientific Analysis Group
DRDO, New Delhi

G. Athithan

DS & CC R&D (SAM)
DRDO, New Delhi

Abstract: *Dependence of modern societies and nations on electronic form of communications, control and transactions has made human lives easier but has also added an element of risk and lack of control. Increased reliance of armed forces on information and communication technologies for distribution of information, command and control of operations, surveillance and reconnaissance is turning the cyberspace into a distinct domain of combat. Nations are now geared up on improving their defensive and offensive cyber capabilities for fighting and winning wars in this new domain of extended battle space.*

This paper explores the unique characteristics of cyberspace that has potential to be used as indispensable military power. Influence of information and cyber technologies on future wars and their effectiveness as military tools is investigated. Significant cyber conflict incidents and their implications for the future are also reported.

It is quite imperative that effective use of kinetic and cyber capabilities would act as a decisive factor and play a significant role in the future wars. A set of cyber strategies are presented, that may be employed along with conventional warfare and would act as a major force multiplier in the battlefield. This includes development of a cyber military force with proper technical skills, training and required infrastructure for defence of military-information networks and for handling major cyber crises. Development of capabilities for disrupting and destroying opponent's computer networks, extracting information without detection and altering information over enemy networks will play a crucial role and also impact operations in other domains of warfare.

1. Overview

Computing, communication, hardware and networking technologies have penetrated in almost all aspects of human life. Remarkable progress in these areas has also encouraged military forces around the world to improve their capabilities [1, 2] in information collection, transmission, processing and control. Weapon systems are infused with sensors, microprocessors and microcontrollers and connected to networks for augmented command and control [3-5]. Developments in intelligent systems and information mining [6] and their potential for integration with military

technologies have opened up a host of enhanced capabilities in the battlefield. Use of smart electromechanical devices, intelligent robots and networked swarm of tiny cyber bots [7] capable of sensing, information processing and interacting with humans would empower intelligence gathering, identifying and signaling incoming threats, providing improved visualization and augmented capabilities to commanders and soldiers fighting in the battlefield and attacking adversaries and their weapon systems. Advances in distributed, ubiquitous and high-performance computing, communication and quantum technologies, visualization and multi-media technologies, sensor and nano electronics and a host of new developing technologies promise to deliver action in the war field [8-13] never seen before. However, such integrated and sophisticated network-centric warfare scenarios [14] of the future also demand availability, protection and security of information [15-17].

Increasing dependence of nations on cyberspace for defense, citizen services and commerce has attracted a host of malicious activities of different intensities ranging from amateur cyber attacks to state sponsored cyber wars. Iasiello [18] defines **cyber attack** as "actions taken through computer networks designed to deny, degrade, disrupt or destroy an information system, an information network or the information resident on them". The UN Security Council in its Resolution 1113 of 2011 [19] defines **cyber warfare** as the "use of computers or digital means by a government or with explicit knowledge of or approval of that government against another state, or private property within another state including intentional access, interception of data or damage to digital and digitally controlled infrastructure and production and distribution of devices which can be used to subvert domestic activity". The CRS Report [20] states that "cyber war is typically conceptualized as state-on-state action equivalent to an armed attack or use of force in cyberspace that may trigger a military response with proportional kinetic use of force". A **cyber war** is considered to be different from **cyber terrorism** and **cyber crime** having different motivations, intent and method of operations. It is often difficult to differentiate between these actions carried out in cyberspace and categorize an attack as cyber warfare.

Cyber technologies have been used to attack computing platforms, information systems, networks and physical infrastructures controlled by computers, leading to disruption and destruction of state machinery, critical national infrastructures, financial and health services and public morale. Organized and state-supported cyber activities (crimes, espionage and warfare) [21-23] using sophisticated cyber tools and weapons is on the rise and a matter of concern for organizations and governments. An ever growing number of nations have placed cyber security as their military priority (Figure 1). In addition to the conventional domains of warfare viz. land, air, sea and space, there is an escalating arms race in the cyber domain. Cyberspace is stated to be the fifth dimension of warfare.

In the military domain, cyber technologies can be used to exploit military networks and information systems, infrastructure and weapon systems. Guidance of smart bombs, drones, fighter planes, war ships and missiles may be disrupted and deflected using cyber attacks [24, 25]. Even the ordinary foot-soldiers who follow wireless and network based commands may be easily confused and misguided.

With the current shift of power among nations and surge in global disturbances and terrorism, cyber attacks are likely to increase in frequency and intensity. In case of a serious attack, the military would require both defensive and

offensive cyber capabilities for its protection and retaliation.

Figure 1. Network monitoring in special US DoD cyber operation centers

The remaining paper is organized as follows. Section 2 emphasizes on the unique characteristics of cyberspace that make it suitable for warfare. In Section 3, we highlight the current limitations of using cyberspace as an independent domain of war and emphasize its use in conjunction and integration with conventional warfare domains. Section 4 highlights the defensive and offensive cyber strategies to be adopted to achieve information superiority. Weapons of cyber war and exploitation strategies for industrial control systems and critical infrastructures are also explained. Section 5 presents cyber warfare strategies to be adopted by nations for staying ahead in the global competition. Section 6 projects the force multiplier effect of cyber systems in warfare and explains the strength of integrating cyber operations with kinetic weapons of war. Section 7 gives the concluding remarks with a note that future conflicts would very soon demonstrate the power of cyberspace.

2. Unique Characteristics of Cyberspace for Warfare

Cyberspace has received considerable attention as a potential domain for warfare due to a number of unique characteristics not present in any of the other existing domains. Cyber attacks are characterized by their stealth, speed and surprise element. Cyber weapons can inflict damage over a wider geographical region but are less destructive in terms of physical damage and loss of lives. Damage can be inflicted by bypassing traditional military defense systems responsible for protection of physical territories. The logic-bomb attack on Russian pipeline system in Siberia (1982) and Stuxnet attack on Iran's Natanz uranium enrichment plant (2007) are examples of unarmed conflicts that have achieved their desired goals.

Unlike physical terrain, the cyber terrain changes and expands rapidly. The greater a nation is technically advanced and dependent on networked control, the more it is vulnerable to cyber attacks. Defense against all possible channels of attack involves very high cost and massive vigilance. On the other hand, cyberspace gives weaker players an attractive domain for directing asymmetric forces against larger adversaries despite their limited capabilities in the physical space. It also offers low price of entry for smaller players and enables low-budget wars that may be fought over prolonged durations.

Unlike conventional domain of warfare where massive infrastructure and sophisticated arsenal are required to participate in a battle, the level of efforts required in cyberspace is comparably lower. However, development of effective cyber weapons requires substantial skills and high quality of intelligence regarding the target.

Cyber weapons are homemade or available openly, commercially or from the underworld market. Such tools are not restricted by sanctions of 'developed' nations or by availability of material in short supply. Due to these reasons cyber weapons are difficult to control and may land up in wrong hands. Military related planning

and cyber capabilities are kept secret and are normally projected as a surprise during war.

Cyber warfare provides freedom to remotely and silently attack tactical and strategic targets with minimal risk to the attackers of being detected or facing the consequence of their actions. A target, irrespective of its physical proximity, may be instantly and anonymously attacked from an obscured source using fake IP address or compromised servers in some other foreign country. Attackers may frequently change locations or attack from multiple sources (as in DDoS attacks) without penetrating physical boundaries. Once attacked, the victim does not get any time for reaction.

3. Current Limitations of Cyberspace for Warfare

Despite a number of benefits of using cyberspace for military operations, currently it has the following limitations as an independent domain of warfare:

i. The coercive ability and destructive power of cyber weapons do not match with those of conventional kinetic or nuclear weapons. The prime ability of cyber war is to disrupt the adversary rather than cause physical destruction.

ii. Cyber weapons are built on vulnerabilities of operating systems, web browsers, communication and security protocols, compilers, databases and other software tools. These tools are normally used single-time in an operation and have limited shelf-life (till the vulnerability is discovered or patched).

iii. Cyber attacks are more uncertain in their outcome; it is difficult to assess the damage inflicted and recognize victory or defeat in this domain.

iv. It is difficult to direct precise weapons on the target and its impact may be less than expected. Effective attacks require intelligence gathering (specific to the target) and complex operations, which are difficult to achieve.

v. The cyber space is difficult to defend as it exists almost everywhere, has no boundaries and gives freedom to attack from anywhere.

vi. In the past, cyber activities have been more successful in non-military domain. There is not much confidence of gaining significant military effectiveness or any strategic advantage during war.

vii. Cyber operations and network centric warfare enhance vision and scope of the commander and troops; however automation and sophistication have given ample opportunities to the adversary for exploitation.

Each independent domain of warfare has its own strength and limitations. It is quite unlikely that a full-blown war would be fought purely with cyber weapons or in any single domain. Substantial increase in the impact of attacks requires cyber operations to be synchronized and integrated with kinetic operations in the conventional warfare domains.

4. Defensive & Offensive Cyber Operations

Technology enabled military weapon systems and infrastructures are critically dependent on computing, connectivity and cyber power. Today, cyber attacks can disable military communication systems and radars and redirect missiles and other ballistic weapons. Though this domain is in its infancy, history presents instances of attacks (Appendix-I) with the level of sophistication that nation states with sufficient budget, planning and infrastructure can support. Hence, it is important to develop both defensive and offensive cyber capabilities and raise military cyber mission units specializing in these operations.

4.1. Defensive Cyber Strategies

The simplest defensive cyber strategy is to use standard security measures and follow prescribed system configurations and policies as these help to prevent majority of the common cyber attacks. Primary protection of premises may be ensured by standard physical security, human entry screening and screening of physical devices and media using manual and automated methods. Standard procedures and tools for network monitoring, vulnerability scanning, and penetration testing and disaster recovery should be used. Automated mechanisms should be incorporated for identification of unauthorized intrusions or attempts, location of source, prevention of spreading, controlling damage and restoration to the extent possible. Watermarking technology may be used to detect website hacking or webpage defacement and automatic remedial measures may be instantly taken without manual intervention.

With dramatic increase in cyber related incidents, establishment of national and military cyber emergency response units is necessary for any developed nation. Figure 2 shows the webpage clips of the Computer Emergency Response/Readiness Team (CERT) of India and the USA. CERT-In, the Indian nodal agency is responsible for responding to cyber / computer security incidents across the country, issuing alerts, guidelines and advisories and developing emergency measures for handling such incidents. CERT-In collaborates and coordinates with other international CERTs including CERT/CC, US-CERT, JPCERT/CC, AusCERT, Korean CERT, Finland CERT, Brazil CERT and CERT-Mauritius.

Figure 2. Webpage clips of CERT-In & US-CERT

Many countries have developed special cyber operation units for military forces with personnel having technical expertise, rigorous hands-on training and required infrastructure and setup to carry out cyber operations. Such forces engage in defending information networks and systems against nation state adversaries equipped with military grade capabilities. These teams also develop expertise for handling major cyber crises in the military domain and chalk out anticipatory strategies for future disruptive and destructive cyber attacks. In addition to CERT, it is important for nations to develop a legal framework on cybercrime and update it from time to time.

Information storage and access have moved from fixed and stationary infrastructure to distributed and wireless infrastructure with mobile end-points. Inexpensive Internet-of-things equipped with computing units, sensors and connectivity (eg. A smart refrigerator, cooling system, washing machine or toaster) provide scope for easy attacks on the larger system or network. An increasing number of critical national and military infrastructures are getting hooked to

public networks. These developments have introduced drastic changes in the security requirements for information protection. It is important to take into account such environment and access points over which conventional security controls may not be applicable. A number of recent attacks have been found to exploit security weaknesses of these environments.

Vital military data flowing over networks, stored data and databases are required to be secured using high-grade encryption. Regular or similar transmissions between fixed points should be secured by steganographic communication, data hiding techniques or use of covert channels. Proprietary or closed (air-gapped) networks not connected to the Internet still face the risk of malware insertion by manual means like portable storage devices or by wireless means by transmission over radio, radar or audio frequencies.

Military networks and systems are assumed to be built using integrated circuits or chips free of any malicious circuits inserted during its design or manufacture. A sophisticated system is expected to have hundreds of IT products developed by different sources including third party vendors from different countries. Intentional insertion of malicious circuitry into such hardware may have devastating consequences during war. Hardware, software and hybrid attacks may be launched from remote locations with the intention of disrupting, misguiding or destroying the adversary military systems and networks.

Use of indigenously developed hardware, software and security products to the extent possible should be used for military applications. Another practical solution to this potentially serious problem (quite often understated) is to build advanced testing procedures and facilities for hardware components, IT & security products to be used in military systems and networks. On a similar scale, testing for resident software for intentional / unintentional vulnerabilities that may be exploited is critically important. For these systems and their components, testing based on high level common-criteria framework is advisable. Trusted foundry, high-assurance platforms and trusted computing paradigms may be employed for building military systems and critical national infrastructures.

Rapid development in quantum technologies is expected to have significant impact on the future of cyber security. Quantum communication, quantum information-processing, quantum encryption and quantum key-exchange promise creation of networks that would be impregnable by attackers. Though such technologies require heavy investments, military and vital government data can be protected with higher confidence against eavesdropping. In the other direction, quantum computers could be used to defeat modern encryption tools and tap adversary information from open networks. A good defensive strategy would be to gradually switch over to quantum-safe cryptographic systems before such technologies could be practically exploited by adversaries for cyber attacks.

4.2. Offensive Cyber Strategies

It is widely agreed that offensive cyber operations will be a critical requirement of future military warfare. It is therefore important to maintain cyber military forces that can disrupt specific information and communication infrastructures of the adversary and launch cyber-physical attacks (Figure 3) if required. However, it makes sense to launch attacks at time-zones that do not provide clues about the participating nation.

Figure 3. An oil pipeline in Turkey targeted by cyber attackers

The simplest form of offensive cyber activities is defacement and disruption of government websites of the opponent. Financial, media and business related websites are often targeted to cripple normal life of citizens. While accessing adversary networks, state actors make substantial efforts to map the adversary's cyber infrastructure from time to time. For creating backdoors, attackers use different vectors for delivering malware to the victim's network.

Analysis and design of sophisticated malware with different functionalities and characteristics (self-replicating, self-morphing, self-encrypting, self-cloaking and self-destructing) is vital for cyber warfare. For maintaining anonymity, it is important to use tools that hamper reverse engineering efforts. Expertise is required for creation of vulnerable blind spots and backdoors in adversary's systems that may be exploited during and after war. A more ambitious target is development and control of botnets for launching powerful DDoS attacks with bandwidth ranging from 100 to 1000 Gbps (currently ~ 250 Gbps).

Attacks on network protocols are launched with the hope of gaining access to useful information and cryptographic private keys. Man-in-the-middle (MITM) and man-in-the-browser (MITB) attacks are used in SSL sessions. Cryptographic attacks like chosen plaintext and cipher text attacks, brute force attacks and key deciphering with distributed computations or multiple machines can be carried out by capturing sufficient data and using high-performance computing infrastructures specially developed for military applications.

4.3. Weapons of Cyber Warfare

Vulnerabilities in operating systems, web servers, compilers and application software have been frequently exploited by malware designers. Morris, Melissa, CIH/Chernobyl, Nimda, Code Red, Slammer, Blaster, Mydoom, Sasser, Colflicker, Heartbleed are some of the popular malware based on buffer overflow, exploitation of access permissions, SQL injection, cross-site scripting, socially engineered attacks like spear-phishing and un-patched vulnerabilities.

One of the most effective software vulnerabilities is a "zero-day" exploit, i.e. a vulnerability that has been newly discovered or has not been patched and may be successfully used for attacks. Sophisticated malware have been designed in the past by exploiting such vulnerabilities in web browsers and other application software trusted by users to be free of such security flaws. Stuxnet, Flame and Duqu could navigate target systems, gather information stealthily, retrieve sensitive data, leave behind backdoors for exploitation, disrupt and misguide command and control systems.

4.4. Cyber Attacks on SCADA Systems

Inclusion of critical infrastructures into cyberspace [26, 27] and dependence of armed forces on commercial infrastructures has widened the scope of security and protection offered by the military. Electrical power generation and distribution systems, nuclear plants, air bases,

refineries and fuel pipelines, water purification and distribution systems, dams, banking and hospital networks, communication systems, email servers, satellites, trains and vehicular networks, emergency systems connected to the Internet or public networks – all are vulnerable to the threats in cyberspace. Network controlled critical infrastructures are irresistible targets during war as attack on these can inflict massive damage to physical infrastructures, environment and human lives and in turn affect both the military and civilian population.

Figure 4 shows common vulnerabilities in industrial networks like weak authentication and access control, unauthorized code updating or modification, remote access vulnerabilities, insecure communication links, poorly configured firewalls and application backdoors [28]. Use of public networks, use of standardized protocols, software and hardware, stringent requirements of availability and resource constraints invite a host of attacks on these systems. Attacks based on system hardware, software, databases, control network and protocol stack have been reported in the past.

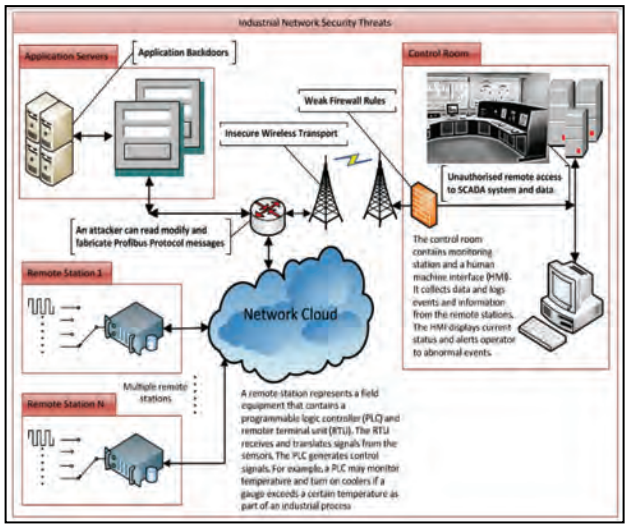


Figure 4. Common vulnerabilities in industrial networks (Source [28])

In 2003, the worm Slammer disabled the safety monitoring system for a few hours at Ohio nuclear plant in the US. Nuclear facilities of a few countries have been repeatedly targeted with malware like Stuxnet, Flame and Duqu. In 2012 Shamoon malware was targeted to disrupt oil production in the Gulf. In 2014 and 2015, the NSA informed that a number of nation-state organized attacks were launched to penetrate U.S. energy, water and fuel distribution systems. Similar attacks [29, 30] were reported in the last two years by many other countries without exposing details.

5. Cyber Warfare Strategies

An increasing number of sophisticated cyber warfare tools are under development in different parts of the world, turning the cyberspace into a new battleground of conflict. Future conflicts over physical space using kinetic weapons are also expected to have a silent cyber component. It is therefore important for nations to invest in military cyber commands specializing in different operations and integrate cyber technologies into military warfare.

A few lessons can also be learnt from cyber incidents in the past (Appendix-I) [31-34]. Use of cyber technologies for coordinated (kinetic and non-kinetic) attacks has been witnessed in Estonia (2007) and Georgia (2008). Such simultaneous attacks confused military forces, damaged national morale and delayed international response to physical conflict and demonstrated that cyber operations are effective military options in the battle space. Cyber weapons like Stuxnet, Flame, Gauss and Duqu were directed against military targets in Syria, Iran and a few other countries and could attain their objectives. Stuxnet was considered by experts to be functionally as effective as any conventional weapon of war. Logic bombs planted on gas pipelines could create explosions

without the use of any physical weapons. Herd of botnets used for DDoS attacks disrupted and paralyzed critical national services and military operations in the battlefield.

Since any network connected to the Internet is vulnerable to attacks, military should have air-gapped proprietary networks and standalone platforms that are never connected to open networks. Even such isolation is unable to provide full security as these networks require protection from manual and wireless insertion of malware. Standard physical security policies and practices should be employed for this purpose.

Encryption is not the ultimate solution for cyber security. However, it helps in effective protection of data during transit and rest. Data-centric security framework using encryption technologies ensures protection of vital data even if it leaves the parent network unintentionally or due to an attack. Robust and high-grade cryptographic devices based on indigenous crypto-algorithms provide security against resourceful state-actors.

Cyberspace is a suitable domain for influencing the perception of enemy during war by manipulating location and timing information. Deception and misinformation are used to create psychological confusion, fear and panic in the battlefield. Obfuscation techniques help to avoid detection of malware and resist reverse engineering of code. Log manipulation is used for destroying traces of attacks and unauthorized access to the victim's network. Replacement of system files on adversary systems is another intelligent disguise technique used in the cyberspace.

Cyber weapons like Stuxnet may be used to achieve objectives without the need of a full-blown conflict in the physical domain, at a fraction of cost and without spilling a drop of blood.

6. Force Multiplier Effect of Cyber Systems

Cyber capabilities combined and integrated with conventional military operations seem to be the most likely mode of future conflicts between nations. Cyber operations can be used to attack the enemy's critical military information processing capabilities, logistics and transportation, early warning and command-and-control systems leading to erosion of capabilities of the adversary to resist war. For example, a cyber attack on the military communication system or air defense system may drastically degrade capabilities of the adversary during war and improve the effectiveness of land and air operations. Also, information dominance gained by cyber capabilities early in a conflict acts as a force multiplier in the battle. In turn, conventional attacks can be scaled up using kinetic capabilities of cyber operations, resulting in a force multiplier effect.

Military conflicts in Iran and Afghanistan indicate that tactical and strategic surprise elements of the cyber space act as force multiplier and help weaker adversaries to develop better resistance against forces in the battlefield.

The stealth and anonymity of cyber operations attract considerable delay of counter operations due to the inherent difficulties in identifying the attacker. This gives a force multiplier advantage to the opponent to continue and multiply its operations in other conventional domains, thereby improving his position in the battlefield.

7. Conclusions

A cyber war fought with bits of software code, hardware chips and communication links operates in a different realm from conventional warfare and offers a new option to the management of modern defense. It is likely that future battles would involve all dimensions of warfare

including the cyberspace. Today, modern military forces require the Internet or Intranet for effective operations in the war field as much as conventional weapons and tools of warfare. Use of cyber weaponry combined and
Integrated with kinetic operations will act as a disrupter and force multiplier in the battlefield.

Disclaimer: All views and opinions reflected in the paper are of the authors and do not represent those of their employer.

References

1. The Military Balance 2014, International Institute for Strategic Studies (IISS), 2014, Retrieved from https://www.iiss.org/en/publications/military-s-balance.

2. Saydjari S., Cyber Defense: Art to Science, Communications of the ACM, Vol. 47, March 2004, pp. 53-57.

3. Miller R.A and Kuehl D.T., Cyberspace and the "First Battle" in 21st Century, Defense Horizons, No. 68, Sep. 2009, pp. 1-6.
4. Liles S., Rogers M., Dietz J.E. and Larson D., Applying Traditional Military Principles to Cyber Warfare, Proc. 4th Intl. Conference on Cyber Conflict, NATO, CCD COE Publications, Tallinn, 2012, pp. 169-180.

5. Ryan J., iWar: A New Threat, its Convenience – and our Increasing Vulnerability, NATO Review, Winter 2007.

6. Wang L.S-L, Hong T-P, Intelligent Soft Computing and Evolving Data Mining: Integrating Advanced Technologies, IGI Global, 2010.

7. Kott A., Alberts D.S. and Wang C., War of 2050: A Battle for Information, Communications and Computer Security, Retrieved from http://arxiv.org/ftp/arxiv/papers/1512/1512.00360.pdf.

8. Carr J., Inside Cyber Warfare, Cambridge, O'Reilly, 2010.

9. Singer P. and Friedman A., Cyber Security and Cyber War: What EVERYONE NEEDS to Know, Oxford University Press, India, 2014.

10. Jajodia S., Shakarian P., Subrahmanian V.S., Swarup V. and Wang C. (eds), Cyber Warfare: Building the Scientific Foundation, Springer, 2015.

11. Rattray G.J., Strategic Warfare in Cyberspace, Cambridge, Massachusetts: MIT Press, 2001.

12. Clarke R. and Knane R.K., Cyber War: The Next Threat to National Security and What to Do About It, ECCO: Harper Collins, 2010.

13. Mazanec B.M., The Evolution of Cyberwar: International Norms for Emerging-Technology Weapons, Potomac Books, University of Nebraska Press, 2015.

14. Katoch P.C., Indian Military and Network-Centric Warfare, Wisdom Tree, 2014.
15. Kabir A.H., Data-centric Security, National Cyber Security Institute Journal, Vol.1, No.3, pp. 21-33.

16. Cyber Security Review, Edition Summer, 2014, Retrieved from http://www.cybersecurity-review.com/wp-content/uploads/2015/03/Cyber-Security-Review_Summer-2014-Contents-page.pdf.

17. Diebert R, Towards a Cyber Security Strategy for Global Civil Society?, The Canada Centre for Global Security Studies and the Citizen Lab, Munk School of Global Affairs, University of Toronto, www.citizenlab.org

18. Iasiello E., Are Cyber Weapons Effective Military Tools?, Military and Strategic Affairs, Vol.7, No.1, March 2015, pp. 23-40.

19. UN Security Council, Resolution 1113(2011), 5 March, 2011, Retrieved from http://www.un.org/en/sc/documents/resolutions/2011.shtml.

20. Theohary C.A. & Rollins J.W., Cyber warfare and Cyber terrorism: In Brief, CRS Report, www.crs.gov, 2015, Retrieved from https://www.fas.org/sgp/crs/natsec/R43955.pdf.

21. Schreier F., On Cyber warfare, DCAF Horizon 2015 Working Paper No. 7, 2015, Retrieved from http://www.dcaf.ch/Publications/On-Cyberwarfare.

22. Tabansky L., Basic Concepts in Cyber Warfare, Military and Strategic Affairs, Vol. 3, No. 1, May 2011, pp. 75-92.

23. Parks R.C. and Duggan D.P., Principles of Cyber Warfare, Proc. IEEE Workshop on Information Assurance & Security, NY, 2001, pp. 122-125.

24. Mulvenon J., Towards a Cyber Conflict Studies Research Agenda, IEEE Security & Privacy, 2005, pp.52-55.

25. Lewis J.A. & Timlink, Cyber security and Cyber warfare, CSIS UNIDIR, Washington DC, 2011, Retrieved from http://unidir.org/files/publications/pdfs/cyber security-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

26. Morris T.H. and Gao W., Industrial Control System Cyber Attacks, Proc. First Intl. Symposium for ICS & SCADA Cyber Security Research, 2013, pp. 22-29.

27. Krutz R.L., Securing SCADA Systems, Wiley, 2006.

28. Abouzakhar N.S., Critical Infrastructure Cyber security: A Review of Recent Threats and Violations, University of Hertfordshire, UK, available at http://researchprofiles.herts.ac.uk/portal/files/2819465/Infrastructure_Sec_NA_final_v3.pdf

29. BCIT Industrial Security Incident Database (ISID), http://www.bcit.ca/appliedresearch/security/services.html

30. Offensive Security: The Exploit Database, http://www.exploit-db.com/, Accessed October 5, 2015.

31. Vaidya T., 2001-2013: Survey and Analysis of Major Cyber attacks, 2015, Retrieved from http://arxiv.org/pdf/1507.06673.pdf.

32. Cyber Defense Hardware Vulnerabilities, Defined Business Solutions LLC, Retrieved from www.definedbusiness.com

33. The Art of Cyber War: Nation Specific Attacks, K7 Computing UK and Ireland Security Blog and News, https://k7press.wordpress.com/tag/cyber-warfare/

34. Weedon J., Beyond 'Cyber War': Russia's Use of Strategic Cyber Espionage and Information Operations in Ukraine, Retrieved from https://ccdcoe.org/sites/default/files/multimedia/pdf/CyberWarinPerspective_Weedon_08.pdf

Appendix – I

Significant Cyber Conflict Incidents

Given below is a list of significant cyber incidents as ramifications of cyber warfare. This list is indicative and not exhaustive as few nations publicise attacks and others do not report even serious attacks. These incidents provide opportunities to learn from history and plan for future cyber operations.

Table 1. List of attacks and related details

Descriptive Name	Year	Targeted Nation	Probable Country of Origin	Mode of Operation / Tools used	Scope / Effect
Logic bomb	1982	Russia	USA	Software with intentional logic bomb.	Gas pipeline explosion due to malfunction of valves, pipeline pump turbines.
Chechen war	1997-2001	Chechnya Russia	Russia Chechnya	Website hacking. Anti-Russian information, news & images uploaded	Hacking & disabling Chechen websites. Use of information operations to influence perception.
Kosovo Internet war	1999	Serbia USA	USA China	Hacking of air defence control. Website hacking.	Facilitated bombing of Serbian targets. US government websites attacked.
Israel-Palestine cyber conflict	1999-2002	Israel	Palestine	Website hacking / defacement, DDoS.	Disrupted Israeli government & defence force information sites, telecom services, banks & stock exchange.
Titan Rain	2004	USA	China	Nature of penetration unknown.	Computer network penetration at DoD facilities.
Estonia cyber attack	2007	Estonia	Russia	Botnet hired DDoS attacks, website defacement.	Paralyzed Estonian government websites, banks & media outlets
Operation Orchard	2007	Syria	Israel	Hacking of integrated air defence systems.	Radar systems subverted to evade detection of fighter jets.
Russia-Georgia war	2008	Georgia	Russia	DDoS attack & traffic rerouting, website defacement.	Georgian servers were down & communications affected for long durations.
DDoS 2009	2009	South Korea, USA	North Korea	DDoS attacks.	Disruption of government, financial & media websites.
Kyrgyzstan DDoS attacks	2009	Kyrgyzstan	Russia	Botnet based DDoS attacks.	Disruption of Internet communications due to attack on all ISPs.
Stuxnet	2010	Iran	Israel, USA	Zero-day exploit based sophisticated	Damage of nuclear centrifuge systems used in uranium enrichment.

				malware.	
CBI_Hack	2010	India	Pakistan	Website hacking.	Defacement of government websites by Pakistan Cyber Army.
PA_Hack	2010	Pakistan	India	Website hacking.	Defacement of government websites by Indian Cyber Army.
Indian Defence hack	2010	India	China	Attack on servers.	Theft of classified military information, email information from Dalai Lama's office.
US satellite hack	2011	USA	China	Attack on satellite control systems.	Two US satellites interfered with for a few minutes.
White House breach	2012	USA	China	Spear-phishing attacks.	Multiple attacks launched on Government computers.
Indian government data breach	2012	India	Unknown / Not named	Attack on email servers, data breach.	Government information & information on troop deployment breached.
US gas data breach	2013	USA	China	Nature of attack not made public.	Security sensitive information of 23 US gas companies compromised.
US defence design compromise	2013	USA	China	Persistent, highly sophisticated cyber attacks.	Design of US defence systems compromised.
US State Department email access	2014	USA	Russia	Data breach.	Information regarding US State Department & White House compromised.
US database breach	2014	USA	China	Massive data breach.	21 million records stored in the US Office of Personnel Management compromised.
US Government data breach	2015	USA	China	Massive data breach.	Private data of 4 million current and former government employees compromised.

Unmanned Systems: Potent Force Enablers and Multipliers for Future Warfare

M. Suresh
Scientist
Aeronautical Development Establishment, Bengaluru

Debasish Ghose
Professor, Aerospace Engg. Dept.,
IISc, Bengaluru

Abstract: *Countries that are decreasing the size of their armed forces are in need of a greater number of force multipliers in order to continue their national and worldwide commitments. It is a myth that only expensive technology and aerospace platforms are the only force multiplier option. Low cost, highly efficient and expendable autonomous unmanned systems with innovative tactics and strategy have proved their capabilities as powerful force multipliers. This paper presents the various unmanned platforms, its capabilities and applications as potent force enablers/multipliers for future warfare.*

1. Introduction

Force multiplication in the context of defence is the enhancement of capabilities of a force achieved by a combination of attributes without increase in the size of the force. In the literature, it is widely defined [1] as a capability that significantly increases the combat potential of that force and thus enhances the probability of successful mission accomplishment. Force multipliers enhance the combat power of a force through various attributes which include increased radius of action of attack platforms, increased persistent endurance on the regions of interest and precision target engagement. The operational roles of these attributes are airborne early warning, aerial refuelling, electronic warfare, precision navigation, intelligence, surveillance and reconnaissance, command, control, communications and computers and network centricity.

Unmanned Aircraft Systems (UASs), which started their journey as supplement for manned platforms for peace time missions and research projects, have grown in their applications exponentially in the past two decades. Globally UAS programmes have made significant advancements in aerospace design methods enabling progression of platforms from fixed wing to rotary wing, tiled wing and flapping wing. Today, there is a UAS solution for many military and civilian requirements suitable for operations ranging from tactical and strategic C^4I^2 Surveillance, Reconnaissance and Targeting, mid-air refuelling, armed (self-protection and defensive) reconnaissance and combat missions that make UAS, truly "Omni-present" platform.

During mission, the existing UAS operating in the world have human in the decision making loop that restrict the autonomy at level 3 in scale

of 10. These UAS must be equipped with 360 degree situational awareness to enable dynamic path planning to exploit en-route events that make the UAS into a self-contained autonomous system, capable of making decisions on its own. A group of such solo autonomous UAS systems is required to cooperate and collaborate in a coordinated manner to achieve complex group autonomous mission. The end objective of autonomous systems can be achieved after transcending several challenges at each level of group autonomy [2]. Several literatures are available demonstrating group autonomous missions including group coordination tactics for a ground attack mission involving cooperation and collaboration among three different types of UAVs like reconnaissance, enemy suppression and attack UAS [3].

The current and futuristic operational roles of UAS matches in all aspects of force multipliers and it proves their indisputable worth by saving lives/operational costs every day in recent times thereby emerging as indispensable platforms during war. This paper discusses various unmanned platforms, their capabilities and applications as potent force enablers/multipliers for future warfare.

The paper is organized as follows, Section 2 presents various unmanned aerial systems and their classification depending on size, range and endurance. Section 3 to 7 justify their role as force multipliers based on their operations such as ISTAR, communication relay, armed reconnaissance, UCAV and cargo UAS. Section 8 discusses the need for reconfiguration of military doctrine and Section 9 concludes with the conviction that UAS are proven combat force enablers / multipliers.

2. UAS Classification

Unmanned aircraft system are either fixed or rotary wing aircraft capable of executing the mission without an on-board crew. Unmanned aircraft systems include aircraft and integrated equipment comprising propulsion, avionics, fuel, navigation and datalinks that are needed for flight. Depending on the mission needs, UAS are configured with mission packages that include sensor payloads to obtain images and videos, communication payloads to extend voice and data, weapon payloads and cargo payloads. UAS can be classified according to their size, range and endurance.

2.1 Very small UAS

The very small UAS class applies to UAS with dimensions ranging from the size of a large insect to 30-60 cm long. They are extremely small in size, very light weight, and can be configured as flapping, rotary and fixed wing. Flapping wing-based UAS allow perching and landing [4] on small surfaces. Examples of very small UAVs are the Israeli IAI Malat Mosquito, US Aurora Flight Sciences Skate and Australian Cyber Technology CyberQuad Mini.

2.2 Small UAS

The Small UAS class applies to UAS that have at least one dimension greater than 50 cm and no larger than 2 m. Many of the designs in this category are based on the fixed-wing model, and most are hand-launched by throwing them in the air. Examples of small UAS are AeroVironment RQ-11B Raven and Imperial Eagle from ADE, DRDO, India.

2.3 Medium UAS

The medium UAS class applies to UAVs that are too heavy to be carried by one person but are still smaller than a light aircraft. They usually have a wingspan of about 5-10 m and can carry payloads of 100 to 200 kg. Examples of medium fixed-wing UAVs are the US Hunter, Searcher UAV

from Israel and Nishant UAV from ADE, DRDO, India.

2.4 Large UAS

The large UAS class applies to the large UAS that can carry payloads more than 300 kg, Examples of these large UAVs are the US General Atomics Predator and the US Northrop Grumman Global Hawk and TAPAS from ADE, DRDO, India.

2.5 Classification according to range and endurance

The UAVs that have a range of 5 km with an endurance of 20 to 45 minutes are classified as short endurance very close range UAS**;** a range of 50 km with an endurance of 1 to 6 hours are classified as close range UAS; a range of 150 km or longer with an endurance of 8 to 12 hours classified as short range UAS; a range of 650 km or longer with an endurance of 20 hours are classified as mid-range UAS; a range of 300 km with an endurance of 36 hours are classified as Endurance UAS.

2.6 UAS across all echelons

Currently UAS are employed across all echelons dedicated for tactical, operational and strategic operations [5]. For Battalion level and lower, close range (less than 25 km) short duration (one to two hours) UAS that operate below the coordinating altitude are thoroughly integrated with ground forces as organic assets supporting tactical operations.

At brigade level, medium range (less than 125 km) and endurance (five to 10 hours) UAS are integrated with ground forces and other aviation assets.

At division level and higher, extended range (200 km or more), long duration (16 hours or more) UAS are used for direct support at tactical and operational levels.

3. ISTAR as Force Multiplier

ISTAR stands for intelligence, surveillance, target acquisition and reconnaissance and it is a process of integrating the intelligence process with surveillance, target acquisition and reconnaissance tasks in order to improve a commander's situational awareness and consequently their decision making. In general, surveillance is the systematic observation on the regions of interest and reconnaissance is the directed effort to obtain some specific information on the area of interest whereas target acquisition is to positively identify and precisely locate targets along with their signatures. These collected data are processed to provide timely, accurate, relevant, coherent and assured information and intelligence to enable mission commander OODA loop (Figure 1). The "OODA Loop," designed by US Air Force Colonel John Boyd [6], stands for Observe, Orient, Decide, and Act. During a mission, source of any action chain is first to be aware of a situation (Observe), and then to determine response options (Orient). The next step is to decide on the best possible response and finally, an action plan is carried out (Act). This loop continues as the situation evolves with respect to decisions and actions.

ISTAR is a standard mission (Figure 2) employed by all types of UAS across all echelons. The UAS designed for these missions are equipped with a mission sensor package that includes electro-optic, infrared, synthetic aperture radar, ground moving target indicator, signal intelligence and electronic attack. UAS operating at different layers enable cross cueing of sensor information and also increase the depth of intelligence. ISTAR missions finally lead to understanding and

mapping of friendly resources, enemy resources, their dispositions and intents. Irrespective of mission intentions and UAS characteristics, ISTAR is the fundamental mission and forms the source of action chain that positions the UAS as force multiplier.

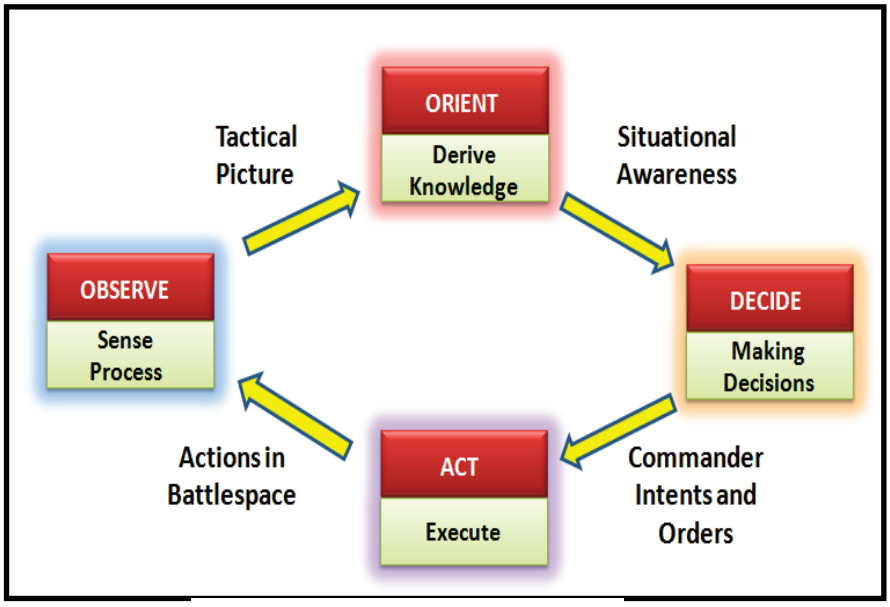


Figure 1. OODA Loop cycle

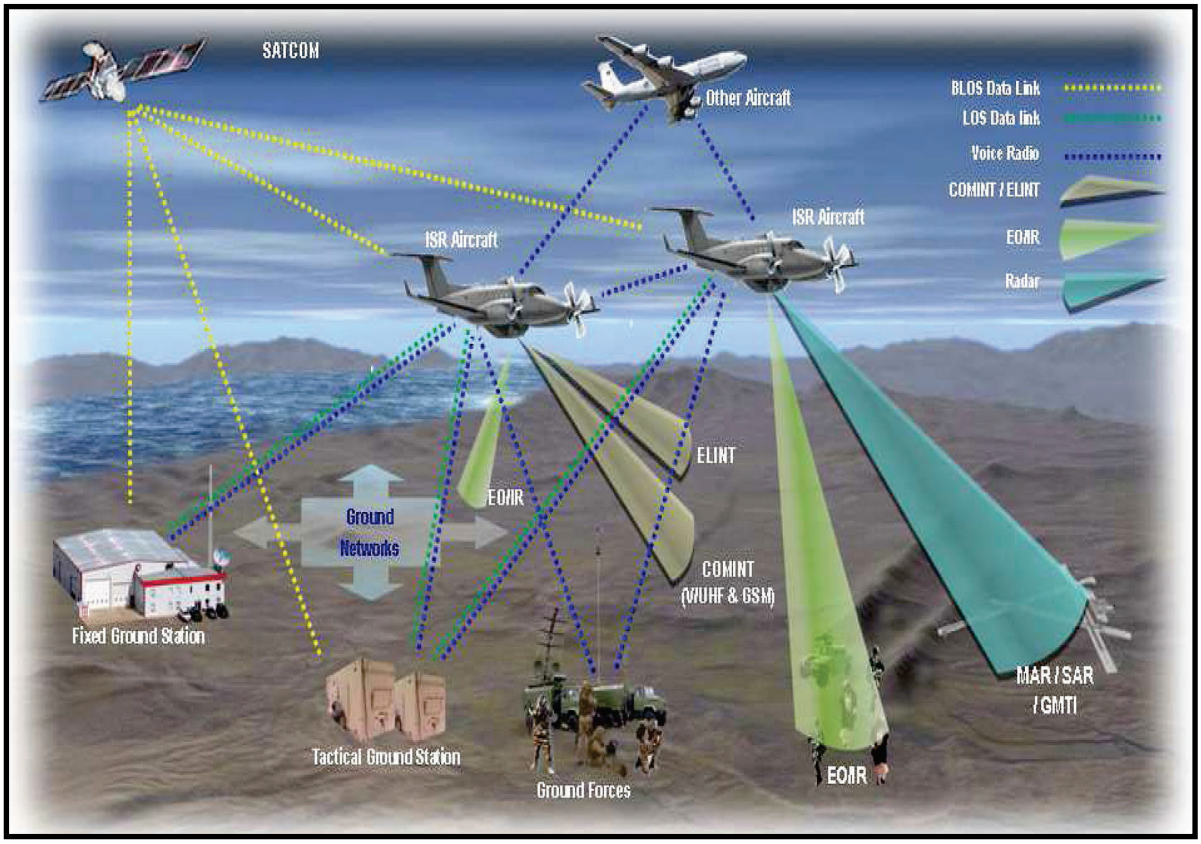


Figure 2. Overview of ISTAR operations [9] ***(Image Courtesy: Raytheon UK)***

4. Communication Relay as Force Multiplier

Communication relay payloads provide the capability to extend voice and data transmissions (enlarge the network by enlarging the footprint of radio on the ground) and allow commanders to share uninterrupted voice, data and real time video. The unmanned aircraft provides an aerial communications capability to extend the network in support of a specific UAS mission and provides retransmission capability for ground operators. For operations involving coalition forces, multi-language information/data translation capabilities [5] are important factors for successful communications and information sharing relative to UAS employment. Future communication payloads may include bridging, range extension and translation capabilities that will allow UAS to communicate between disparate types of radios, data links, and networks by supporting multiple wavelengths, waveforms and data formats. Additionally, these relays would reduce the dependence of SATCOM where frequencies may not be available or satellites might not have coverage in areas of operations.

In mountainous terrains, where the performance of ground based radars is extremely restricted, even AWACS (Figure 3) will perform sub-optimally due to radar shadows. This problem could be resolved if UAS equipped with airborne radars perform the role of gap fillers (force enablers) in the valleys and radar shadow areas. UAS with communication relay payloads capable of transmitting interoperable data and voice are a vital force multiplier to reduce the sensor to shooter timeline.

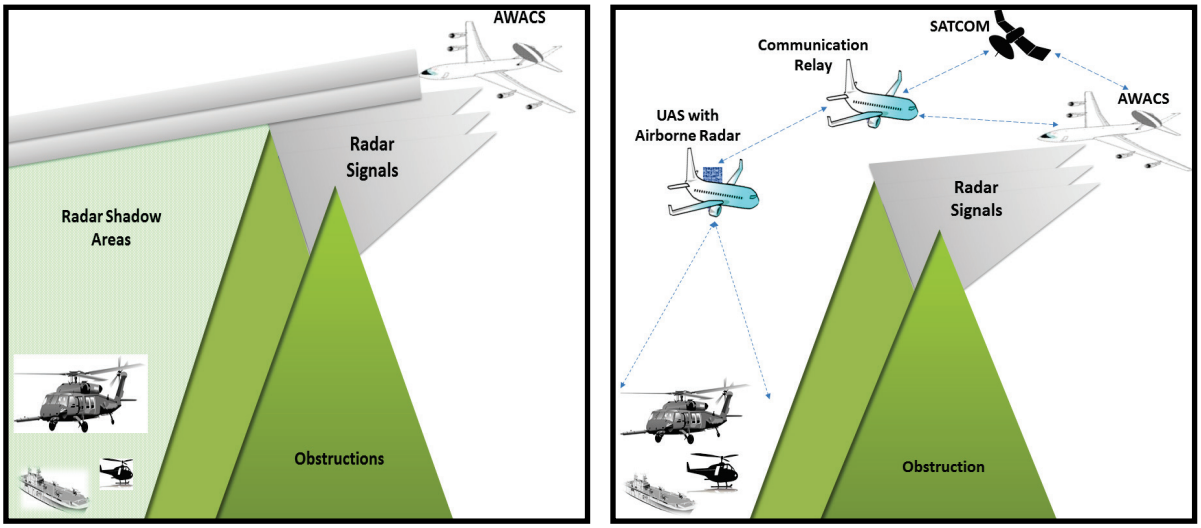


Figure 3. UAS role as "Gap Fillers" in Radar shadow areas (Force enabler for AWACS).

5. Armed Reconnaissance as Force Multiplier

The addition of defensive measures like low observable technologies and counter measures increases the survivability of the UAS system that enables interdiction/penetration missions. While doing these missions, it is quite natural for UAS to encounter highly sensitive, time critical perishable targets. In the conventional approach, the information of time critical targets are transmitted to the mission commander, who executes the OODA loop and initiates action plan to depute strike aircraft for target engagement. In this process, there is high degree of probability that targets will be missed, due to high sensor to shooter time line.

During mission, in order to engage the targets of opportunity at the instant of detection, UAS is required to be configured with additional feature “weaponization” that migrates UAS from traditional ISTAR role to multi-role UAS capable of armed reconnaissance / strike missions [7]. These UAS carry one or more missiles and upon detection of time critical targets fire a missile against them that exponentially reduces the sensor to shooter timeline.

The MQ-1B Predator is an armed, multi-mission, medium-altitude, long-endurance UAS that is employed primarily as an intelligence-collection asset and secondarily against execution of dynamic targets. Apart from Multi-Spectral Targeting System, the UAS carries two laser-guided missiles, Air-to-Ground Missile-114 Hellfire, that possesses highly accurate, low-collateral damage, and anti-armour, anti-personnel engagement capabilities. The Predator gives little warning of attack; it is relatively quiet and the Hellfire is supersonic, so it strikes before it is heard by the target.

6. UCAV as Force Multiplier

Due to technological advancements and ever growing needs of armed forces, efforts are being focused by researchers to design and develop unmanned combat aerial vehicle as a complement to manned combat aircraft [7]. The initial operational role for the UCAV is a "first day of the war" force enabler which complements a strike package by performing the Suppression of Enemy Air Defence mission [8]. In this role, UCAVs accomplish pre-emptive destruction of sophisticated enemy integrated air defences (IADs) in advance of the strike package, and enable the attacking forces by providing reactive suppression against the remaining IADs. Throughout the remainder of the campaign, UCAVs provide continuous vigilance with an immediate lethal strike capability to prosecute high value and time critical targets. By effectively and affordably performing those missions the UCAV system provides "no win" tactical deterrence against which an enemy's defences would be ineffective, thereby ensuring air superiority.

7. Cargo UAS

Sustainment/Cargo UAS may eventually deliver and or pick up supplies, equipment and personnel and it will ensure responsive and uninterrupted operations by transporting mission critical, time sensitive sustainment payloads. Cargo UAS [5] can support numerous small units, forward operating bases and combat outpost spread across extended distances characterized by impassable or un-secure road networks and rugged terrain where wheeled vehicles cannot reach.

8. Reconfiguration of Doctrinal Policy

The existing military deployment doctrine centred on manned resources with unmanned assets in a

supporting role. Also, the current doctrine involves human in decision making loop of any unmanned systems deployed across all layers in all echelons. Even in this deployment architecture, UAS has demonstrated its capability as force multiplier. This encouraging trend needs to be exploited by suitably reconfiguring the military doctrine, in order to unleash its full potential. This also necessitates the increase of autonomy level [2] of UAS to perform dynamic path planning on its own to exploit target of opportunity and avoid threats. Also, these solo autonomy UAS must be employed together in group autonomy mode in order to achieve complex missions on their own.

As UAS are operating at all layers in airspace, it is essential to build a robust integrated intelligence network by merging the information flow across space, air and ground based assets to enable net centric operations and warfare. Thus, reconfiguration of our military doctrines centred on unmanned systems as both force enabler and force multiplier for strategic and tactical operations is the need of the hour in 21st century.

9. Conclusion

The armed forces currently employ UAS across all echelons as dedicated support platforms for their tactical manoeuvre and intelligence operations across the depth and breadth of the battlefield. UAS are a proven combat force enabler/multiplier because they increase situational awareness, reduce workloads, and minimize the risk to deploying forces. In the future, the need for UAS will exponentially rise in tune with armed forces operational needs in network centric battlefield and emerging technologies. The armed forces envisioned, 25 years from now, will employ UAS across different operational environment, across different functional areas and across entire spectrum of operations as a key force multiplier.

References

1. Dictionary of Military and Associated Terms, Department of Defence, Joint Publication 1-02, 2015,http://www.dtic.mil/doctrine/dod_dictionary.
2. M. Suresh and D. Ghose, Role of information and communication in redefining unmanned aerial vehicle autonomous control levels, *Proceedings of IMechE, Part G: Journal of Aerospace Engineering*, 224(G2), pp. 171-197, 2010.
3. M. Suresh and D. Ghose, UAV grouping and coordination tactics for ground attack missions, *IEEE Transactions on Aerospace and Electronic Systems*, Vol. 48, No. 1, pp. 673-692, 2012.
4. Paranjape, S.-J. Chung and J. Kim, " Novel Dihedral-Based Control of Flapping-Wing Aircraft With Application to Perching", *IEEE Transactions on Robotics*, Vol. 29, No. 5, Oct 2013, pp.1071-1084
5. U.S. Army Unmanned Aircraft Systems Roadmap 2010-2035, US Army UAS Centre of Excellence, Alabama
6. Boyd, John R. “A Discourse on Winning and Losing,” 1987. Unpublished set of briefing slides available at Air University Library, Maxwell AFB AL, Report no: mu43947.
7. Michael Franklin, “Unmanned combat air vehicles: opportunities for the guided weapons industry?” Royal united services institute for defence and security studies, September 2008.
8. Atul Kumar Singh, “Transformation of Air Defence in Asia”, *Knowledge World International*, 2008
9. Chris Pocock, Raytheon UK develops New ISR Solutions, December 2014,http://www.ainonline.com/aviation-news/defense/2014-12-04/raytheon-uk-develops-new-isr-solutions

Airborne Early Warning System: A Potent Battlefield Force Multiplier

Dr K Rajalakshmi Menon
Sc 'G', APGD - AEW&C

Suma Varughese
OS, PGD - AWACS(I)

M S Easwaran
OS, PGD - AEW&C & Director

Centre for Airborne Systems, DRDO, Bengaluru

***Abstract**: Forewarned is Forearmed, the adage known to all. The forewarning of the impending attack by an enemy enables the country under attack to prepare itself for facing the eventual attacks. During the WW II, the lethality and force multiplier effect of air war was recognised. This also forced the countries participating in the war to device methodologies to detect advent of such air attacks. This resulted in one of the most important sensor namely Radar emerged which could detect flying targets at long ranges much before the aircrafts can reach their point. Though the ground based radars could provide reasonable warning of flying targets, these radars became limited when these aircrafts flew below horizon. Hence, the next logical step was to raise these radars to the heights from where these can "see" low flying targets. Thus started the precursor to the airborne early warning system, which today has emerged into one of the most potent force multiplier of the strategic as well as tactical battle field.*

1. History

It was British who recognised the advantages of hosting the radar system on to the aircraft and flying, whereby, these systems were able to detect targets flying low below the horizons. Figure 1 below shows the first such system developed by British during Second World War.

Though British showed the initial path, it was the Americans who recognised the potential of airborne force multiplier and began their quest for development of these systems in several flavours. Further, they also recognised the advantages of multi sensor systems and also bringing in the command and control element into these systems. Thus began the illustrious Airborne Warning and Control System(AWACS) which emerged as one of the most potent and effective force multiplier in the battlefield so much so that possession of such systems have become as essential part of the force projection.

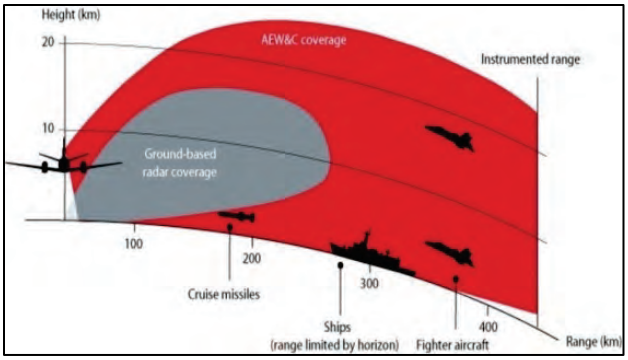


Figure 1. First Airborne Radar

2. The AWACS

The potency of an airborne multi sensor system, which can provide not only the early warning of the low flying aircraft, but also can do command and control functions on board was pioneered by AWACS. This enabled the system to be a potent on its own command and control system, which along with its assets can be deployed far away from the Home base and yet direct the complete air war without any limitations that would have otherwise affected such operations. US have developed several airborne surveillance systems with an intention of early warning oriented towards different mission requirements. The chief among them which made real mark were the famous E-3 sentry and E2 Hawkeye. The E3 was actively deployed in Operation Desert shield/ Storm and proved its mettle. It is stated that the E3 controllers engaged in 38 of the 41 air to air kill during the conflict [1]. The E3 was inducted into NATO as a major system which is currently under operation with their mid life upgrades having state of the art electronics. During the initial years, the E3 sported a mechanically scanned radar system on dome with IFF and associated electronics such as Mission Computer and operator work station on a Boeing 707 platform. Since then the system has gone through several upgrades, in terms of both hardware and software. The Electronic Support measure system has been added as an upgrade. In terms of command & control, the E3 can carry out multitude of functions such as interception management.

The variants of E3 have been now purchased by Japan, which has been developed on Boeing 767 platform. Around 45 numbers of E3- Sentry AWACS systems are in operation worldwide including with US, NATO, French and UK. (Figure 2). The USSR, not to be outdone, developed their own AWACS named A-50 Mainstay. (Figure 3)

Figure 2. AWACS (US)

Figure 3. A 50 Mainstay (Russia)

3. The AESA Revolution

The US E3/E2 and A-50 utilise mechanically scanned antenna installed in a rotor dome. The rotor dome itself rotates at a specific speed in tune with the coverage requirements. During the late 1990's, there were several advances in the electronics which profoundly affected the further development of AWACS/AEWs. These were the,

a) Development of digital computers
b) Decrease in size of the components
c) Development of Active/Passive Phased array technologies.

Owing to these, multiple countries then took up development of AEW/AWACS system utilising these technologies. One of the first to do so was M/s Ericcson of Sweden, who developed an AEW System on a SAAB 2000 aircraft which was much smaller than the AWACS of US/USSR called ERIEYE.

The Brazilians followed this with development of the same system from M/s Ericsson on Embraer 145 jet aircraft. Several of these systems were built and are operational. The main shortcoming of these systems is that they can cover only 240 degrees on either side of the aircraft.

Similarly, Israelis developed several version of these system on various aircrafts, such as 707(falcon), IL-76 for Indian Air force and Compact AEW on Gulfstream for themselves and Singapore. Out of this the IL-76 based system is the only true fully AESA based system that can provide full 360 degrees coverage without any degradations in any directions.

The Australians launched their AEW&C quest by placing an order for development of Wedge tail AWACS on Boeing 737 platform (Figure 4). The system makes use of "Top Hat" Configuration of the radar with normal antenna on the sides and end fire type antenna for coverage on front and back. However, the shortcoming in this system is that while there is full long range coverage on the sides, the range coverage in the front and aft is limited due to end fire configurations.

Figure 4. Various AWACS

4. Other airborne Early warning Systems

Though historically the AEW&C/AWACS basically refer to the Airborne Surveillance Systems aimed towards detection of the flying targets such as aircrafts, over the period other types of Early warning surveillance systems have been developed aimed towards varied applications/roles. These include Maritime Early Warning systems such as P8, surveillance and targeting attack radar systems such as JSTARS, ASTOR etc. Smaller format of these systems are hosted onto smaller aircrafts with varied payloads and functionalities. While the maritime aircrafts aim towards early warning of ships, boats as well as aircrafts over the sea lanes, the target attack radar systems such as JSTARS etc., are aimed towards warning and neutralisation of hostile entities on ground using imaging radars and systems.

Currently, the unmanned aerial vehicle revolution is in the offing which is opening up a whole new early warning system approaches.

5. The Indian Airborne Early Warning and Control System (AEW&C)

In India, the quest for acquisition of indigenous AEW&C began in 2004 (Figure 5). The system configuration envisaged a complete suite of sensors, which includes a fully active electronically scanned radar system, aided by other sensors such as the Identification Friend or

Foe system(IFF), Signal Intelligence sensors(ESM & CSM), Voice & Data communication Links and the onboard mission computer. The system is equipped with total C^3I and battle field management operations by adapting the multi sensor data fusion techniques. These systems are integrated on Embraer executive jet platform. The systems are flight tested and induction is likely in 2016.

Figure 5. Indian AEW&C

6. Airborne Early Warning as force multiplier

The modern airborne surveillance systems are generally referred to as force multipliers due to the reason that they not only provide early warning of the approaching hostile vehicles (aircraft, ships, boats or mechanized vehicles in ground), but also have requisite command and control elements which enable guiding of the friendly elements towards these hostiles to neutralise them through an element of surprise much before these hostile elements reach the point where they can pose a real threat.

Further, these modern systems are able to operate in an network centric environment, whereby the information from these systems can be communicated to the decision makers on ground, as well as to the weapon elements such as fighter aircrafts in air, ships in seas and to the own troops on ground where by providing them a vital vision of the overall battle field. All of these capabilities of these systems make them a potent force multiplier in the hands of the services which possess them.

7. Components of a Typical Airborne Early Warning System

A typical Airborne Early Warning and Control System contains all elements needed for it to be a C4ISR (Command, Control, Communications, Computer, Intelligence, & Surveillance) System. The major components of a typical system can be broadly classified as

a) Sensor suite to detect the targets in air, sea or ground.
b) A communications Suite to enable the dissemination of the information to the various decisions making centres.
c) On board command and control suite which typically can be to enable detection & tracking of targets in Air/Sea/Ground as the case may be, Identification & Classification of these detected targets through appropriate decision aid algorithms. Additionally functionalities for neutralising the threats through appropriate guidance/targeting of own weapon systems, such as airborne interceptors, missiles/bombs, UAVs etc.
d) An on-board mission computer system which will combine the information from on-board sensors and fuse them to provide a refined and recognisable situational awareness to the operators on board as well as on ground/sea.
e) A human machine interface with the system through suitable console/displays to enable the operators to have pictorial view of the situational awareness and also provide them capability to control the on-board sensor and communication suite to get the optimised operational performances as per the mission objectives.

All of these elements are housed in a typical aircraft and operate in an integrated manner

through appropriate interfaces on board and off board.

8. Primary Sensors of AEW&C

The Primary Radar forms the most important and critical sensor of any Airborne Surveillance system, due to its nature of being both long range detection and all weather operational capability. Most of the radars in a typical airborne surveillance system can provide multiple functionalities such as air target detection, sea target detection as well as imaging modes. The Synthetic Aperture Radars enable imaging of ground and are the primary modes in the surveillance systems such as JSTARS, ASTOR, and Maritime Surveillance etc. The pulsed Doppler radar system is the main sensor on a typical AWACS/AEW&C system.

The modern radar based on electronics scanning technology and distributed transmitters (Active Electronically Scanned Antenna Systems) provide capability for AEW system to detect, track and identify the targets rapidly and update the situational awareness in a controlled manner.

The Secondary Radar System of Identification of Friend or Foe system is derivative of radar systems, which enables identification of the targets detected by the main radar system.

9. Other Sensors of AEW&C/AWACS

The modern AEW&C systems also have SIGINT sensors (ESM& CSM) that scan the environment for emitters (Communication and Radars). This information can be used to further identify the targets through their on board radars/communications signatures.

Maritime Systems also host optical sensors for further detection and identification of sea borne targets.

10. AEW&C as Net Centric Command and Control centre

The modern battle is fought through a fully networked sensor, weapon and command control systems. The AWACS/AEW&C are no exceptions. With the multiple data and communication links on board the AEW&C has evolved into a much potent network centric command control centre. The networked operational capability has fully enhanced the force multiplier capabilities of these potent C4ISR systems.

With the early warning capability in conjunction with the ability to communicate with the command control systems off board on ground, sea or air, the AEW&C are emerging to have complete “Sensor to Shooter” capability. These are expected to be fully visible in the coming years.

11. Future of AWACS/AEW&C

In tune with the changing times the airborne surveillance systems are also undergoing changes in tune with the changing warfare. As mentioned above, the AEW&C’s future will be a potent networked command and control system with full sensor to shooter capability. Some of these are tight integration between the weapon systems such as missile command and control and an airborne targeting platform, such as an AEW&C system. The airborne platform must detect, track and sort the targets, relay very accurate position and velocity data to the missile command and control deploying the missiles, and then provide continuous real time target tracking updates as the missiles fly out to engage the targets [2]. As usual US leads the way with program in this with Naval Integrated Fire Control –Counter Air (NIFC-CA) program, which aims to provide “Engage-On-Remote and OTH capability to counter manned aircraft and cruise missiles”, “Link E-2D elevated sensor to Aegis ships and Navy fighter aircraft to

expand Air Defence battle space" and to "Utilize full kinematic range of active missiles". (*www.dtic.mil/ndia/2011IAMD/Pandolfe.pdf)*

Boeing also has successfully demonstrated simultaneous command and control of three Scan Eagle unmanned aircraft systems (UAS) from a Royal Australian Air Force (RAAF) Wedge tail 737 Airborne Early Warning and Control (AEW&C) aircraft flying over Washington state.

Further to these, both US & Israel are working on eliminating the manned crews on board AWACS. Whereby, the complete mission command and control will be done from the command & control centres on ground.[http://www.militaryaerospace.com/blogs/mil-aero-blog/2007/12/awacs-and-hawkeye-flight-crews-soon-may-disappear-into-the-pages-of-history.html]

12. Conclusions

The future conventional warfare is morphing predominantly into air and space warfare with Missiles, Unmanned Aerial vehicles emerging as dominant weapon systems. Further a convergence of surveillance, targeting and weapon systems in a single unmanned entity also is predictable. Further, the surveillance capabilities will also be raised to space, where the satellites are likely to play major role. The use of UAVs in conjunction with the more traditional radar based systems will enable the systems provide effective early warning at much larger distances. In due course the space based surveillance systems will emerge as ultimate early warning systems. A view from space can give even greater detail and surveillance than ever before. A combination of space and air-based early warning systems will enhance the force multiplication effect multi fold to levels hitherto not possible.

References

1. en.Wikipedia.org/wiki/Beoing_E-3_sentry
2. Future AEW&C Capabilities for maritime warfare.(www.auspower.net)
3. Forewarned is forearmed. http://www.satellite-evolution.com/digital/GMC-June2009/PDFS/awacs-web.pdf

Electronic Warfare Systems: Battlefield Force Multipliers

J. Manjula
Outstanding Scientist & DG (ECS), DRDO HQrs

1. Introduction

Warfare has evolved from positional warfare to Maneuver Warfare. Maneuver Warfare relies on the destruction of adversary's **"WILL to FIGHT"** rather than the **"ABILITY to FIGHT".** It relies on speed, surprise and application of firepower and movement. Warfare therefore is a competition based on time and space. The ability to enter into the enemy's OODA (Observe, Orient, Decide, Act) Loop, maintaining higher tempo of operations, creates opportunities for destabilizing the enemy's Centre of Gravity. Therefore, profound understanding of the enemy is of paramount importance. Hence Force Multipliers are an operational necessity to ensure optimal application of military force and achieve decisive results in short time frame. **Force multiplication**, in military parlance, is an **attribute** which makes a given force more effective than it would be without it.

Electronic Warfare (EW) has always been considered as a significant force multiplier with the adage that "The Army that Controls the EM Wave Controls the Battle Space". However, in terms of the objectives to be attained, EW can be defined to have the following functions:

Dominate: Dominate the electromagnetic spectrum, so that friendly forces can gain information on the adversaries and attack their systems (Soft/ Hard Kill).

Deny: Denying the adversaries use of the spectrum by disrupting C4I2 and facilitate use of the spectrum to own advantage.

Enable: Suppression of enemy surveillance resources and communication networks thereby **enabling** own operations thus achieving battlefield supremacy.

Electronic Warfare has offensive and defensive aspects that work in a "move-countermove" fashion. Often, these aspects are used simultaneously and synergistically to support the operations. Careful integration of EW into military operations will detect, deny, disrupt, deceive, or destroy enemy forces in varying degrees to enhance overall operational effectiveness. Through proper control and exploitation of the EM spectrum, EW would improve the likelihood of operational success. It enhances situational awareness through the interception, detection, identification and location of adversary electromagnetic emissions. It

enables friendly forces Freedom to Maneuver, Attack, Sustain, Protect, Control & Enhance the Operations.

The main elements of any battlefield are sensors, communication systems, weapons, platforms and counter measure systems as shown in Fig. 1.

EW systems contribute to Force Multiplier effect in battlefield from the sensing to neutralizing the hostile threats. In fact, EW sensors being passive are also employed to carry out the passive seeker function in the modern missile systems.

The following sections briefly discuss the trends in the Electronic Support & Electronic Attack systems contributing to the Battlefield Force Multiplication.

2. ES Systems

The main role of Electronic Support (ES) System is to search for, intercept, identify, and/or locate sources of radiated electromagnetic energy for the purpose of immediate threat recognition. These systems act as the "Eyes and Ears" of the Fighting Formations engaging in or engaged by EW operations and provide vital information essential to the success of military operations. Even though, ES is generally catered for tactical missions over multi-octave frequency coverage with 100% Probability Of Intercept (POI), the peace-time signal intelligence collection will be carried out by Signal Intelligence (SIGINT) Systems. The information and subsequent intelligence gathered by the SIGINT systems will be used for building the radar library of ES systems to address the immediate threat recognition in the hot war scenario so as to initiate appropriate Counter Measures. ES assets are totally controlled by the theatre commander at operational and tactical level while SIGINT assets are responsive to tasking at strategic level. Another distinction between SIGINT and ES systems is the type of signals of interest. The SIGINT systems operate in an unknown electromagnetic environment and attempt to record sufficient data for subsequent analysis. ES systems are employed primarily in detecting and identifying EM emissions with established signal parameters. In performing this function, an ES receiver could be employed during a tactical reconnaissance mission or as a Radar Warning Receiver (RWR) on an attack aircraft. While the operational roles of ES and SIGINT systems are distinct there is commonality in the system architecture and basic parameters to be measured. ES systems are envisaged for the detection and analysis of either Radar or Communication signals and accordingly they are classified as Radar-ES or COM-ES systems. Similarly, for strategic role, SIGINT systems are classified as Electronic Intelligence (ELINT) systems for the detection and analysis of Radar signals and Communication Intelligence (COMINT) systems for the detection and analysis of communication signals.

2.1 Radar-ES/ELINT Systems

Military systems, employ wide variety of radars like search radars, fire-control radars, weapon locating radars, tracking radars, terrain-following radars, imaging radars and weather radars. These radars operate in the frequency bands of HF to MMW
(30 MHz – 95 GHz) in Pulsed and CW modes. Present day radars using LPI (Low Probability Of Intercept) signals pose challenges to ES receiver systems attempting to detect them. Techniques likes Spread Spectrum by Frequency Hopping, Frequency modulation and waveform coding with poly phase and barker codes, pulse compression, Low transmitted peak powers, phased array based search & track modes, adaptive power control etc. are being

incorporated in radar systems to reduce the vulnerability of radar detection by conventional ES/ELINT systems. On the other hand, the modern ELINT systems are being configured with MW/MMW channelized / superheat receiver front-ends and high speed digital receivers for achieving enhanced sensitivities of the order of -90 dBm with fine parameter measurement accuracies for the detection and analysis of LPI radars. Similarly, the wide-open receivers intended for instantaneous multi-octave frequency coverage are configured by employing techniques like homodyne down conversion and Direct Digital Synthesis (DDS). The Direction of Arrival (DoA) is the most important parameter in ES/ELINT systems which is generally measured by employing amplitude, phase or time difference of arrival techniques. Present day ES/ELINT systems are capable of measuring DoA and frequency information with an accuracy of <1 deg. rms and <0.5 MHz rms respectively in real time and can handle 1 MPPS. By using the DF information, it is possible to carry out the location fix (CEP) of the hostile radar emitter for the purpose of initiation of a Counter Measures either by soft kill or hard kill methods. Radar Finger Printing System (RFPS) is another important capability of present day ELINT systems, which facilitates intra-pulse and fine grain analysis for the purpose of unique identification of radars. By exploiting this capability, the commanders can track & monitor the movement of hostile troops and derive strategic intelligence about the adversary.

2.2 COM-ES/COMINT Systems

Military forces generally use communication systems in HF, VHF and UHF bands. The signals may be short duration, i.e., burst and/or spread spectrum (FH, DS-SS) with various analog and digital modulation schemes. Line of Sight (LOS) Microwave links, Cellular phones (GSM, CDMA) and SATCOM links are commonly employed to disseminate voice and data. Surveillance and weapon systems usually exchange data via voice or digital links. Software Defined Radio (SDR), Combat Net Radio (CNR) and satellite phones are also important potential targets for the COM-ES/COMINT systems.

The communication emissions are characterized by parameters viz. frequency, bandwidth, power level, modulation, time of intercept, and Direction of Arrival (DOA). Communication Electronic Support Measure (ESM) Receivers must perform Reconnaissance and Direction Finding (DF) by means of wideband high speed frequency and spatial search. This permits to detect and process signals of interest in a multi-user interference environment in an accurate and timely fashion. The DOA information provided by DF system is the primary key for sorting radio emissions stored in the database of detected signals. By measuring DOA's from at least two (preferably three or more) different DF stations whose locations are accurately known, the Position Location (PL) of the radio source can be obtained. In EW applications, knowledge of the DOA enables timely execution of Electronic Counter Measures (ECM) i.e, soft skill, whereas PL information helps in EOB generation to carryout hard kill.

COM-ES/COMINT system mainly consists of two subsystems, Direction Finding subsystem and Monitoring & analysis subsystem. The DF system gives the DOA information about the hostile communication emitters. These systems usually operate in the frequency band of 30-3000 MHz and employ techniques like correlative interferometry, Pseudo Doppler, Time Difference of Arrival techniques. DF accuracies of the order of 2-4 deg. rms and scan speeds of the order of 80

GHz/s are envisaged from the COM-DF systems. On the other hand, the monitoring receivers mainly cater for the narrow band signal analysis (modulation recognition, estimation of modulation related parameters), demodulation with audio output and decoding. Narrow band Signal Analysis is an activity that provides valuable insight into the signal being analyzed and requires significant time for analysis.

3. EA Systems

The objective of EA systems is to reduce or suppress the effectiveness of enemy defence systems and their relevant weapons systems through softkill actions such as confusion, distraction, deception, or seduction. In the absence of Electronic Counter Measures (ECM), the kill probability of the current generation of weapons systems is very high and could produce a high attrition rate (i.e., large number of casualties and destroyed assets) during a combat mission. ECM systems cover the whole electromagnetic spectrum and are named in accordance with either the wavelength/bandwidth in which they operate or the equipment function against which they operate as Communication-ECM (C-ECM) to work against communication systems and Radar-ECM (R-ECM) to work against radar systems. Although C-ECM systems are only of the active type, R-ECM systems can be either of the active or passive type. Chaff in the RF band provides the countermeasure without any signal transmission, usually a seduction through the concealment of the real target.

3.1 Radar ECM Systems

Basically two types of radars are countered by R-ECM systems: surveillance and tracking radars. The surveillance or search radar functions are designed to locate and automatically track targets within a large volume. This allows the commander to perform threat evaluation and weapon assignment. Because surveillance radars have to detect targets at long range, they usually operate at lower frequency bands of the EM spectrum. These radars are usually characterized by a rotating antenna, either the parabolic- plus-cosecant-square (cosec^2) type, which provides 2-D target location, or the phased array type, which provides 3-D target location. The typical transmitted waveforms are pulse-compression signals with 3-D radars having also some form of waveform agility in the elevation scanning.

The tracking radars are high-priority threats that need to be countered by R-ECM equipment because they are associated with the engagement of a weapon system, especially in the terminal phase. When a tracking radar is locked onto a target, the associated weapon is also expected to be directed at the target. The task of the R-ECM system is to cause the tracking radar to break lock, which in turn removes the guidance information used by the weapon to converge on the target. The tracking radars are characterized by a narrow beam supported by a relatively small dimension antenna, usually operating at high RF frequencies (X to Ka band).

Each aircraft or ship that can be engaged by a weapons system has to be sufficiently protected by R-ECM systems capable of providing for its self-defence. In the airborne case, it is generally desirable to supplement the strike aircraft's self-protection system with either an Escort Jammer (EJ) or Stand-Off Jammer (SOJ) system. These systems are carried on escort platforms. Escort jamming involves a dedicated aircraft carrying high-power jammers that accompanies the friendly strike force and provides a protective RF jamming shield in support of the entire strike force. Stand-off jamming involves a platform that stands at some distance beyond the effective range of the weapons that defend the target.

Present day R-ECM systems employ either deception or noise jamming techniques for countering the hostile radar threats. Digital Radio Frequency Memory, RF Decoys and Phased Array based Multi-Beam jammers are significantly contributing towards the force multiplication in the modern day battle field scenario.

3.2 COM-ECM Systems

The main objective of C-ECM systems is to deny, over a defined area and by means of jamming, the transportation of information performed through the RF links, communication or radio systems of the adversaries. The most important adversarial RF links to be jammed are the ones that are connected to the Command and Control centers (C2). Modern communication systems use mostly digital modulations, but a large number of legacy communication systems that employ analog modulations are still employed in the battlefield. Due to the relative short effective jamming range, CECMs are mainly employed in ground battlefield application either in expendable or stand-in jammers on board ground vehicles or unmanned aerial systems. Expendable jammers are usually small units with a limited operational life(that of their batteries) and with a small ERP.

Present day C-ECM systems employ either deception or noise jamming techniques for neutralizing hostile communication emitters. Follow-on jamming / multi-frequency jamming techniques are applied against modern SDRs. Imitative jamming for deception using pre-recorded messages / voice signals against FH signals, burst and Fixed Frequency signals are also being employed in the battled field scenario.

Typical Indigenous EW systems developed by DRDO are shown in Fig. 2 (a, b & c).

4. Conclusion

The prime focus on the futuristic EW systems is on Size, Weight and Power (SWaP) considerations with multi spectral frequency coverage ranging from HF to MMW and beyond. The present demarcation of dedicated systems for tactical and strategic roles is blurring and unified architecture encompassing both ES & EA functionalities on a common hardware is envisaged to counter the emerging threats in both radar and communication systems. Multi Sensor Data Fusion and networking of sensors, platforms and weapon systems is emerging as a major trend to achieve enhanced battlefield Force Multiplication.

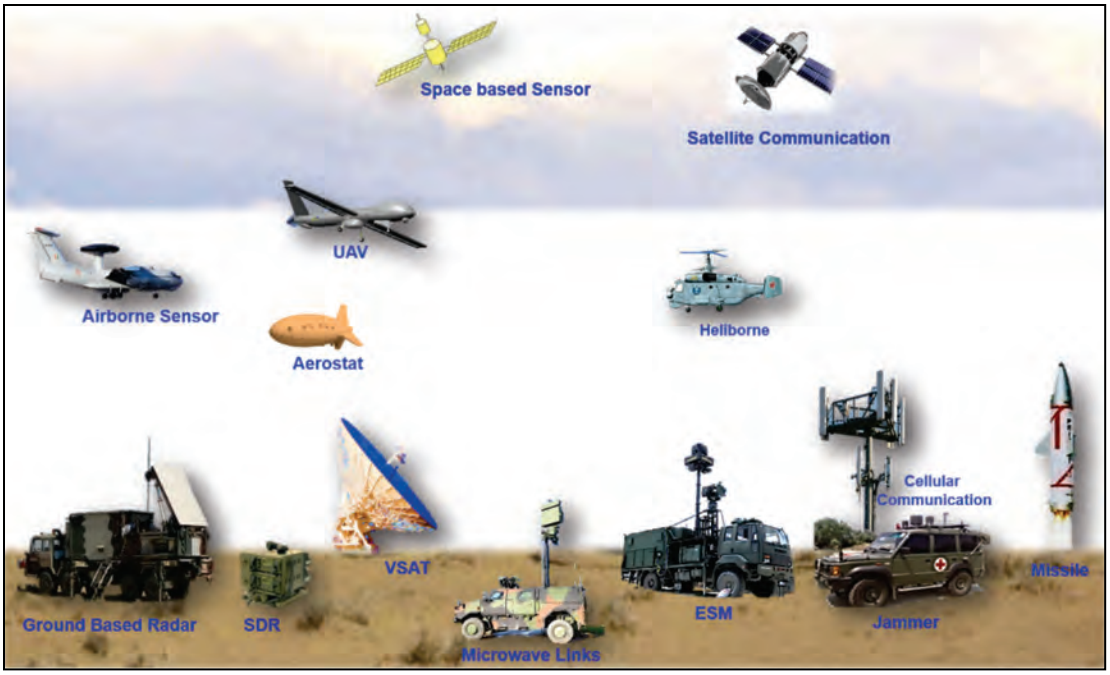


Figure 1. Typical Battlefield Elements

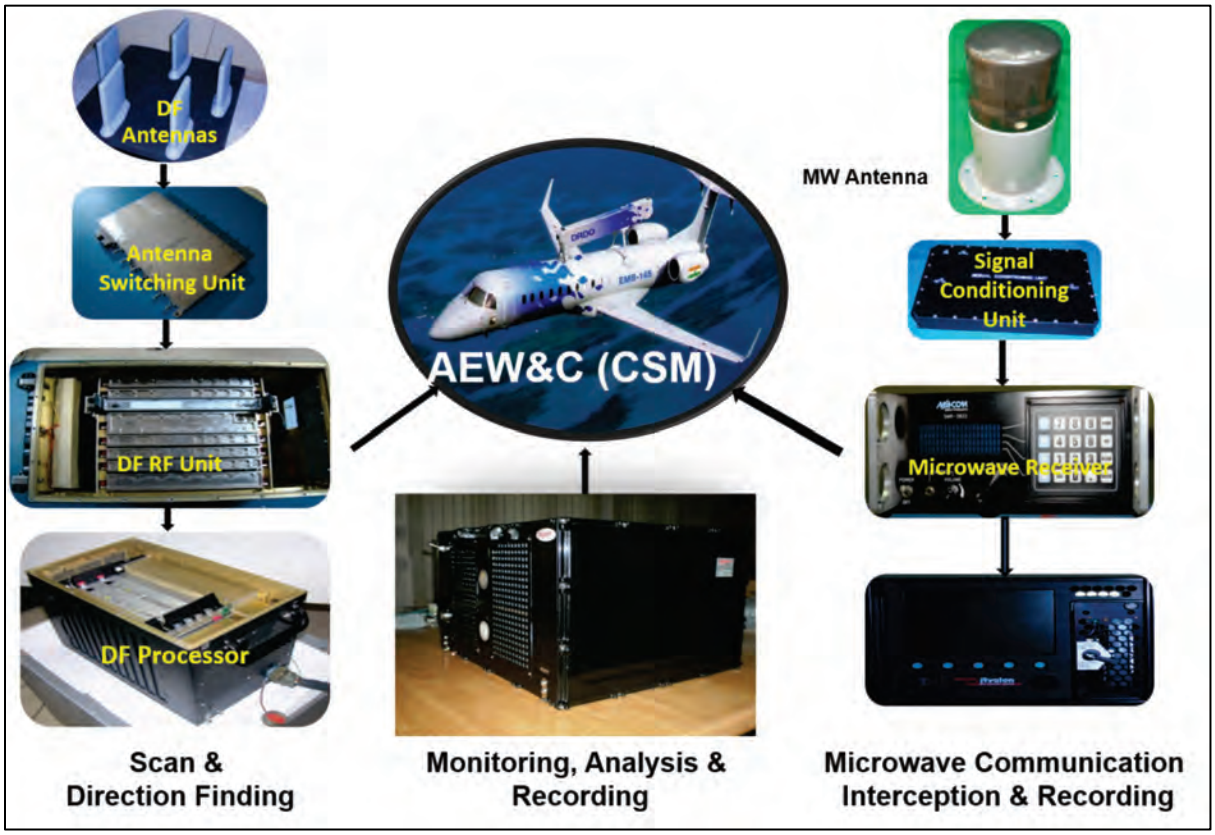


Fig: 2(a). Indigenous COMINT System on AEW&C platform.

Figure 2(b). Indigenous Ground Based EW Suite consisting of ES, ELINT & EA

Figure 2(c). Indigenous Ground Based Communication Jammer System

Electronics Leading to Force Multiplier Effects in Undersea Surveillance

Jojish Joseph V, Sc 'E'

Arun Kumar K S, Sc 'E'

Unnikrishnan N, Sc 'C'

Saravanan S, Sc 'C'

P. Balakrishnan, Sc 'G'

Naval Physical and Oceanographic Laboratory, DRDO, Kochi

Abstract: *Naval surveillance capability is of utmost importance in securing and maintaining peace and stability in the Indian Ocean Region. The advances in electronics and communication technologies have made possible a number of innovative ways where harnessing of disparate sensors and systems lead to a force multiplier effect in the operational arena. This paper looks at some areas where the technological progress in electronics and communication area can be made use of to improve naval surveillance capabilities and the future trends in that direction.*

1. INTRODUCTION

Naval surveillance capability is becoming all the more important in protecting vital national interests in the twenty-first century. India is blessed with a long coastline, abundant natural resources along its coast and exclusive economic zones. To safeguard these interests and also to provide efficient deterrence against any aggressive intentions, it is of paramount importance to maintain naval superiority in the Indian Ocean. Historical lessons over the past centuries also point to the key role played by naval forces in shaping the outcome of decisive engagements. The philosophy of Alfred Mahan is still valid and is being pursued by all major maritime powers in the Indian Ocean Region (IOR)[1,2].

Indian policy making has understood these issues and from the start of this millennium has consciously worked to attain a blue water fleet. With an increased pace in the induction of advanced

warships as well as robust submarine building programs, Indian navy is poised to become a force to reckon with in the IOR. Most of these platforms are equipped with state-of-the-art surveillance systems and formidable weapon systems which enhance the strike capability.

In an increasingly networked world, innovative technologies are the key value providers in bringing together the different fighting units and providing a force multiplying effect. Networked sensors and combined information presentation systems are the key areas where new advances in electronics drive the firepower multi-fold. In this paper we look at the key areas where advances in electronics technology offer significant force multiplier effects in naval surveillance and targeting.

2. PRESENT SCENARIO

Naval surveillance is taken up in three domains - on air, on surface and sub-surface. Long range aerial surveillance is achieved through specific air-borne early warning sensors. Warships typically carry surveillance equipment including radars for detecting aerial and inside-horizon targets, hull mounted sonar for detecting underwater targets and low frequency variable depth towed array sonar for long range surveillance. The sub-surface complement of submarines have integrated surveillance suites with an array of sonar taking sensor information from different sensor arrays placed at various locations on the platform which operate at varied frequencies and offer an integrated underwater surveillance picture to the user. Specific surveillance measures also include airborne low frequency dunking sonar carried on helicopters for specific missions and torpedo defence systems which include towed array sonar and towed & expendable decoys for torpedo defence.

In all these spheres, technological advances have made quantum jumps in the capability and performance metrics of the individual sensors. India has developed commendable indigenous capability in naval surveillance specifically in undersea surveillance domain. Most Indian naval platforms are equipped with indigenous sonar which offer at par and better performance when compared with any foreign sonar of similar specifications and have the distinct advantage of having superior ocean database, modeling and analysis capabilities in the Indian waters. Advances in state-of-the-art electronics has allowed the computational capability to go up while simultaneously achieving a reduction in size and power of the hardware required, thereby packing powerful algorithms in much lesser form factor.

3. NEED FOR FORCE MULTIPLIERS

Naval warfare perceptions are changing from large scale engagements at sea towards distributed and asymmetric threats from near home. Scanning the littoral coast is becoming important part of naval surveillance. This scanning needs to be often sustained and continuous to provide near real time detection and response to it. Littoral surveillance is challenging due to the high density of vessels, very high levels of ambient and correlated noise sources in the areas of operation and the amount of data which needs to be processed in real time. To effectively maintain a credible surveillance and attack capability over both littoral and deep waters an integrated approach where different subsystems seamlessly interoperate is necessary.

This calls for novel ideas where advances in electronics, communication and signal processing techniques would bring in methods of synergizing the various elements of surveillance and provide a force multiplier effect. Electronics and communication domain has seen quantum jumps in

technology advances over the past few decades. We are at a stage where the power and price per processing unit is at an absolute minimum thus offering enormous choice for system builders. The last decade has also seen the explosion of concepts like internet of things, distributed sensor networks as well as efficient technologies for cloud based computational units to achieve a common goal. Signal processing techniques like compressed sensing which led to the one pixel camera are pointers to the unique opportunities where optimum solutions to often intractable problems can always be found with proper technology and vision.

4. FORCE MULTIPLIERS IN NAVAL SURVEILLANCE

4.1 Distributed Systems

In the traditional surveillance system mode, a platform has many sensors which are independent entities. They offer area coverage but are independent of each other in specific modes or bands. To synergistically add value to the surveillance capability a meaningful combination of these units are required. Typical combat management systems try to offer these solutions where an integrated view from all the sensors is provided. But a far more powerful approach is to have the basic surveillance system itself to have the capability to make use of a flotilla of platforms to gather intelligence and present a meaningful picture.

Multi-static operational capability which is present in the new generation sonar offers a glimpse to the possibilities in this area (Figure 1). In a fleet with many ships each with different sonar there also exists a mode of operation in which one sonar on one ship assumes a master configuration and directs specific transmissions from a designated transmitter. All the receiver platforms use this information and process the data from their receiver arrays and achieve a total area surveillance result. A typical example is a helicopter carrying a dunking sonar going ahead making a transmission using a dipped projector and all the ships in the fleet use the pulse to detect the returning echoes to achieve much higher area coverage in underwater surveillance. This has been enabled by the networking capabilities which are at present available to each ship and being extended to the sensor, the sonar. The common console where all the information is aggregated has a large and clear picture of the whole operational theatre and need not even have the specific sensor on-board to achieve this.

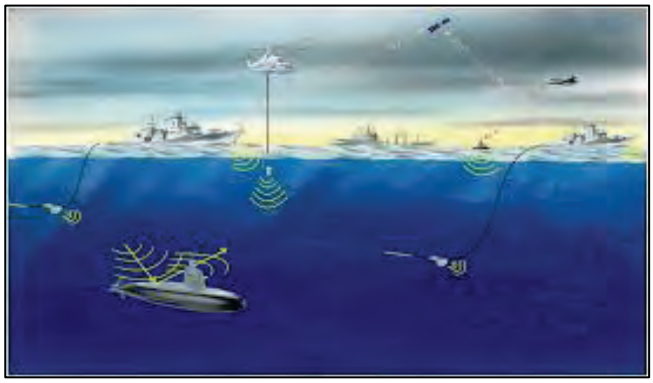


Figure 1. Multi-static Sonar Operation

4.2 Unmanned Underwater Vehicles

Unmanned underwater vehicles (UUVs) have been in the realm of theory for long but with limited application to elaborate surveillance due to various limitations. But of late, navies all over the world are giving renewed focus and budget to developing robust UUV capabilities. US Navy has developed a host of different types of UUVs for its needs and continues to invest heavily in building technologies and systems for UUVs[3]. The use of a network of remotely operated UUVs as the first line of defense against mine hunting and mine clearing have moved much closer to reality (Figure 2). Reliable methods of underwater communication, improved sensors and imaging sonar which are custom built on the

UUV and enough computation resources to do online analysis has made UUVs a preferred choice for littoral surveillance applications.

The technologies for ad-hoc networks, large scale sensor networks and their communication protocols specifically tailored to underwater scenario have been topics of current research in the signal processing and networks domain. Combined with the advances made in high frequency sensors, precision sampling and high speed data acquisition systems along with quantum jumps in processing power the option of a deployable army of UUVs for area surveillance is no more in the realm of fantasy.

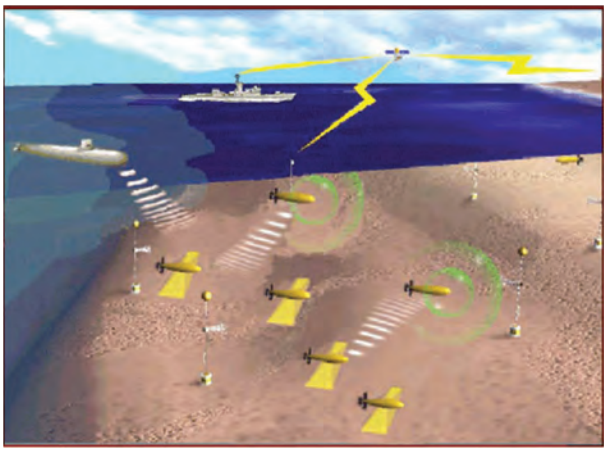


Figure 2. UUV for Mine Hunting

4.3 Specialized vehicles for Surveillance

The idea of having specific platforms for surveillance alone was in vogue even a decade earlier [4]. US navy operates silent shallow water vessels fitted with very long low frequency towed arrays and no other equipment. Specific mini submarines with surveillance equipment alone are also being manufactured. These platforms offer absolute low noise environments in which the sensors can operate and the platform is designed around the sensors which they are supposed to carry. The future maritime surveillance will definitely be having a significant amount of platforms which are primarily designed to be carriers of sensors.

4.4 Space Technology

Space technology has now reached a technological level where it can actively aid in the domain of surveillance and military engagements. Dedicated satellites for military surveillance were used by nations in the past years. Present systems have the capability of real time data communication using satellites to present a unified picture during a military exercise. Advanced navies have dedicated satellites which offer this capability where the entire fleet is always in complete connect with its commander in chief at all times. The major challenge in satellite based surveillance is in the automated data processing and analysis of the large volume of raw data which gets generated. Intelligent autonomous systems which have the ability to sort and sieve through this data and to make meaningful inferences are the key to making space based surveillance effective.

4.5 Network Centric Warfare

The Network Centric Warfare (NCW) for navy aims in interconnecting multiple naval platforms (including ships, submarines and aerial vehicles) and satellites using high speed network connectivity hardware and software to form an integrated wide area network (Figure 3). Sonar and Radar data collected by participating units are made available to other units in the network in real time. The focus is now on having various command, control, communications, computers and intelligence, surveillance, targeting and reconnaissance (C4ISTAR) programs. The Indian Navy has set off its transformation as a network centric force by installation of maritime VSATs (Very Small Aperture Terminals) in its ship and utilizing the GSAT-7 satellite.

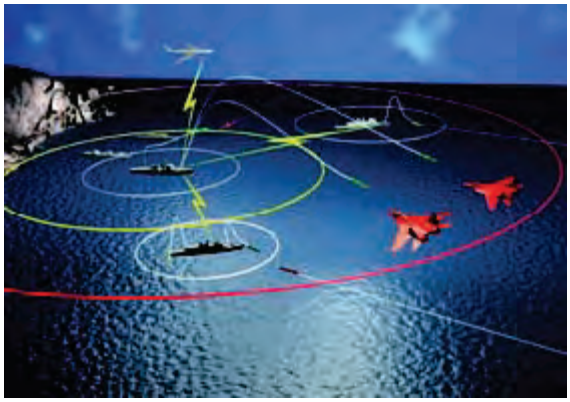


Figure 3. Network Centric Warfare

4.6 Deployable ASW Sensor Networks

The present day anti-submarine warfare (ASW) focuses on sensors fitted on ships, submarines and helicopters for surveillance. Large costs in procuring and maintaining platforms with ASW capabilities has led to migration of ASW tasks to cost effective off-board surveillance systems. Large sensor fields can be distributed without engaging multiple warships/submarines. These systems consist of multiple sensor arrays deployed on the sea bed which uses acoustic channel for communication and buoys with RF or satellite links. Multiple sensor nodes cooperate to perform data aggregation and data fusion. The target information is then communicated to the surface buoys which in turn transmit the same to shore station via RF or satellite links. Seabed array project executed by NPOL is India's first step in this direction.

4.7 Submarine Sonar Suites

Submarines no longer spend most of their time on deployment in the open oceans. Today, they are increasingly required to operate in shallow coastal waters, where the acoustic environment is complex and noisy. The shift in operating conditions calls for modular acoustic systems with very high levels of performance in order to provide submarines with the capabilities they need to perform their missions effectively and safely. One solution is to incorporate high-performance acoustic sensors, integrated processing electronics and advanced user interfaces. By combining subsystems such as bow-mounted sonar, flank array sonar, obstacle avoidance sonar, intercept sonar and passive towed-array sonar, submarines are provided with all-round situational awareness together with the ability to detect, locate and classify all types of threats at short, medium and long range across a broad spectrum of frequencies.

5. ELECTRONICS AS THE ENABLER FOR FORCE MULTIPLIERS

Technological innovations in electronics are the key drivers which have led to realization of the force multipliers described above. New age communication systems provide high bandwidth, reliable and long range communication make information sharing between systems possible and has led to distributed systems and Network-centric Warfare. Advanced embedded processors and rugged high performance boards have made significant computational resources available at reduced power and form factors which have enabled system architects to achieve greater levels of performance. Technology drivers of the present day like the philosophy and design based on "internet of things" make large scale sensor networks type of applications feasible. Unmanned Underwater Vehicles and low cost sensors for surveillance can now be realized without much difficulty and at a lower cost owing to advances in electronics.

6. SUMMARY AND CONCLUSION

State-of-the-art naval surveillance systems are inevitable to establish naval superiority in the waters which surround the Indian peninsula. Systems which leverage the advances in electronics and communication to synergize the various

elements of surveillance and provide force multiplier effects will give us an edge in safeguarding Indian interests in this region. A multi pronged approach of developing and deploying distributed systems, unmanned underwater vehicles, special surveillance vessels and underwater sensor networks along with equipping itself for Network Centric Warfare is the way ahead for Indian Navy to meet future challenges.

Acknowledgement

Authors are immensely grateful to Shri. S. K. Shenoy, Sc.'H', Director NPOL, for his support and encouragement.

References

1. Toshi Yoshihara and James Holmes, Chinese Naval Strategy in the 21st Century: the Turn to Mahan (London: Routledge, 2007);
2. Toshi Yoshihara, 'Japanese Maritime Thought: If Not Mahan, Who?' Naval War College Review, 59:3 (2006), pp. 23-51.
3. Don Aker, 'NUWC Newport - Providing undersea superiority for the Navy', UNDERSEAWARFARE, Issue No. 53, Winter 2014.
4. J.R.Benedict, 'Future Undersea Warfare Perspectives', JOHNS HOPKINS APL TECHNICAL DIGEST, volume 21, Number 2.

Radar as Force Multiplier for Land Systems – Indian Scenario

Rajesh Yadav[1]

Angela N M[2]

Shobha Verma[3]

Benjamin Lionel[4]

[1]Sc 'E', PO-II, DRDO HQ, New Delhi
[2] Sc 'G', LRDE, DRDO, Bengaluru
[3] Sc 'G', PO-II, DRDO HQ, New Delhi
[4]Sc 'G', Head PO-II, DRDO HQ, New Delhi

Abstract: *The military operations in the last 30 years have conclusively proved that no battle gains can be consolidated without "boot on ground". It has been established by the campaigns in Afghanistan, Iraq, Libya and Syria. The ground forces have a direct threat perception from 1 km up to 2.5 km and indirect threat from ranges beyond. Effective deployment and neutralization can be done only by detecting the location of various platforms that engage moving columns. Radars have proved to be basic ingredient aiding in the detection of these threats. This paper focuses on the various types of radars that have been developed for our armed forces and gives a future roadmap.*

1. Introduction

The ground forces in any combat zone face multiple threats from sniper fire to artillery and missiles. Human participation and intervention in modern field is indispensible. Technology advancements have helped to detect the incoming threats in time and neutralizing the same by launching suitable counter measure or evasion mechanism.

Ever since the invention of radars in 1935, it has proved itself to be a force multiplier by enabling the ground forces to detect the incoming threat, thereby enhancing their protection and survivability. This paper elaborates the various threats that are faced by the ground forces and the radars developed by DRDO and Industry partners for neutralizing the same.

2. Ground Based Radars

Threat perception of the moving ground forces is depicted in Fig 1. As can be seen the threats emerge from 1 km to 2500 km. The infantry and tank columns have a combat range of 2-3 km and the immediate threat is from the opposing ground forces.

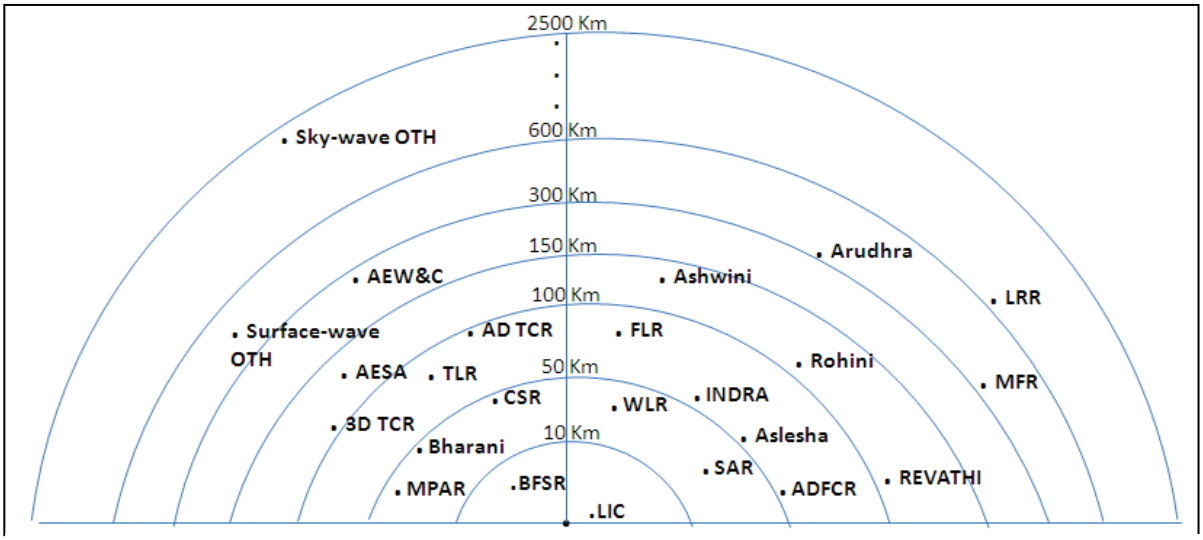


Fig 1. Threat Perception of the ground forces and various radars

Fig 2. Battery Field Surveillance Radar (BFSR)

2.1 Direct Threat Detection

Battery Field Surveillance Radar (BFSR) has got an operational range of more than 10 km and can detect even a soldier at a distance of 2 km. This enables the land forces to detect the first level of threat which can be neutralized by themselves or with support from the rear.

BFSR is portable radar for border surveillance and weights about 30 kg. It operates in X Band and the azimuth sector is settable from 30 deg to 180 deg. The radar is integrated with IR Sensors, networked and has self sustenance batteries. There is automatic target detection & classification. These radars have proved their performance in the field and have found export markets.

2.2 Low Altitude Threat Detection

The second layer of threat to the ground forces is from 5 km to 40 km from artillery, helicopters & UAVs. This threat can be detected and neutralized by Weapon Locating Radar (WLR), BHARANI and ASLESHA class of radars.

The Weapon Locating Radar (WLR) (Fig.3) has been primarily designed to locate guns, mortars and rockets. WLR in its secondary role can track and observe the fall of shot from own weapons to provide correction to own fire. Detection location and tracking Of requisite targets are handled by advanced algorithms and state-of-the art hardware. The Radar is in C Band and has range of 50 km for the required cone angle.

Fig 3. Weapon Locating Radar (WLR)

The Low Level Light Weight Radar – BHARANI is for surveillance in mountainous terrain against hostile aerial targets like UAVs, RPVs, helicopters and fixed wing aircrafts flying at low and medium altitude. The radar is transportable by vehicle, group of men and animal.

ASLESHA (Fig. 4), similar class radar in S Band, has semi active aperture antenna with full 3D capability using multi beam technology and has detection range of 50 km. It has modular design for easy transportability and quick assembly / dismantling.

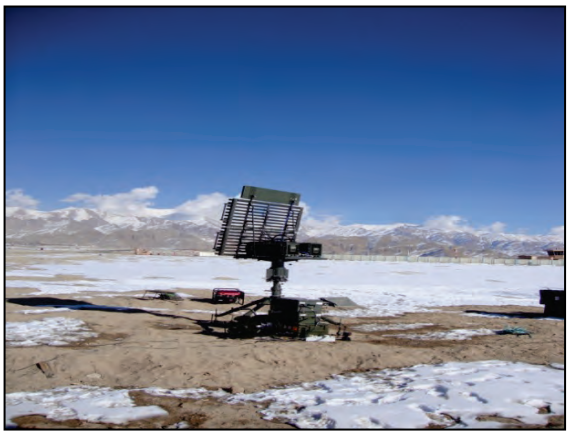


Fig 4. Low Level Light Weight Radar ASLESHA

2.3 Fighter Aircraft Threat Detection

The third level of threat is from fighter aircraft that can deliver bombs or missiles and have to be detected from 70 km to 150 km. This can be done by 3D Surveillance Radar – ROHINI (Fig. 5), 3D Tactical Control Radar and Low Level Transportable Radar – Ashwini. ROHINI is 3D surveillance radar in S Band and has single Cosec square transmit beam and 6 stacked receive beams. The 360 degree azimuth coverage is ensured.

Fig 5. 3D Surveillance Radar - Rohini

These threats need not be tackled/ handled by the front line columns as they can be neutralized effectively by the supporting segment from the rear.

2.4 Missiles Threat Detection

The next Level of threat from 150 to 300 km can be detected by Medium Power Radar-ARUDHRA and Multi Function Radar (MFR), and can be neutralized by long range missiles. ARUDHRA (Fig. 6) is fully active S Band 300 km range, rotating phased array radar with Digital Beam Forming Technology. The radar has both rotating and staring modes of Operation, scalable architecture and automatic target classification.

Fig 6. Medium Power Radar - ARUDHRA

Threats from 400 to 600 km range can be detected by Long Range Radars which have been realized for Air Defence against Ballistic Missiles. These radars have been integrated with the weapon systems. These sensors provide target data to missile which can engage / destroy the incoming enemy missile at various heights.

3. Fire Control Radars

The Fire Control Radars (Fig. 7 & 8) have applications for Army and Air Force. These fire control radars have been integrated with command and control centre, surveillance radar and missiles. The Fire Control Radars along with the Command & Control Centre for Air Defence Systems are in the use with the Armed forces. These radars are Multi Function Phased Array Radars having Target Search, Target Tracking, Missile Acquisition, Missile Tracking & Missile Guidance capability. These radars can handle multiple targets and multiple missiles simultaneously. These radars have played the role of seeker also as the command guidance codes are generated & uplinked to the missile from the radar itself.

Fig 7. Fire Control Radar – Troop Level Radar (TLR) for Army

Fig 8. Fire Control Radar – Flight Level Radar (FLR) for Air Force

The Air Defence Fire Control Radar (ADFCR) for Guns has four sensors (i.e. Surveillance radar in X Band, Fire control Radar in Ka Band, IFF and Electro-Optic System) integrated on the same platform.

The Radar for Quick Reaction Surface to Air Missile (QRSAM) can search and track targets on the move & fire weapon on short halt.

4. Airborne Radars

The Airborne Radar viz. Airborne Early Warning & Control (AEW&C), Maritime Patrol Radar (MPAR) for Advanced Light Helicopter (ALH) and Synthetic Aperture Radar (SAR) for UAV have been developed. Active Electronically Scanned Array Radar (AESAR) for Fighter Aircraft and other airborne radars aid the land based systems in destroying the enemy targets. The target information from these sensors can be sent to the command & Control centre for assigning target to the appropriate firing units.

5. Low Intensity Conflict (LIC) Radars

Radars for LIC applications viz. Coastal Surveillance Radar (CSR), Ground Penetrating Radar (GPR) (Fig. 9) and Through Wall Imaging Radar (TWIR) (Fig. 10) are other indigenous products. The Coastal Surveillance Radar (CSR) is for 24x7 detection & tracking for low RCS boats in dense multi target scenario against sea clutter background. These radars are in dual band (X band & S Band). The normal operation is in X Band while in bad weather conditions the radar operates in S Band.

Ground Penetrating Radar (GPR) is for the real time detection of buried targets viz. Anti Personnel Mines (APM), Anti Tank Mines (ATM) and Improvised Explosive Devices (IED). GPR can detect targets buried in various terrains viz. Sand, Red soil, Laterite, Black Cotton.

Through Wall Imaging Radar (TWIR) is for detecting, locating and monitoring humans behind walls during hostage rescue. This radar is both Hand Held & Tripod Mounted. GPR & TWIR uses the Ultra Wide Band (UWB) Technology.

Fig 9. Ground Penetrating Radar (GPR) – Hand Held and Vehicle Mounted

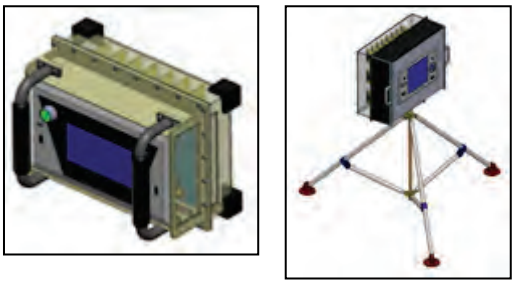


Fig 10. Through Wall Imaging Radar (TWIR) – Wall Mounted and Tripod Mounted

6. Future Radar Systems and Technologies

6.1 Active Protection System (APS)

Modern tank systems have developed heavy 'passive armour' and also ERA (Explosive Reactive Armour) to defend themselves from the various projectiles. However, considering the heavy weight penalty, focus is now on to develop effective countermeasures to neutralise the incoming very high speed projectiles. APS uses radar to detect the incoming threat of very low

cross section from 500 m and the onboard defence suite launches a countermeasure that impacts the incoming projectile before it reaches the tank.

6.2 Over-The-Horizon (OTH) Radar

The Over-The-Horizon (OTH) Radar is categorized as Sky wave Radar & Surface wave radar. The Sky-wave radars are dependent on ionosphere for its operation while Surface-wave radar uses the surface-wave mode of propagation.

6.2.1 Sky wave Radar

Over-The-Horizon (OTH) Skywave radar provides vast coverage and has the ability to survey inaccessible regions (i.e. mid-ocean). However, the real estate demand and cost of operation and manning is high. The performance of the Skywave OTH Radar is dependent on the ionosphere. This region is at heights between 50 km and 350 km. The Skywave OTH radar uses HF band to bounce radio signals from ionosphere and receives back the signal from reflecting surfaces. The information about the ionosphere in real time is of primary importance because of the choice of frequency of operation. The Skywave OTH radar can provide surveillance up to 3500 km but the skip zone limit for these systems is 350 km.

6.2.2 Surface Wave Radar

The High Frequency Surface Wave OTH Radar utilizes the surface-wave mode of propagation and operates in the frequency band of 3-30 MHz. The surface waves propagate efficiently in vertical polarization and the signal attenuates directly as function of range, frequency and surface roughness. It requires a conducting surface, i.e., Saline Ocean for propagation [4]. The radar detection range is dependent on the frequency of operation, radiated power, ship size and environmental conditions. The radar signal attenuates as the radar frequency is increased, or if the sea state increases. The Surface wave radars have range up to 400 km range.

6.3 Multi Static Air Defence Radar

Multi Static Air Defence Radar (MSADR) for detecting targets employing stealth technology is a future requirement. The systems can have Bi-static and Multi-static radar configurations.

6.4 Foliage Penetration Radar (FOPEN)

In recent times, our country has been a victim of low-intensity conflicts of various types, threatening the homeland security. In order to counter the anti-national activities that use foliage as an effective means of concealment, there is need for an airborne sensor that can penetrate foliage and provide wide area surveillance of forestry areas and detect stationary objects hidden under the foliage cover. These radars are generally in L-Band, as in this frequency band the penetration is possible through the foliage.

7. Conclusions

The traditional Line of Sight (LOS) microwave radars are limited to the maximum range of 50-60 km. The surveillance can also be done by airborne microwave radars, but these airborne systems provide only a snap shot in time of activity within the area and operational costs are very high. The Sky-wave OTH radar can provide surveillance from 350 km to 2500 km and Surface wave OTH radar up to 400 km. Therefore, in order to provide complete surveillance all the radars are required. Moreover, these radars should be integrated to provide a fused picture at the command & control centre for suitable action.

Acknowledgements

The above products are an outcome of significant contributions of innumerable scientists and staff of Electronics and Radar Development Establishment (LRDE), Bangalore and their industrial partners. The authors are thankful to Ms J Manjula, DG (ECS) and Shri S S Nagaraj, Director LRDE for giving permission to publish this work.

References

1. Bassem R. Mahafza, "Radar Systems Analysis and Design Using MATLAB", Chapman & Hall/CRC, USA.

2. M.I. Skolnik, Introduction to Radar Systems", 2nd Edition, New York: McGraw-Hill, 1980.

3. Surface Based Air Defense System Analysis by Robert H.M. Macfadzean.

4. Anand Manikutty, Shashidhar Merugu, G. Manimaran, C. Siva Ram Murthy, "DREAD: Distributed Real-Time Air Defense System", 5th IEEE Int'l Workshop on Parallel and Distributed Real-Time Systems (WPDRTS) Geneva, Switzerland, April 1-3, 1997.

5. Anthony M. Ponsford, Jian Wang, "A review of high frequency surface wave radar for detection and tracking of ships", Turk J Elec Eng & Comp Sci, Vol. 18, No. 3, 2010.

6. Levent Sevgi, "Modeling and simulation strategies in high frequency surface wave radars", Turk J Elec Eng & Comp Sci, Vol. 18, No. 3, 2010.

Fighter Aircraft and Advanced Technologies as Force Multipliers

Vijay Kumar Sutrakar
Scientist –'D'
Aeronautical Development Agency, Bengaluru.

Abstract: *In this paper, at the outset the term 'force multipliers' is defined with respect to a fighter aircraft. Next, the concept of a futuristic complex combat scenario involving fighter aircraft is described. The various missions performed by fighter aircraft are then examined. Subsequently, it is shown as to how the aiding platforms and electronics could help the fighter aircraft in generating mission plans and their successful completion. Finally, the advanced technology developments and correspondingly the intelligent concepts of operations that could become pivotal elements in futuristic complex combat environment are discussed in terms of advanced platforms, precision weapons, advanced sensors and advanced information technology.*

1. Introduction

Ever since man has mastered the art of flying, fighter aircraft has always been a dominating factor in wars. Conflicts of the past have repeatedly demonstrated that the success of any major military operation depends on the ability of a force to achieve air superiority as swiftly and as effectively as possible and sustain it till the end of the conflict. Establishing air superiority is therefore an absolute prerequisite to attain success in future conflict scenarios too. In this direction, the present day fighter aircraft are coming up with multi role capabilities, i.e. air-to-air and air-to-ground for obtaining air superiority that would help them destroy enemy Air Defence Systems (ADS) and various valuable assets in an efficient way. These modern aircraft would also be able to swing the role (from air-to-air to air-to-ground) during the same mission. These combat missions entail significant penetration into enemy territory and consequently, a huge amount of threat. Ensuring survival, within adversary airspace, is of paramount importance. Apart from this, the success of a mission in a future complex war scenario would not only depend on the capabilities of a fighter aircraft alone, it would also heavily depend on the capabilities of supporting platforms and their systems; smart weapons and sensors; and the smart supporting facilities.

2. Force Multipliers:

The definition as per the United States DoD is "A capability that, when added to and employed by a combat force, significantly increases the

combat potential of that force and thus enhances the probability of successful mission accomplishment" [1]. The stated capability could be other fighters, unmanned platforms, advanced warning systems, radars, satellites, and associated systems, weapons, communications facilities etc.

Fighter aircraft along with other aiding platforms and their systems, smart weapons and sensors need to be coupled with supporting communication facilities in a judicious way for achieving high chances of success in a future combat. In order to couple the above platforms and systems, it is important to generate a futuristic complex combat scenario, as discussed next.

3. Futuristic Combat Scenario: The approach of System of Systems (SoS), binding together the *operative system* and the *force multiplier system*, is the future scenario of air warfare, as shown in Fig. 1[2]. This architecture consists of a 'front end' which is the '*operative system'* supported by a host of nodes/platforms that constitute a '*force multiplier system' (sometimes referred to as the cooperative system)*. In general, the *operative* segment consists of direct involvement of aerial platforms, both manned and unmanned apart from precision guided and unguided weapons. On the other hand, the *force multiplier* segment normally consists of tankers, Airborne Early Warning & Control (AEW&C), Intelligence, Surveillance, and Reconnaissance (ISR) aircraft, Signal Intelligence (SIGINT) aircraft, Electronic Warfare (EW) aircraft, Ground Control Stations and satellites. The effective utilization of the *operative systems* coupled with the *force multiplier systems* could only be possible with an advanced information technology network. This coupling requires a high bandwidth, secured jam resistant operational data links in conjunction with control stations thus enabling net-centric operations.

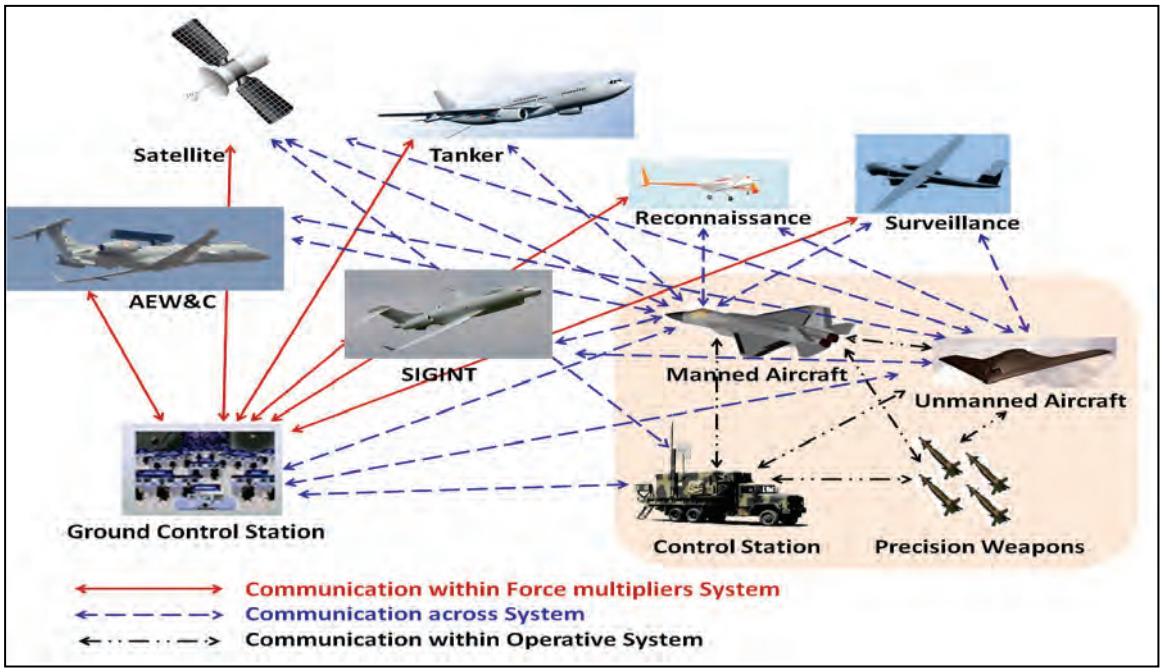


Fig. 1 : A futuristic scenario consisting of force multipliers and operative systems.

4. Fighter Aircraft Missions: A fighter aircraft would be required to perform both air-to-air and air-to-ground missions for achieving air superiority. These missions could either be offensive or defensive depending upon the role an aircraft needs to perform. The typical missions are [3]:

4.1 Combat Air Patrol (CAP): In this mission, aircraft performs patrolling for point and area defence.

4.2 Intercept: In this mission, an aircraft performs air to air interception of enemy aircraft.

4.3 Escort: In this mission, a strike aircraft is being protected from enemy aircraft by escorting it up-to the designated target without being attacked by the enemy aircraft.

4.4 Suppression/ Destruction of Enemy Air Defence (SEAD/DEAD): In this mission, aircraft reduces the enemy air defence assets by destroying radars, surface to air missiles (SAM) and anti-aircraft artillery (AAA).

4.5 Strike: It is an air-to-ground mission flown against a vast variety of enemy targets. During a strike mission it is ensured that the aircraft hits the assigned target or at least reduces the operational status of the enemy assets significantly. This mission could also be **Deep Strike**, if the aircraft penetrates deep into the enemy territory for destroying the high value enemy assets. Some of these typical missions are described next, in some detail, along with the force multiplier elements in order to illustrate the point.

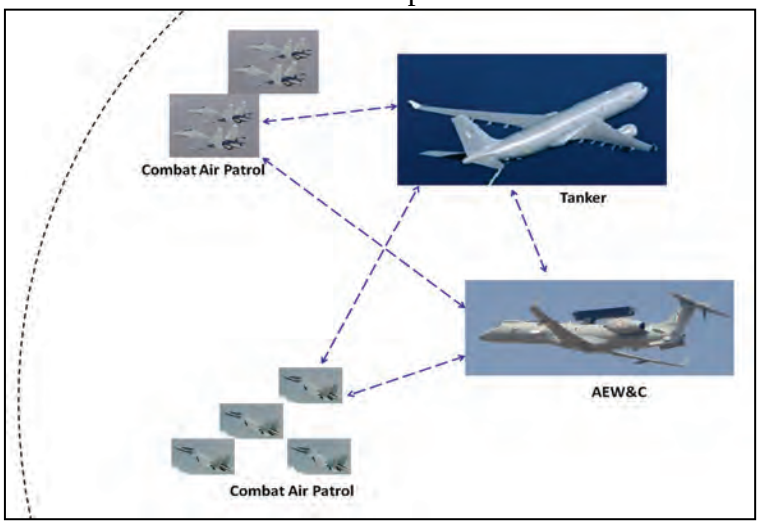


Figure 2. A Typical CAP mission and its force multipliers

5. Force Multipliers for Fighter Aircraft:

5.1 Scenario - I: In a **CAP** mission, where the aircraft needs to protect High Value Assets and targeted areas, it may be required to fly for a long duration which requires aerial refuelling. In order to perform this mission a tanker needs to be positioned for air to air refuelling of the aircraft performing the **CAP** mission, as shown in Fig. 2. It is also important for the tanker to continuously obtain the fuel status of the other aircraft performing the mission. This would be helpful for the tanker to position itself at an appropriate location for performing the aerial refuelling both during the day as well as night Operations.

In order to position the tanker at the appropriate location, it would also be important to know the

exact locations of the aircraft performing missions. In order to continuously update the locations of the aircraft and tanker, an AEW&C (or could be done via ground control station) would need to be positioned, as shown in Fig. 2. It is evident, from the above discussion, how several platforms could be networked to make the mission successful and in addition, the significance of continuous and effective communications between the operative system and the force multipliers system.

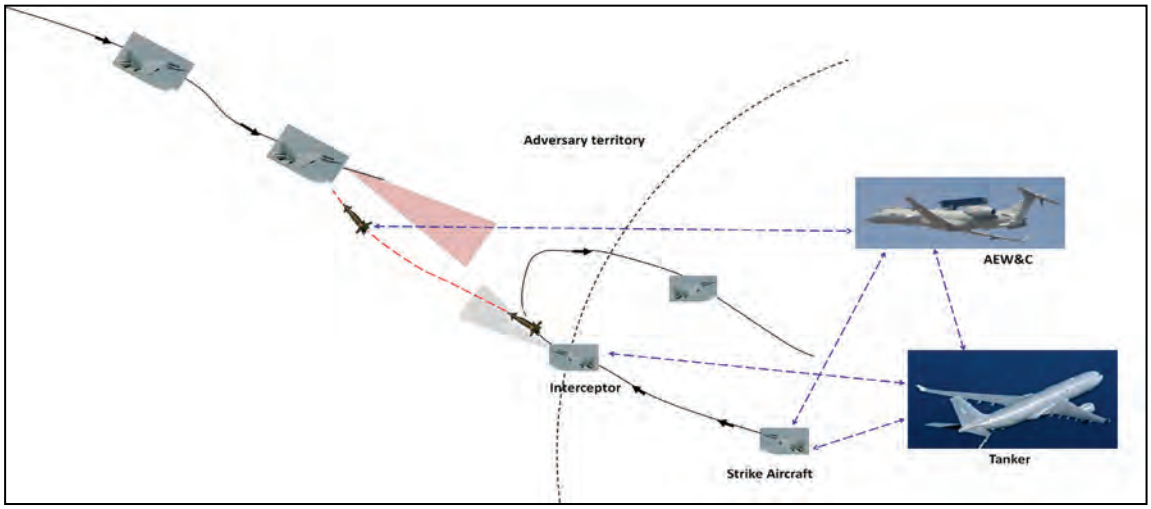


Figure 3. INTERCEPTOR missions and associated force multipliers.

5.2 Scenario - II: In this scenario, **Interceptor** missions are discussed, as shown in Fig. 3. In a case, where an adversary aircraft is approaching, an interceptor could be vectored either by AEW&C or ground stations. If it is assumed that both the aircraft are having the same capabilities and same weapons, then the chances of survivability are limited. In such cases, an AEW&C could be linked with the interceptor aircraft and it would pass the information to the interceptor about the adversary aircrafts. The interceptor aircraft would be radio silent and rely on the AEW&C for target information and it can vector the interceptor in a favourable location for combat. The red shaded region shows the detection capabilities (high detection range) of adversary aircraft. The gray shaded region shows the stealth capabilities (low detection range) of the interceptor. It is assumed that both the adversary as well as interceptor has the similar radar (mounted on the nosecone of the aircraft) capabilities. It can be seen that, being stealthy, the interceptor could destroy the approaching adversary aircraft very efficiently.

5.3 Scenario - III: A **Strike** mission, where the aircraft is flying on an air-to-ground mission, with the potential to destroy a vast variety of ground targets, is shown in Fig. 4. A strike fighter aircraft, that is deployed to destroy adversary ground targets, needs to penetrate into the enemy air defence space. Each of these combat missions entails a huge amount of threat and consequently, ensuring survival within the adversary airspace becomes more challenging. In order to increase the survival rate, the strike aircraft must have low radar signature and could further go radio silent. The Communication of strike aircraft could be linked with an AEW&C or satellite for transferring the information of locations via data

link. IRS aircraft could also be utilized for providing the details of the adversary assets to AEW&C. The AEW&C would in turn update the strike aircraft with the locations of high value assets as well as the locations of air/ground threats, if any. The strike aircraft, would then release the precision weapons onto the designated targets, at the appropriate time and location from a stand-off distance. Strike aircraft may also require aerial refuelling for higher reach, i.e., for increasing radius of action (RoA), where refuelling needs to be carried out in non hostile territory.

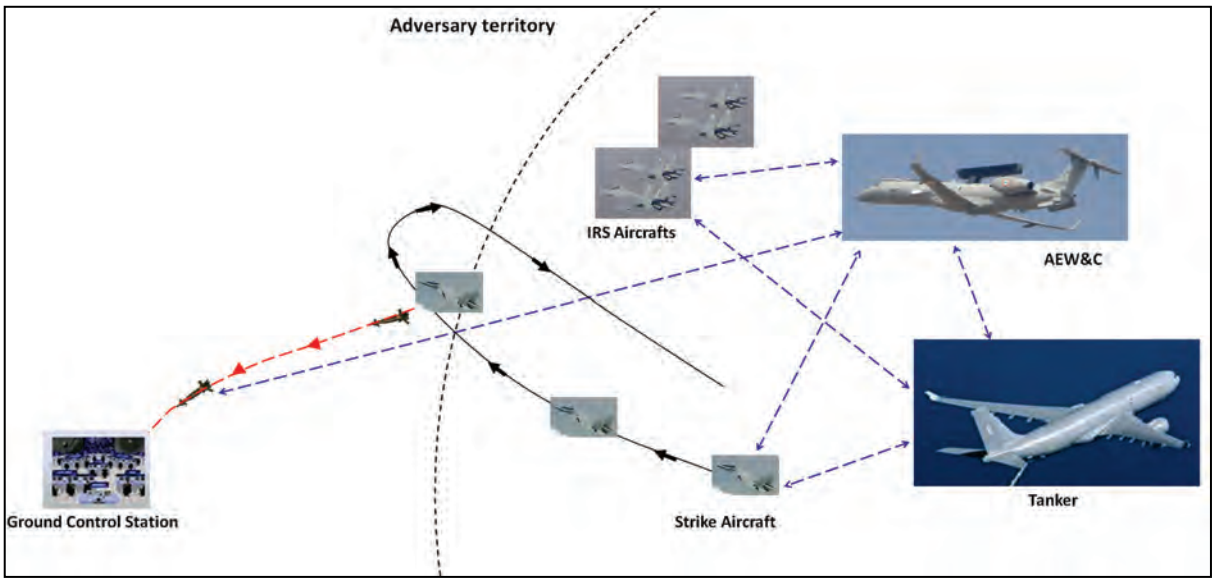


Figure 4. A Typical STRIKE mission of fighter aircraft and its force multipliers

In all the above scenarios, it is very clear that the advanced platform with low signatures (i.e., stealthy aircraft), precision weapons, advanced sensors, and advanced electronics for transforming/transferring information across various force multipliers would drive the future air combat. The advancement of technologies, combined with smart concepts of operations, could become the pivotal element of futuristic air warfare. In the recent past, a large number of advanced technologies such as stealth, precision stand-off attack and enhanced information have been evolving and are also being adapted to operational requirements. Present aerospace technologies either proven or on the horizon promise to generate even more dramatic changes in the futuristic air warfare [4]. These technologies could be broadly categorised into (a) advanced platforms; (b) advanced Pilot Vehicle Interface (PVI); (c) precision weapons; (d) advanced sensors; and (e) advanced information processing.

6. Advanced Platforms

The Advanced Platforms constitute the next generation whose design is driven by low observable (LO) capabilities. The survival of LO aircraft is enhanced because of their low detectability and use of threat avoiding tactics such as flying at night or in rough weather. The LO aircraft can fly at very high altitude for minimizing the risk of detection from surface to

air missiles (SAM) and anti-aircraft artillery (AAA)[4].

7. Advanced PVI

As warfare scenarios are becoming more complex, cockpit of fighter aircraft is getting flooded with information from the on-board sensors and off-board sensors and the time available for the pilot to make decisions is getting compressed. Advanced PVI generally consists of Large Screen Multi Functional Display (LSMFD) with situation based reconfigurable and interactive display pages. Advanced PVI reconfigures LSMFD and controls the demands of pilot for presenting important information in an effective manner. In this direction, Pilot Associate (PA), i.e., a co-operative knowledge based system to help the pilot to make decisions in battle space, is emerging. It is an intelligent associate system that supports real time planning and decision making in dynamic and evolving tactical situations by recommending action plans. The PA consists of system status monitoring, mission planning and tactical planning, enhanced situational awareness through integration of multiple sensor data and its presentation on LSMFD.

8. Precision Weapons

Precision weapons are having many-fold increase in destructive power, as compared to the unguided weapons. These precision weapons need to have near-zero miss distance accuracies. Also, they could be designed and built smaller in size. These systems include Precision Guided Munitions (PGMs) and Joint Direct Attach Munitions (JDAM). Advanced PGMs would have sensor fused smart weapons that would be able to recognize, identify, and sort targets even as their sensors guide them; achieving accuracies in centimeters rather than meters. There is also advancement on disruptive weapons, such as energy (lasers and high power microwave bursts), electrons (directed radio frequency energy), and deception are progressing. High power microwave and laser weapons may work in tandem with or replace many traditional explosive weapons. They may, for example, penetrate an enemy fighter cockpit, illuminate the fire warning light, shut down digital engine controls, or make other surreptitious inputs like penetrating flight controls and forcing an un-commanded break turn. It would also help for destroying formation integrity and make the enemy predictable [4].

9. Sensors

The information for generating battle-space awareness in Net Centric Warfare (NCW) is provided by numerous sources, for e.g. stand-alone intelligence, surveillance, reconnaissance platforms, sensors employed on weapons platforms or human assets on the ground. In the fundamental shift to network-centric operations, sensor networks emerge as key enablers of increased combat power. The operational value or benefit of sensor networks is generally derived from their enhanced ability to generate more complete, accurate, and timely information than can be generated by platforms operating in stand-alone mode. Networked sensors have several advantages including decreased time for engagement, increased ability to detect low signature targets, improved track accuracy and continuity, improved target detection and identification and reduced sensor detectability to the enemy [5].

It is important for understanding sensor management to manage, coordinate, and organize the use of scarce and costly sensing resources in a manner that improves the process of data acquisition while minimizing the threat due to radiation of sensors from various platforms. It is also important to understand the problem of how to dynamically manage and control the emission of active sensors in multiple platforms to minimize the threat posed to these platforms in combat situations. Due to widespread use of sophisticated networked sensor platforms, there is increasing interest in developing a coordinated approach to control their usage to manage the emission and threat levels [6].

Emission management/control is emerging in importance due to the essential tactical necessity of sensor platforms satisfying a low probability of intercept (LPI) requirement. This LPI requirement is in response to the increase in capability of modern intercept receivers to detect and locate platforms that radiate active sensors. The emission management/control system needs to dynamically plan and react to the presence of an uncertain dynamic battlefield environment. The design of an emission control system needs to take into account the following subsystems [6]: (i) *Multiple Heterogeneous Networked Platforms of Sensors*, (ii) *Threat Evaluator, and* (iii) *Sensor Manager*. With minimum communication overheads over the network, the platforms can dynamically regulate their emission and hence decrease their threat levels. As a result the bandwidth in the network can be utilized for other important functionalities in NCW.

10. Information Technology

The tenets of NCW are [6]: (1) a robustly networked force improves information sharing; (2) information sharing enhances the quality of information and shared situational awareness; (3) shared situational awareness enables collaboration and self-synchronization, and enhances sustainability and speed of command; and, (4) these, in turn, dramatically increase mission effectiveness.

The technology supporting NCW is inherently complex, but not significantly more so than the technology used to digitize and network the civilian world. It must however be more resilient physically, thermally, electrically and be better resistant to hostile penetration, and in wireless systems, hostile jamming. The prerequisite for an NCW capability is the digitization of combat platforms. A combat aircraft with a digital weapon system can be seamlessly integrated in an NCW environment by providing digital wireless connections to other platforms. Without the digital weapon system, and its internal computers, NCW is not implementable.

Provision of digital wireless connectivity between combat platforms, is a major technical challenge which cannot be understated. The followings are the key parameters that could create problems for providing military networking [7]: (a) Security of transmission, in terms of robust encryption. Also, even if a signal cannot be successfully decrypted, its detection provides an opponent with valuable information on the presence, position and often activity of the platform or unit in question. (b) Robustness of transmission, during solar flares, bad weather and hostile jamming, networks must continue to function. (c) Transmission capacity. (d) Message and signal routing to specifically address and access other platforms or systems in a networked environment. (e) Signal format and communications protocol compatibility. It is

essential that dissimilar platforms and systems can communicate in a networked environment.

A large number of signal formats and protocols have been used extensively in the current and legacy aircraft [7]. A case study of air to air combat with and without Link 16 is discussed here [8] for demonstrating the usefulness of network centric operation as an example. In this case study, the framework of Joint Tactical Information Distribution System (JTIDS) is examined utilizing the performance of tactical fighter aircraft (F-15s) equipped with Link 16 data communications terminals. It is found that F-15s equipped with Link 16 is significantly more effective in air combat than F-15s equipped with only voice communications. Pilots are able to improve execution of air combat tactics by taking advantage of their increased awareness, as well as the increased time they had available for decision making. This improvement in tactics execution is enabled by the increased information and decreased time required for information gathering in Link 16-equipped force packages as compared to only voice communications. The improved tactics could be (a) an increased number of engagements in the same time period; (b) deploy as combatant rather than defensive patroller; (c) earlier and more accurate vectoring to engage the enemy aircraft from position of maximum advantage; and (d) employment of co-operative formations to trap and destroy the enemy aircraft [8].

11. Conclusions

In this article, an attempt has been made to define the concept of a futuristic complex combat scenario for fighter aircrafts and its force multipliers. Typical missions of fighter aircraft are discussed and few scenarios are presented. These scenarios captured the possible needs of future development of fighter aircraft and associated technologies (in terms of advanced platforms, precision weapons, advanced sensors, and advanced communications). Finally, the advancement taking place across the globe, in terms of aircraft platforms, precision weapons, sensors and information technology are discussed. The paper also suggests the possible technology area that needs to be focused for succeeding futuristic complex combat scenario efficiently.

Acknowledgement

The enthusiastic support and guidance received from Shri C D Balaji, Programme Director (CA) and Director, ADA, Dr. A K Ghosh, Outstanding Scientist and Project Director (Advanced Medium Combat Aircraft), ADA, and Mr. J V Kamesh, Scientist 'G', ADA and other team members of AMCA Directorate are gratefully acknowledged.

References

1. Dictionary of Military and Associated Terms, US Department of Defence, 2005.
2. P S Subramanyam, Technology Challenges in Future Fighter Aircraft Development, 65th Annual General Meeting, AeSI, November 2014, Hyderabad, India.
3. John Paterson, Measuring Low Observable Technology's Effects on Combat Aircraft Survivability, American Institute of Aeronautics and Astronautics, Inc. 1997, 1-16.
4. Benjamin S Lambeth, Technology and Air War, Air Force Magazine, November 1996, 50-53.

5. G Gagnon, Network-centric special operations–exploring new operational paradigms. Air and Space Power Chronicles, February 2002.
6. Vikram Krishnamurthy, Emission Management for Low Probability Intercept Sensors in Network Centric Warfare, IEEE Transactions on Aerospace and Electronic Systems, January 2005, 41, 1, 133-152.
7. Carlo Kopp, Understanding Network Centric Warfare, Australian Aviation, January/February 2005
8. Daniel Gonzales, John Hollywood, Gina Kingston, David Signori, Network-Centric Operations Case Study, Air-to-Air Combat With and Without Link 16, RAND National Defense Research Institute, Santa Monica, CA, 2005.

Airborne Surveillance in a Network Centric Context



Dr. Michael Wiedmann **Dr. Uwe Wacker** **Reiner Zimmermann**

Airbus Defence & Space GmbH, Ulm, Germany

Abstract: *Surveillance in a Network Centric Surveillance Context and the contributions of Airborne Surveillance will be discussed. The sensed environment, the sensors to be used, the determination of track objects, the classification, identification and threat evaluation for tracks and some aspects of SW engineering will be addressed.*

1. Introduction

The goal of surveillance is to detect all Objects of Tactical Interest in a given Surveillance Volume and to determine their state accurately and reliably. Depending on the task at hand Objects of Tactical Interest will be:

- Airborne objects such as manned aircraft, helicopters, and unmanned vehicles. Such objects will be called to exist in the "Air Environment".
- Surface objects such as commercial vessels, military ships, other boats or floating objects either manned or unmanned. Such objects will be called to exist in the "Surface Environment".
- Sub-surface objects called to exist in the "Sub-surface Environment". Sub-surface objects will not be discussed further.
- Ground objects such as civil and military vehicles and installations of tactical interest on the ground. Such objects will be called to exist in the "Ground or Land Environment".
- Objects in the "Space Environment" will not be further discussed.

The determination if an object class of a certain Environment is of tactical interest depends on the surveillance task at hand.

The Surveillance Volume depends as well on the surveillance task. It could be as restricted as a volume extended a few km around a ground site or as large as the space covering a country including its immediate neighbors or a continent.

Objects of Tactical Interest are to be detected whenever they reside in the Surveillance Volume. Their state to be determined comprises but may not be limited to: location, kinematic behavior, directly sensed attributes such as size, attributes derived from replies or emissions originating in the object, attributes derived from the behavior of the objects and their adherence to known models, rules or tactical regulations.

The Surveillance System has to determine the Environment, the Kinematics, the nature/ Classification and the affiliation/ Identity, the intent/ Threat of all objects. The term accuracy relates to numerical attributes such as location, speed, or heading. Such parameters need to be determined accurately enough to allow the determination of derived attributes such as adherence to tactical regulations or Threat. To use such derived attributes for Classification, Identification or Threat Analysis a certain degree of Reliability of these attributes must be assured. Such parameters need to be a reliable basis to allow the correct interpretation of the tactical situation, to decide on defensive actions or to control coordinated counter activities, as applicable.

The availability of a consistent Situation Picture across agencies is a vital pre-condition for effective decision making. Sensors using different physical principles and reporting regimes will be used to obtain "surveillance observations" about Objects of Tactical Interest in the sensed environment. Such sensors will include:

a.) Active Primary Surveillance Radars illuminating objects with their radiated electromagnetic energy. They are capable of detecting even non cooperative objects by actively illuminating the object.

b.) Secondary Surveillance Radars operating on replies of cooperative objects.

c.) Passive Radars where the illumination of the objects comes from other sources of electromagnetic energy. They provide just a receiving and signal processing capability to detect even non cooperative objects.

d.) Optical Sensors make use of a wide range of the electromagnetic spectrum. They operate on light in various frequency ranges as radiated and/or reflected from the surface of objects.

e.) Sonar Sensors which operate on radiated or reflected sound energy, mostly used under water but as well used in air.

Sensors may be located in space carried by various types of satellites, on airborne manned or unmanned platforms, on land, on the surface of the water or under water. Other types of sensors and systems report on either non-cooperative objects or on cooperative objects. All of these sensors will report in near real-time observations about the "detection" of objects in the surveillance volume and in addition they may report "attributes" such as signal strength or size of the object or codes which are provided by a cooperative object. Real-time in this context will be defined as to provide an observation fast enough while the object has not substantially changed its state. The Surveillance systems will synthesize a situation picture from the surveillance observations. Track representations are created for objects of persistence while nuisance observations are suppressed to "clean or de-clutter the view" on the situation. Depending on the surveillance task at hand either individual sensors or a "layered network of complementary sensors" will be used in order to both create a track representation for every tactical object of interest. Modern surveillance systems will associate the sensed situation picture with prior knowledge such as general situational knowledge, object models, mission plans, thematic maps, libraries comprising characteristics/ attributes in order to assist human operators in the correct interpretation of the situation picture. Providing such functions in automatic data processing systems has the advantage that computers "don't get tired" and they can browse databases much faster and with better hit rates than human operators. Routine work will be off-loaded to computer systems. However, human operators have still a leading edge in the correct and fast interpretation of behavioral patterns and

incomplete, vague or cluttered information. This is why "easy to understand" user interfaces with sufficient "explanation capabilities" are essential for operational interaction. Complex surveillance systems will comprise large amounts of Software. Powerful SW engineering approaches are vital for the practical usability of such systems.

The requirements allocated to Surveillance systems could be summarized as: "**maintain a unique, identified, and classified Track with an impact assessment for every Object of Tactical Interest for as long as the object exists in the Surveillance Volume using both all available sensor observations and all available background knowledge**".

Quantitative requirements to surveillance systems such as probability of detection, track coverage of target trails, track continuity, track uniqueness, track accuracy, and confidence into the classification, identification and threat assessment are used to measure the effectiveness of the surveillance functions.

2. Sensed Environment

In this article, generally the definition of the levels of data fusion as published in the Joint Directors Laboratory (JDL) model is followed. Figure 1 shows a simplified version of such model.

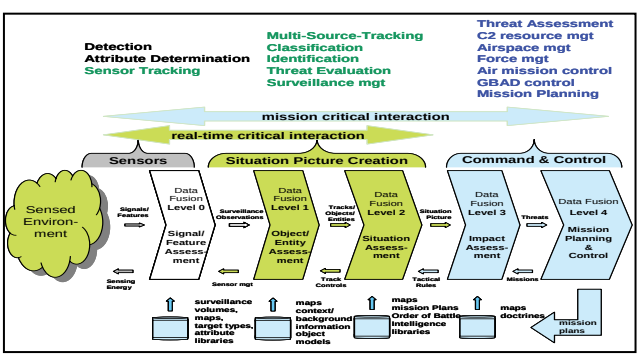


Fig. 1. **Simplified version of a Joint Directors Laboratory (JDL) model of Data Fusion Levels applied to an Air Surveillance task.**

JDL Models were initially published by the US DOD in 1988, by Alberts, Garstka, Stein [1], and were later updated and modified several times; see a later version by Steinberg, Bowman, White [2]. The original document may be subject to ITAR restrictions. Therefore the simplified version is based on articles published later in the open literature.

The Sensed Environment comprises the Objects of Tactical Interest. These Objects in which the surveillance functions are interested in are intermingled with other objects which may exist in the volume to be monitored. Further, the Sensed Environment comprises the propagation environment for signals in space.

3. Sensors and Sources

In Data Fusion Level 0, sensor systems attempt to detect all objects in the Sensed Environment and to determine their kinematic and, as applicable, their non-kinematic attributes such as SSR mode codes, ESM signal characteristics, size/ extension of the objects as determined by optical and/or Synthetic Aperture Radars etc. Sensor systems may comprise a local tracking function to control their spatial and temporal sampling sequence. The goal is to "keep permanent eye" on interesting objects and to adjust the beam-form, the detection waveforms and the processing to their movement and behavior.

4. Tracking

Sensors provide a sequence of surveillance observations which are in the best case sufficient in sampling rate, accuracy and attribute reliability to follow an object's movement and its capability to change its detectable characteristics. The Data Fusion Level 1 Tracking Functions will create a persistent model/ track for every object in the Sensed Environment from the Surveillance Observations. In many cases a single sensor may not be sufficient to maintain a track of every object. In such cases a set of complementary

sensor systems may be needed. Such complementary sensors may be distributed at individual locations, they may apply different physical measurement principles and they may use specific reporting rates. The sensor mix needed to maintain a persistent track on all Objects of Tactical Interest depends on the type of objects and their maneuverability, the environment and on the capabilities of the individual sensors to detect the objects, to determine their characteristics and to provide reports to a Command and Control capability.

Complex surveillance systems use "Multiple Models" concurrently and finally tell out a state estimate mixed from the individual model contributions to cover the complex behavior of the objects to be followed. Traditionally the models are mainly based on kinematic considerations. For example, one model uses heavy smoothing of measurement outliers whereas another model may assume more frequent object maneuvers. In additions, we will see in the future models variations based on attributes as well. For example, if we can safely assume from the classification functions that a track model represents a commercial airliner, then high maneuvering models used for highly maneuverable aircraft are not needed in a mix of models. Traditionally complex surveillance systems have used a Multiple Hypothesis design to allow different hypotheses for the association of surveillance observations to a given track. Such Multiple Hypothesis tracking algorithms are traditionally based on kinematic deviations between the predicted states of objects to be followed and the measurement deviations of surveillance observations. In addition, we will see in the future hypotheses based on attributes as well. If we can safely assume from the classification functions that a track hypothesis represents a commercial airliner then association hypotheses which would associate ESM observations which carry the signal characteristics of a military aircraft model don't fit with this type of object.

5. Determining Tactical Track atributes

In the Data Fusion Level 2 functions, an assessment of the overall track situation is made. The nature of the track objects is classified and their affiliation is identified. (Note: we apply the definition of Classification and Identification according to NATO STANAG rules [3]). The STANAG 1241 states: "There are many elements of information which contribute to the assessment of the degree of threat of a platform. While assigning an order to these elements, it is clear that circumstances alone will dictate which elements are available and the order in which they become available." The result of this process is the assessed Situation Picture in the monitored surveillance volume.

The subsequent Data Fusion Level 3 will determine the impact which an object may have on own assets. This level may provide functions to manage defensive actions to mitigate threat.

6. The use of Prior Knowledge

The Data Fusion Level 4 functions will "refine the surveillance and situational assessment process". General background knowledge about the situation to be monitored, geospatial information models about the kinematic behavior of objects, models of the "visibility" of objects including their non-kinematic characteristics, models of the physical processes involved in the signal propagation in space and the detection of signals, mission plans for own tactical objects, intelligence information including an order of battle status, the structure and nature of the surveillance volume, the location and characteristics of own assets, the availability and capability of own defensive forces will be assembled and maintained to support the various stages of the Data Fusion processes.

7. Real Systems and the JDL Model

Obviously no real surveillance system will implement all levels of Data Fusion as mentioned earlier. Real systems may not strictly follow the functional separation as indicated by the Data Fusion levels 0 through 4. However, the JDL model as stated in [2], "developed in 1985 by the U.S. Joint Directors of Laboratories (JDL) Data Fusion Group, with subsequent revisions, is the most widely used system for categorizing data fusion-related functions. The goal of the JDL Data Fusion Model is to facilitate understanding and communication among acquisition managers, theoreticians, designers, evaluators, and users of data fusion techniques to permit cost-effect system design, development, and operation".

8. Airborne Surveillance

Sensors on airborne platforms fill a vital gap in the mix of sensors used to monitor a surveillance volume. From the location of an elevated platform terrain obscuration is widely avoided except for those cases where objects on or near to the ground are located in steep valleys. Platform visual range to objects is only limited by the curvature of the earth which in turn depends on the height of the sensor platform.

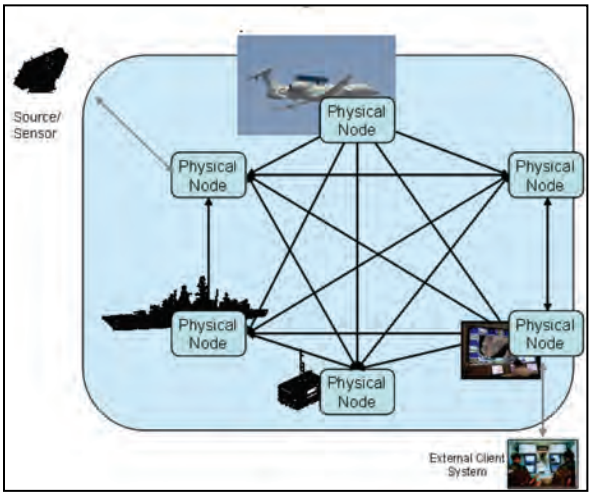


Fig. 2. Command and Control Network with Airborne Surveillance.

The high mobility of an airborne platform allows its flexible deployment to choke points of tactical interest. Together with the long surveillance range the number of airborne sensors required to cover a given area of interest is rather low.

Due to the missing terrain obscuration elevated sensor platforms are capable of efficient networking in a tactical communicating network. They could even act as communication relays to provide communication links between other sites which are beyond of the line of sight between each other.

However, airborne sensor and Command and Control platforms will only provide efficient services if the usable communications bandwidth into the tactical network is sufficient. As we talk about tactical data communication, the communication has to provide sufficient information security. Usually such communications are encrypted and protected against jamming and intrusion.

Airborne sensors will provide a large amount of surveillance data. On top of the Objects of Tactical Interest they will detect and report on all kinds of other objects which share the surveillance volume. Together with noise and jamming, etc. this will result in a high amount of nuisance reports. In order to reduce the bandwidth to communicate the local situation picture of the airborne platform before it is shared with the tactical network, an assessment of the nature of the surveillance reports is needed. Automatic functions such as map based suppression of terrain reflections, automatic clutter mapping, and tracking will assist in the "down selection" of nuisance reports. However, until now human operators are indispensable when it comes to an "intelligent interpretation" of uncertain and partially contradictory information, behavioral patterns and the overall situation. This is why

airborne surveillance platforms of today are usually manned platforms.

There will be in the future more unmanned airborne sensor platforms. They will automatically pre-process and then communicate their local situation picture to an airborne "mother-ship". The communication to an airborne mother-ship is less vulnerable to both intended and unintended disturbances. The locale situation picture of one or more "daughter-ships" will be compiled into a concise airborne situation picture. After confirmation by human operators on board the mother-ship this airborne situation picture will be a valuable contribution to the overall network-wide situation picture. If usable bandwidth allows, the data from unmanned airborne sensor platforms may be directly forwarded into ground or surface based Command and Control centers.

9. Some SW Engineering Aspects

Surveillance networks including airborne surveillance platforms tend to be in use for many years spanning across multiple system upgrades and across several SW engineering approaches. It is important to design such systems with SW upgrades in mind already.

Very time critical functions like e.g. the scan control and sensor management of a Primary Surveillance Radar needs to be located as closely as possible to the Radar signal processing. This way the time critical functions are encapsulated within the Radar. The next generation Radar will not re-use the sensor management of a predecessor design anyways. The general rule will be to "encapsulate services into consistent functional units" which will communicate to their outside clients only information which is cleaned up, concise and relevant for the client.

Use "loose coupling" between services in a network. Information shared in a network centric context is time critical down to some 10 – 50 ms. the objects to be monitored don't change their state within than a few milliseconds. This allows the network wide communication to be based on standardized asynchronous processes like TCP/ IP and the tools and standards which are based on such standards. Currently e.g. CORBA, DDS or equivalent Tactical Data Links would be candidates for communication standards to be used. Less time critical communication will be easier to be replaced by coming technologies than very time critical links.

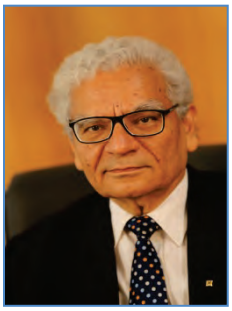
SW design in general, specifically the interfaces between the services, shall be specified at the highest level of abstraction available. Currently SYS ML or UML modeling would be the best choice. If such models capture the characteristics of the interfaces completely, all application code (used for interface, communication, recording, replay, display, etc) in most current, and in potentially most future, programming language bindings can be automatically generated. If later modifications of the messages, the message structures or the communication attributes are necessary both sender and receiver of the data need to agree on the interpretation of the bit data stream which is communicated. As long as message structures don't change the correct interpretation will be embedded into the existing code. Some communication designs like e.g. XML would allow the structure of messages to be communicated together with the message content. However, the communication of message structures and the XML representation will create a high bandwidth demand which is prohibitive specifically for radio communication with airborne platforms. Nevertheless the advantages of communicating message structure can be used if the message structures, i.e. the data model information, are communicated only if needed

because of a message design update or otherwise rarely. Receivers of such structural information could then execute code generators to update their code and enable the services to communicate updated messages/ structures. Obviously this helps only with those functions where automatic code generation along known patterns can be used. The implementation of changed semantics is still needed by a proper SW design, as applicable.

References

1. Alberts, David, John Garstka and Fred Stein. "*Developing and Leveraging Information Superiority*". Proceedings of the 1st national Symposium on Sensor Fusion 1988 Orlando Florida. Note: "This document may contain information subject to the International Traffic in Arms Regulation (ITAR) or the Export Administration Regulation (EAR) of 1979"
2. A. Steinberg, Ch. Bowman "Revision to the JDL Data Fusion Model" Chapter 2 in Handbook of Multi Sensor Data Fusion 2001 CRC Press LLC
3. NATO STANAG 1241. "NATO Standard Identity Description Structure for tactical Use"

Global Navigation Satellite System (GNSS) – An Indian Stride



Surendra Pal
Distinguished Scientist and former Founder Programme Director
of Satellite Navigation Program – India (ISRO)
Presently Vice Chancellor, Defence Institute of Advanced Technology, Pune

Abstract: *Global Navigation Satellite System (GNSS) is a vast system of systems, providing global positioning, navigation and timing information to scores of users in oceans, land, air and even in space. Here we trace the history of navigation, evolution of navigation satellites, the present constellations and world scenario. India has taken a significant step in this direction, with its SBAS system GAGAN and deployment of its own Regional Navigation Satellite Constellation (IRNSS). The article touches upon the various GNSS connected aspects, their applications and the Indian perspective.*

1. Navigation

Navigation, perhaps, is the only science & technology associated with early man from immemorial days. Navigation is the science of chartings one's own route from point 'A' to point 'B' with respect to known references, both in spatial as well as in temporal domain. Identifying and remembering objects and landmarks like rocks, trees, rivers, markings on trees or leaving mile stones/flags and looking at stars, sun and moon, as points of reference as navigation aids were used by early man to find his way in jungles, deserts, mountains etc. The time reference was day/night or even could be seasons. In sea or large lakes to start with : near shore land marks, sea weeds, birds, ocean currents, islands, smells and of course celestial visible objects like Sun, Moon, Pole Star and some constellations like Great Bear etc. were used as navigational references. When moved far-away places latitude, longitude height and time references were required.

"Navigation" word has perhaps its origin in 'Naoka' –'Nav' boat – 'Gati'-Velocity in Sanskrit.

1.1 History of Navigation

Phoenicians, Vikings and Greek were undertaking sea voyages and had great navigational skills even 3000 years back. Phoenicians claimed to have circumnavigated Africa from Red sea, sailing via the Cape of Good Hope. Burning fire on mountain tops were used as light houses. The legendary Light House of Alexandria was an example. Not much is written in the modern history about Navigation activities in Asia-Pacific region. Chinese, Arabs etc., had under taken lots of sea voyages. In Mohanjedaro ruins (Indian sub continent) one clay tablet was found which depicted a boat. Sindhu or Indus valley civilization ruins (parts of Pakistan, Gujarat, and Haryana) do show that

perhaps a successful business existed with Romans, Babylonians and Sumerian civilizations. Out of 18 Tamil Sidhas, Sidha Bhoganathar said to have gone to China via sea route (even he is supposed to have designed an aeroplane) and lived in China as Lao-tzu, spread Taosim. He is attributed to have great navigational skills.

The great Sanskrit scholar Kalidas (4th century A.D) was the first one to imagine above land navigation. In his famous Sanskrit composition `Meghdoot' [Fig 1], Kalidas's Yaksha instructs `Megha', as how to navigate from Ramagiri to Alkapuri. He used complete Bio-Sphere as Navigational Control Points.

कर्तुं यच्च प्रभवति महीमुच्छिलीन्ध्रामवन्ध्यां तच्छ्रुत्वा ते श्रवणसुभगं गर्जितं मानसोत्काः।

आ कैलासाद्बिसकिसलयच्छेदपाथेयवन्तः संपत्स्यन्ते नभसि भवतो राजहंसाः सहायाः॥ ११॥

Having heard your thunder, pleasing to the ear and which causes the earth to abound with mushrooms and to be fruitful, the royal geese, yearning for Lake Manas, bearing pieces of lotus root as victuals for the journey, will fly together as your companions in the sky as far as Mt Kailasa. (11)

Fig. 1. Meghdoot

Fig. 2. Site at Lothal

Archeological site at Lothal [Fig 2] (Gujarat, India) has got remains of a port which indicates that more than 4500 years back India had advanced sea transport system. The dock is almost of the same size as that of Visakhapatnam, modern port.

1.2 Position Determination Evolution

Not much is recorded about early tools used for navigation. However some historical evidence suggests that Egyptian Groma, Cross Staff and Astrolab were used for noting the star position. Traverse boards were use for charting the return route, minute/hour sand or water glasses along with equidistant knotted ropes, and logs were used for boat speed/velocity measurements along with the dead reckoning techniques (still used). These tools were handy (from 14th – 16th century) till compass for direction finding was invented. From 17th to 20th century, chronometer, sextant, compass and beginning of the 20th century even Radio Ranging were used, that included HF/VHF/radio communication, Radars, VOR, LORAN the Land Based Radio Position System. In 60-80's the space based system like Transit, SECOR, TSIKAD etc and then GPS & GLONASS came to be used for 3D position determination. [Fig. 3 gives pictorials depiction of the progress].

Fig. 3. Stages of Navigation

During the primitive stages of navigation [Fig.3], it was possible to fix the latitudes with various techniques mentioned earlier, however fixing a longitude was a tough job, in want of an internationally accepted reference or prime meridian or 0^0 longitude since earth is almost spherical. There were no good, accurate and authenticated maps. The situation became more complicated in want of accurate time measuring clocks and reference. Clocks with Pendulum, water/sand hour glasses etc were affected by humidity, gravitational changes, ship movements, temperature changes, above all poor reliability with high drift rates and want of prime meridian as reference, made the task of sea voyages extremely difficult and risky. The sailors used to move more because of good luck, rather than navigational tools or skills. The biggest recorded tragedy is of a single accident on Oct 22, 1707, at the Scilly Isles near the south western trip of England, four home bound British warships under the command of Admiral Sir Clowdisley Shovell ran aground and nearly two thousand men lost their lives. Shocked by such accidents the British Parliament in its famed longitude Act of 1714 AD' set the highest award/reward of that time, naming a prize equal to £ 20000/- for a "Practical and useful means of Determination of Longitude using a Chronometer". English clockmaker John Harrison, a mechanical genius took the challenge and pioneered the science of portable precision time keeping, made the Chronometer excelling the requirements, in 1764 AD. This chronometer changed the pace of navigation as it was only used to lose less than a second in 24 hours, even in voyage undertaken in high seas. [Fig-4]

Time keeping is an important activity since one degree of longitude equals FOUR minutes of time the world over and distance at equator is 68 miles virtually become, a point at poles. **This called for fixing a prime meridian reference (0^0 Longitude)**. Fig 4 & Fig 5 give a historical perspective of progress in time determination & accuracies, where now we are looking for picoseconds accuracies. If we lose one nanosecond, the error in distance is 30cm.

In the year 1884 AD at the International Meridian Conference held in Washington DC, 26 Countries voted to make the common Prime Meridian and Greenwich Meridian as the prime meridian of the world. This also became the GMT.

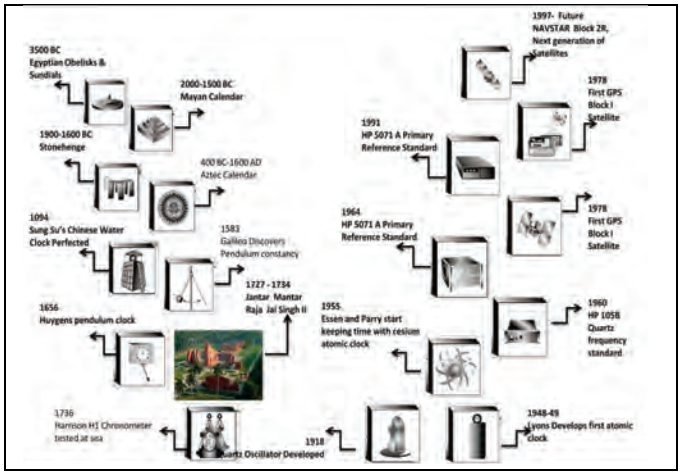


Fig. 4. History of Time

2. Satellite Based Navigation

With the launch of Sputnik in 1957 the era of space based navigation and communication started. Scientists of the John Hopkin's University of Applied Physics laboratory, who studied the signal and Doppler shift, were able to predict the orbit. This gave birth to the idea that if ephemerides of satellites are known then observer position can be determined by Doppler measurement. However, for 3D measurements and increase in accuracy clock was to play an important role along with tones and Doppler measurements in Transit, Secor, Tskylon, Tiskada & Timation (for runner of GPS). The s/c 621B used PRN codes. The future satellites were

provided with atomic clocks. By 1978 all efforts of various US agencies were merged and NAVSTAR or GPS programme came in to existence. USSR developed the GLONASS constellation and both were fully operation in 1998.

2.1 Position Fixing

The position determination with reference to: three predetermined locations, fixes the accurate position of an individual, using the well known triangulation technique. [Fig. 5]

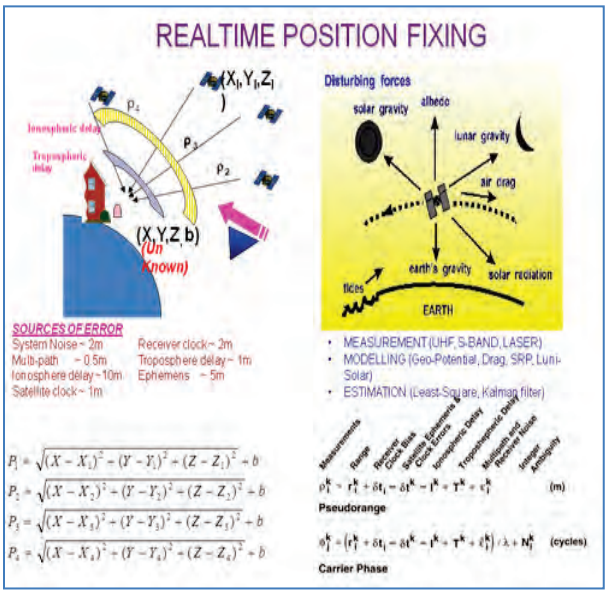


Fig 5. Real Time Position Fixing

However there are errors and time biases in the measured range called PSEUDO range. To remove this we make measurements with respect to FOUR references. In satellite navigation scenario, the four references are the spacecrafts in orbit whose ephemerides are accurate and well known. Three spacecrafts are used for determining the three unknowns of position while the fourth one is used to 'removed of bias particularly related to time. Errors are also introduced due to iono, tropo, multipath etc.

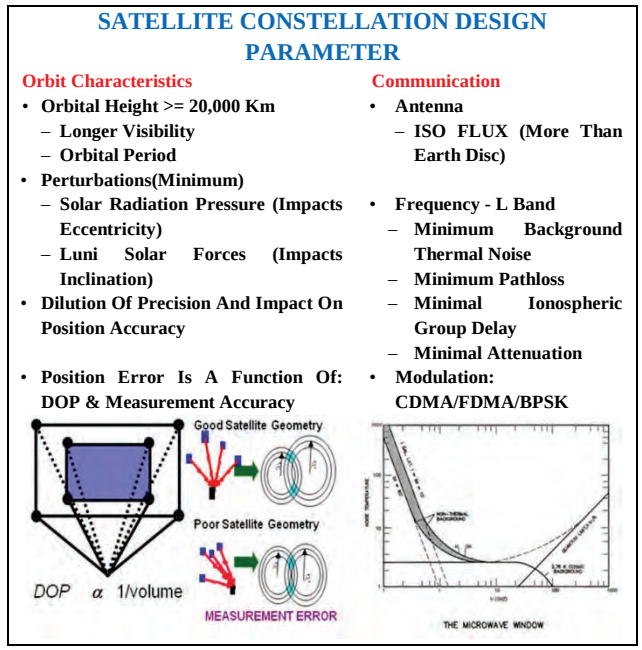


Fig. 6. Satellite Constellation Design Parameter

During the planning of GPS & GLONASS it was consciously decided to go for 'L' band, [Fig 6] frequencies, where the background microwave noise is minimum. To give a global coverage, satellites were put at 19000kms to 22000kms in multiple planes. US/GPS Programme decided to use three planes, same frequency but with CMDA & different codes, while GLONASS used six planes & FDMA multiple access techniques. The higher orbits, above VanAllen radiation belts were chosen. It also provided ≈12 hours orbital period with longer visibility. The satellites were small with short appendages like solar panels etc. so that solar and Luni radiation pressures do not impact the orbits. Minimal and essential orbit maintenance manoeuvres were planned so that orbits remain stable. Onboard isoflux antennas with precise known location of phase centres were designed and employed. The range obtained from four satellites is PSUEDO range. The errors due to iono, clock, ephemeris, tropo, multipath etc. are estimated and removed [Fig. 5]. To get good GDOP (Geometrical Dilution of Precision$\alpha \frac{1}{v}$) one should have widely

Separated satellites enclosing large volumes. [Fig 6]

2.2 Present Scenario

Presently GPS and GLONASS constellation are fully operational & GALILEO (European Union) has launched 10 satellites and Chinese 20 satellites. There are two regional constellations – Indian Regional Navigation Satellite System (IRNSS) [5 – Satellites] while Japanese QZSS [1 satellite] are in orbit. There are four operational Space Based Wide Area Argumentation System, augmenting the GPS Constellation: WAAS (2s/c), EGNOS (2 s/c), GAGAN (Indian) (2+1s/c), MSAS (Japanese) (one). These help the seamless civil aviation activity across the globe ($\approx\pm 50^0$ N/S). Russia is planning SDCM System for GLONASS.

GNSS Scenario

- 4 Global Constellations:
  - GPS (24) & GLONASS (29) fully operational
  - Galileo (30) – 10 satellites are operational
  - Beidu (35) – 20 satellites are operational
- 2 Regional Constellations:
  - IRNSS (7) – 5 satellites are operational
  - QZSS (7) – 1 satellite is operational
- GNSS (SBAS) Augmentations: WAS,

The world wide trend is to have a multi-constellation system with multi frequency receiver developments so that one can have improved availability, accuracy and multipath mitigation. The dual and triple frequencies are available for civilian users with added iono corrections. There is an effort towards having systems with improved resistance to jamming and spoofing. The modernized signals of GPS/Galileo/GLONASS and even IRNSS (by 2020) will provide faster TTFF, weak signal tracking and acquisition, indoor positioning (Assisted GPS), messaging, improved multipath, search and rescue, disaster warning and even environ monitoring.

3. Indian GNSS Paradigm

Satellite Positioning System (SPS) receiver development of ISRO started in 1996 to determine orbits of low earth satellites accuracy First SPS was used On Board IRS-P4. In-house developed orbit determination software SANGAM was used successfully. SPS is a regular phenomena onboard Indian all low earth orbit satellites. The orbital predication has become quite accurate and easy, better than 50m. The system was developed jointly by ISAC/ISRO and M/s Accord Software [Fig. 7, 8 & 9]. Fig 9 depicts the performance of SPS over years.

Description	Specification	Remarks
Type of System	GPS Receiver, L1, C/A (6/8/10/12 Channel SPS) L1 C/A, L2C & GAGAN (21 Channel SPS)	In Future, this could change in a Multi-GNSS environment
No of Channels	6/8/10/12/21	More Channels need More On-board Resources
Time To First Fix	480/100/85/80 (Sec)	Faster is Better
Velocity	± 10 km (Doppler range of about 100KHz at L1 frequency)	LEO Satellites typically orbit at 28,000 km/h speed
Acceleration	5g	High during launch/re-entry. On-Orbit much lesser.
On-board storage	2 Orbits Data	Down linked at 16 kbps through a Ground Station
S/C Interface	MIL-1553B or Serial	Mission Requirements

Fig. 7. Major Specifications of SPS

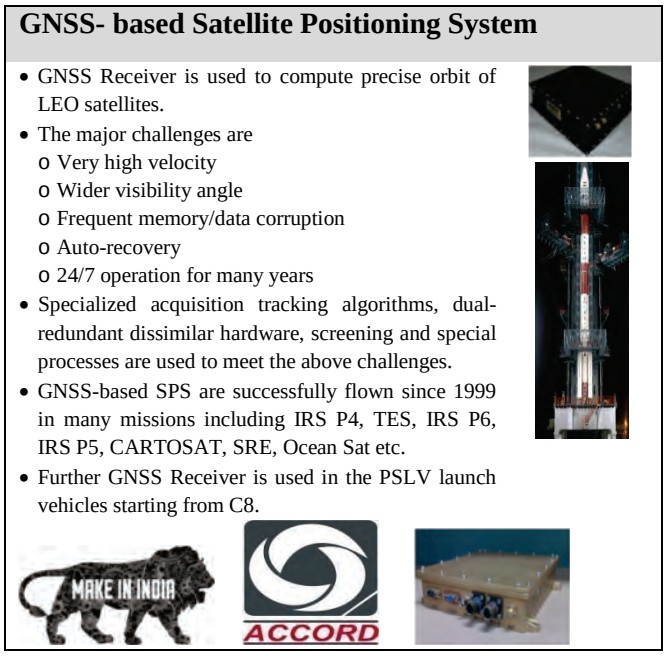


Fig 8. GNSS based Satellite Positioning System

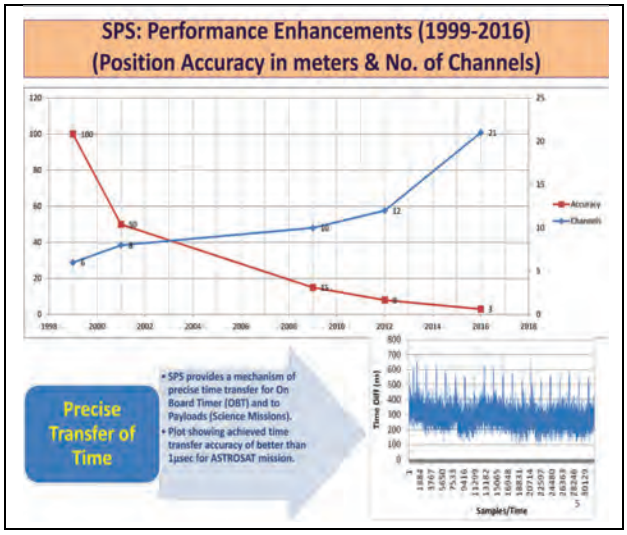


Fig 9. Accuracy & Channels Vs time

3.1 Satellite Based Augmentation System (SBAS) studies were undertaken by ISRO along with AAI in 2001. GAGAN (GPS Aided Geo Augmentation Navigation) project was formed in 2003. Technology Demonstration System (TDS) was over in 2007 and Final Operational Phase (FOP) spread over years 2009 to 2013. GAGAN got certified for APV1.0/1.5 in April, 2015. GAGAN system is an open system available to everyone free of cost. The system transmits GPS like signal with all corrections to the user receiver so that majority of errors are removed. GAGAN accuracies are much better than many DGPS system. (Fig 12 gives a comparison of positional accuracies of various places in India using GAGAN & GPS receivers respectively.) Fig. 15, 16 & 17 depicts the capabilities & achievements of GAGAN.

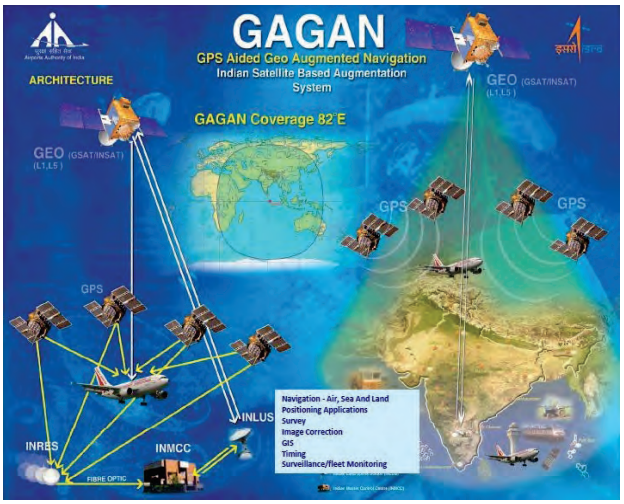


Fig 10: GAGAN coverage

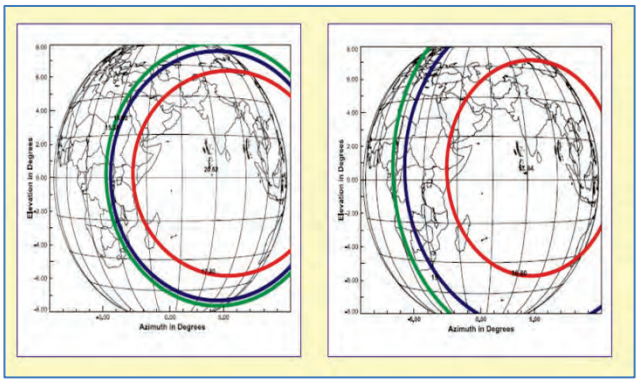


Fig 11. GAGAN Payload L1 & L5 band coverage contours

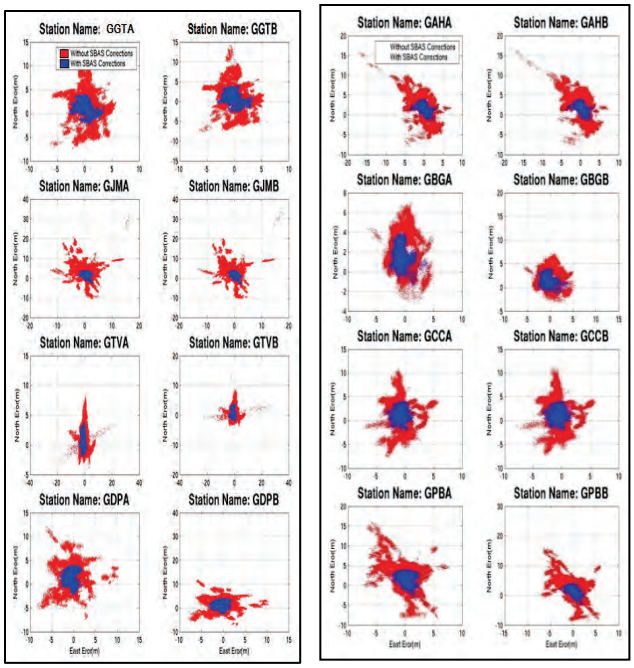


Fig. 12. GAGAN TDS Position Plots for 24hrs using GPS (Red) & GAGAN enable receivers (Blue) respectively

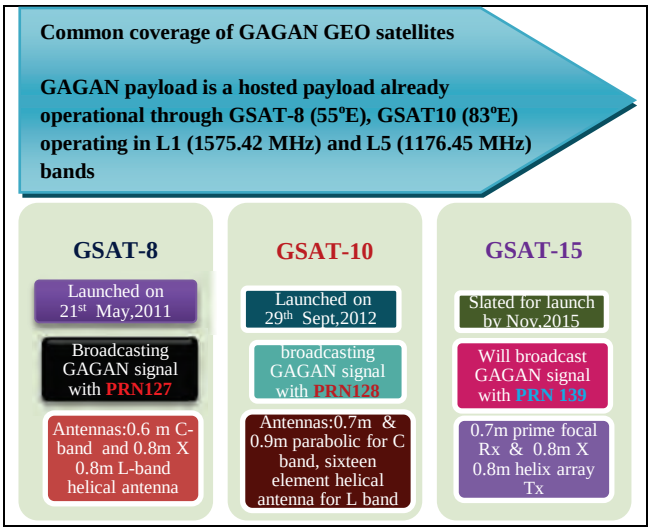


Fig. 13. GAGAN Space Segment

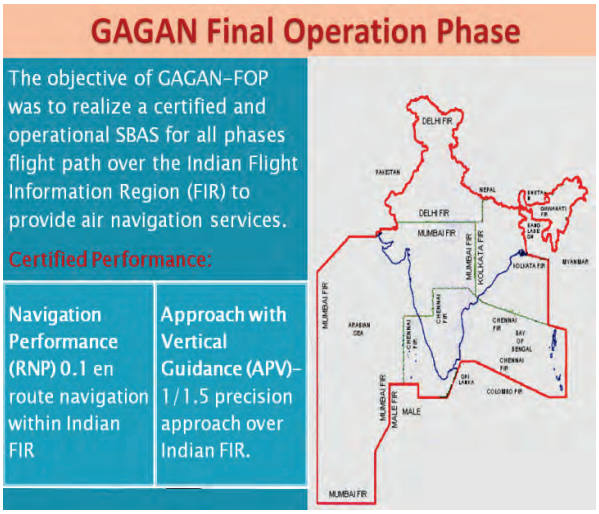
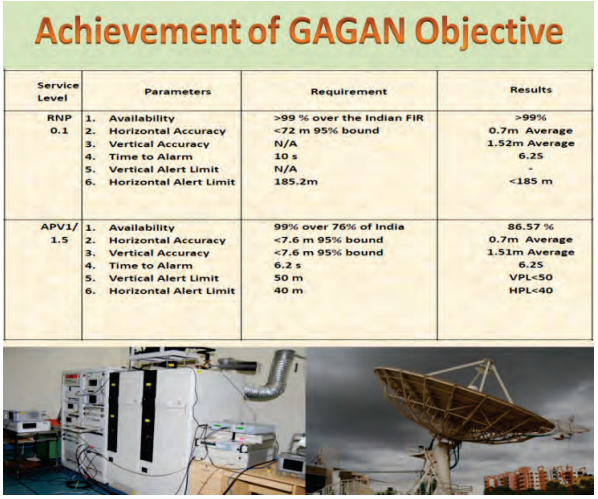


Fig. 14. GAGAN Final Operation Phase



Achievement of GAGAN Objective

Service Level	Parameters	Requirement	Results
RNP 0.1	1. Availability	>99 % over the Indian FIR	>99%
	2. Horizontal Accuracy	<72 m 95% bound	0.7m Average
	3. Vertical Accuracy	N/A	1.52m Average
	4. Time to Alarm	10 s	6.2S
	5. Vertical Alert Limit	N/A	-
	6. Horizontal Alert Limit	185.2m	<185 m
APV1/ 1.5	1. Availability	99% over 76% of India	86.57 %
	2. Horizontal Accuracy	<7.6 m 95% bound	0.7m Average
	3. Vertical Accuracy	<7.6 m 95% bound	1.51m Average
	4. Time to Alarm	6.2 s	6.2S
	5. Vertical Alert Limit	50 m	VPL<50
	6. Horizontal Alert Limit	40 m	HPL<40

Fig. 15. Achievement of GAGAN Objective

GAGAN Certifications

GAGAN has been certified by Directorate General of Civil Aviation (DGCA) for the provision of RNP 0.1 and APV 1.0 services.

- RNP 0.1 Service
  Certification: 30-Dec-2013
  Commissioning: 14-Feb-2014
- APV 1.0 Service
  Certification: 21-Apr-2015
  Commissioning: 19-May-2015

3 GEO's GSAT-8, GAST-10 and GSAT-15 carry GAGAN Payload.

Fig. 16. GAGAN Certifications

3.2 Indian Regional Navigation Satellite System (IRNSS): Since GPS & GLONASS are controlled by US & Russian defence agencies, with a warning that services may be denied, India has decided to develop its own navigation satellite system to keep in pace with the emerging geopolitical situation, where besides GPS, GLONASS, QZSS China's Compass and Beidu satellites systems are getting deployed.

Studies were started in 2003. Project formulation was completed in 2006. First IRNSS satellite was launched on 1st July, 2013 * the full Constellation of seven satellites is slated to be completed by 2016. An exhaustive collaborative studies and efforts have been continuously undertaken with GPS, GLONASS, EGNOSS/GALILEO and JAXA. Ionospheric & Tropospheric – Studies and modeling were undertaken and that resulted in to development of a special ionospheric model for ionogrids both for GAGAN & IRNSS, so that accuracies are much better than stand alone GPS.

To start with the Indian Regional Navigational Satellite Systems (IRNSS) is of seven satellites, 3 Geo- stationary while '4' are Geo-synchronous, with 29^0 inclinations, to provide good GDOP & position determination accuracies comparable or better than GPS. IRNSS provides the designated services over the Indian subcontinent + 1500kms beyond Geopolitical boundary of India. Four more satellites added in suitable Geo Synchronous (properly phased) orbits with higher inclinations and proper orbital spatial and temporal phasing can increase both position determination accuracy and coverage in future.[Fig 17 to 20 depicts various aspects of IRNSS]

Due to non availability of spectrum slots in and around L-band, India has decided to go by L5 (1164.45 – 1188.45 MHz) and S-band (2483.5 to 2500 MHz) with standard positioning services (SPS) using grid based iono corrections. IRNSS uses BPSK (1) for SPS and it has an encrypted with long code services for restricted users (Restricted Service) with BOC (5, 2) modulation.

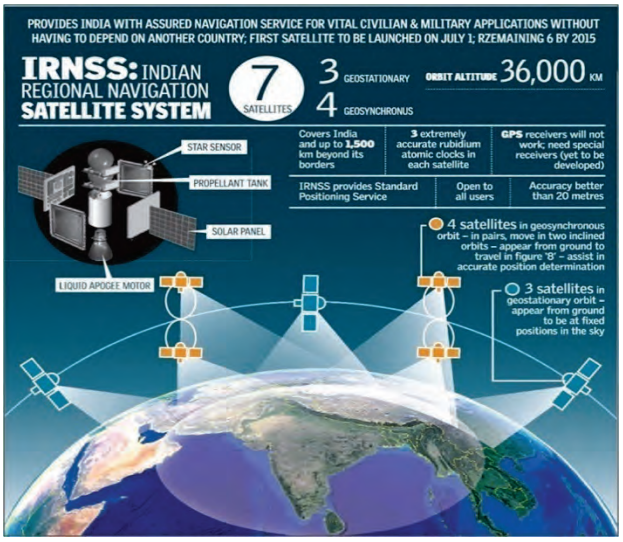


Fig 17. IRNSS – Orbital Positions

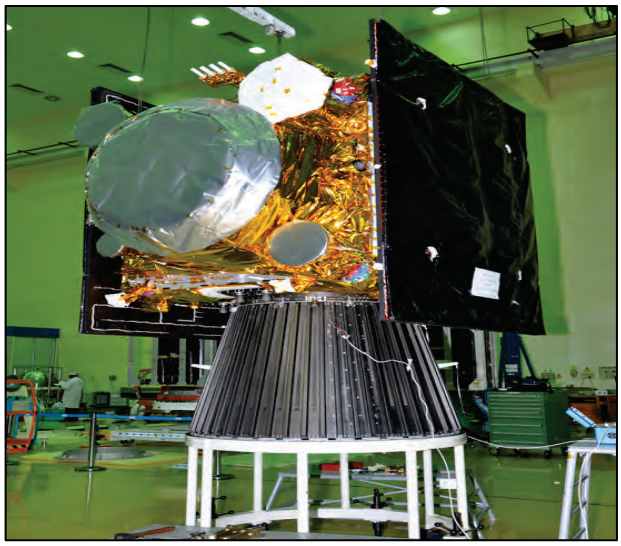


Fig. 18. IRNSS Satellite Communication

Currently 5 satellites are in orbit – IRNSS constellation of seven satellites will be completed & be operational by mid 2016. Four satellites results are extremely accurate & encouraging [Fig 21].

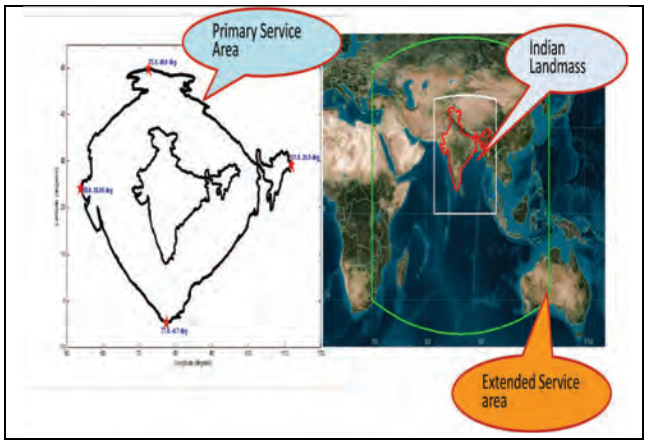


Fig. 19. IRNSS - Service Area Definition

IRNSS service area is divided into three regions:

Indian Land Mass: The area encompasses the Indian Geo-Political boundary.

Primary Service Area: The area covered by 1500 km contour from Indian geopolitical boundary inclusive of the Indian Land Mass.

Extended Service Area: The area between primary service area and area enclosed by the rectangle of Lat 30^0S to 50^0N, Long 30^0E to 130^0E.

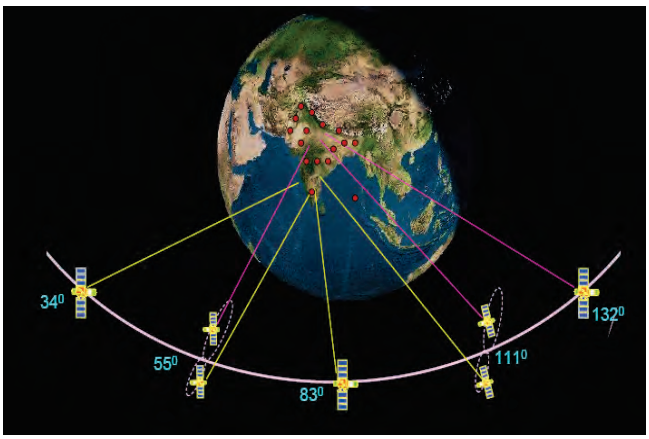
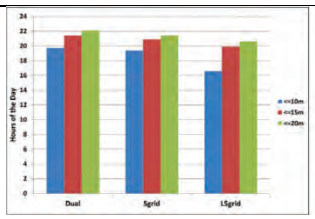


Fig 20. IRNSS coverage

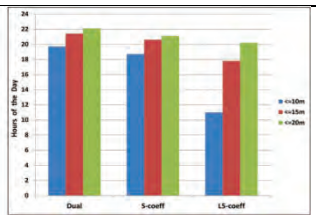
- IRNSS - Regional Navigation Satellite System with 4 GSO + 3 GEO Satellites
- L5 and S-band Signals
- SPS (Standard Positioning Services) and RS (Restricted Services)

3.3 IRNSS Uniqueness

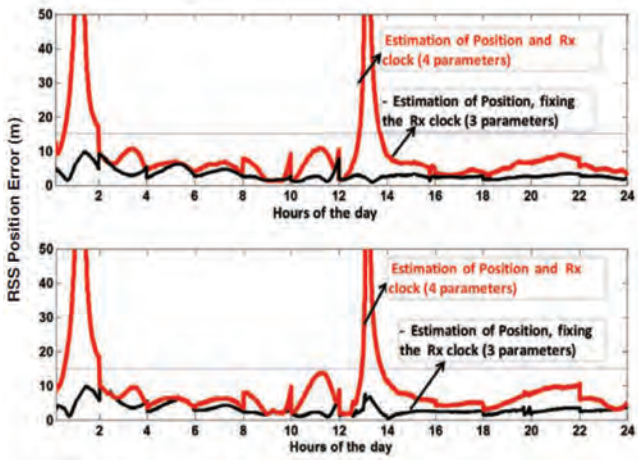
IRNSS is an indigenous system – Uses Dual Frequency (L5/S) for Civilian Users & third satellite navigation system (worldwide) to be fully Operational by mid 2016, Uses Grid based model for ionosphere delay correction (accurate for single frequency users at L5/S band), S-band for navigation – first time being used (low ionospheric delay to benefit single frequency users, IRNSS can be used to broadcast short messages (potential to be used also as a Disaster Warning Dissemination System), all satellites are visible over Indian region for almost all the time, RS (Restricted Services) signal for strategic users. Using '4', IRNSS satellite namely IRNSS – 1A, 1B, 1C & 1D – over sixteen hours in a day, accuracies obtained are much better than GPS and comparable or better than GAGAN [Fig. 21].



Position errors for single-frequency user equipment using grid-based corrections compared with dual-frequency receivers



Position errors for single-frequency user equipment using coefficient-based corrections compared with dual-frequency receivers



RSS Position Error at Bangalore and Bhopal Reference Stations with 4 IRNSS Satellites

Fig. 21. Position error comparison

3.4 IRNSS Satellite Payload Functions & Signals : Reception of navigation uplink data through TC, Generation of navigation message, SV time, code generation, code encryption, Spreading codes, modulation, up-conversion, amplification, filtering and transmission, Three signals in each L5 and S Band (SPS, RS-D, and RS-pilot signals, Interplex signal is added to maintain the constant envelope characteristic of the composite signal, The IRNSS Payload nominally transmits signal with SPS (22.2%), RS-D (44.4%), RS-Pilot (22.2%) and Interplex (11.1%) power distribution, SPS signal is BPSK (1) Modulation, RS-D and RS-Pilot uses BOC (5,2) Modulation, Onboard Rb Atomic Clock for Highly Frequency Stability. [Fig 22 & 23]

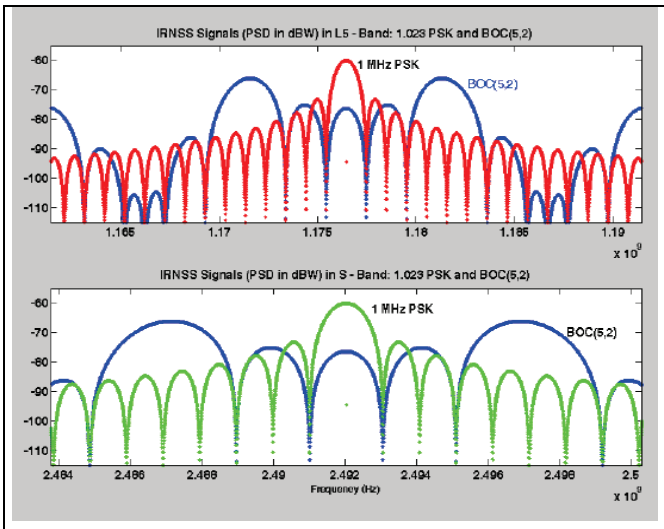


Fig. 22.: IRNSS signals in L and S band

Service Type	Signal	Frequency	Accuracy
Standard Positioning Services (SPS)	BPSK (1)	L5 (1176.45 MHz) S (2492.028 MHz)	Single Frequency < 20 mtrs
Restricted Positioning Services (RS)	BOC (5,2)	L5 (1176.45 MHz) S (2492.028 MHz)	Dual Frequency < 10 mtrs

Fig 23. IRNSS Signals, Services & Accuracy

4. GNSS & IRNSS Applications

4.1 GNSS Application Areas

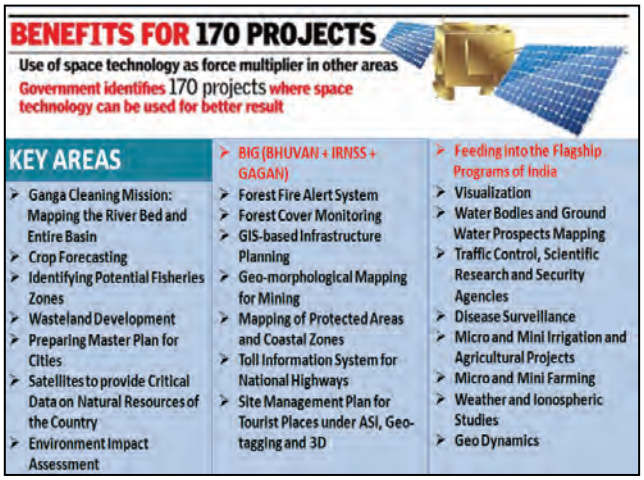


Fig. 24. GNSS applications areas

4.2 Defense Applications of IRNSS

Maritime, Aeronautical & Terrestrial Navigation, UAV and Aerial Delivered Weapons, Gun, Mortar, Launcher Alignment and Short Range Weapon Navigation, Aid to Inertial Navigation, Precision Timing Applications, Synchronizing Secure Radio, Synchronizing Communication Networks, Timing of Navigations Parameters, Launch Complex Synchronization, Marine, Aeronautical and Terrestrial Navigation, UAVs and Aerial Delivered Weapons, Gun, Mortar, Launcher Alignment & Short Range Weapon Navigation.

Fig. 25. GNSS various applications in defence

4.3 Satellite Navigation Aided Inertial Navigation System : In Weapon System, Primary mode of Navigation is the Inertial Navigation System (INS), Inertial Navigation: It is a process of measuring movements of a vessel based on sensed acceleration in known spatial directions, Gyroscopes, Accelerometers, Electronic computers.

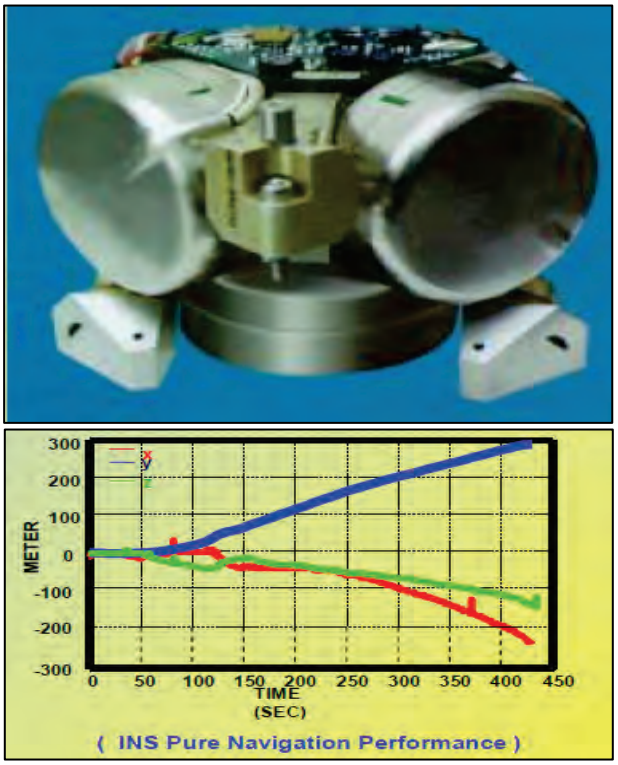


Fig. 26. Application in INS

4.4 Civilian Applications of IRNSS

4.4.1 IRNSS based Disaster Warning System Agencies like IMD, INCOIS, CWC etc. can generate disaster related alerts, Alerts transmitted via VSAT network to INC, Alert message will be up-linked to IRNSS Satellite by TT&C Centre, IRNSS navigation message structure can transmit certain short messages, and short message can be received by all INRSS User Receivers.

4.4.2 Road Navigation : Road Navigation, Tracking, Tracing and Scheduling Vehicle Routing, Remote Condition Monitoring, Fleet Management, Intelligent Transportation System, Speed, Emission Control, Load Monitoring, Safety and Security, E-tolling, PAYD Insurance, Accident Reporting, Working time Directive.

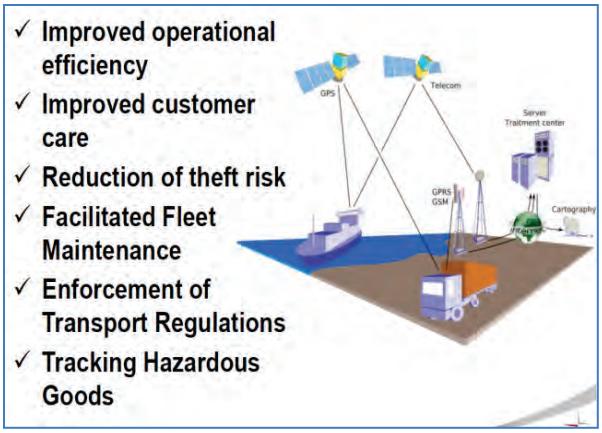


Fig.27. Fleet Management

4.4.3 Rail Transportation : Train control, Signaling, Traffic information, Transportation of dangerous goods (Real time track surveying, performance monitoring & condition monitoring), Prevention of collision, derailments and rails switch errors, Asset monitoring and location, Increase capacity and efficiency, Equipment location awareness, Automatic track survey and inspection, Time synchronization of communication systems.

Fig. 28. Real time tracking

4.4.4 Automatic Train Tracking System: For Indian Railways (12000+ Trains), Technology used: IRNSS, MSS, GSM/GPRS

Fig. 29. Application in tracking technology

4.4.5 Maritime : Observing sea level changes, Dredging operations, Wreck locations, Laying pipe lines, SAR of sinking vessels, Positioning of oil rigs, Prevention of piracy, Automatic Identification System, VMS (Vessel Monitoring System), Coastal Surveillance, Maritime domain Awareness.

4.4.6 Coastal Surveillance: Tracking of ~ 2.5 Lakh small boats (< 20 m) in Indian Coastal Region, Coastal security & Maritime Domain Awareness (MDA).

4.4.7 E-CALL (Emergency Calling): Vehicle automatically dials E-CALL (emergency number) in case of an accident, Sends IRNSS co-ordinate to emergency service, Sends vehicle data (point of impact data), and Improves response time.

4.4.8 Space Exploration: Indian Launch Vehicles, Space shuttle tracking, Inter-planetary navigation, Re-entry and landing of space missions, International Space Station (ISS), Orbit and attitude determination of spacecraft.

4.4.9 Emergency Location: Car mounted with GNSS Receiver and Cellular Telephone, Micro-computer monitors airbag deployment system installed in car, If the air-bag is deployed, the micro-computer calls service center over cell phone, Service center passes information to the local emergency services who can respond to the emergency.

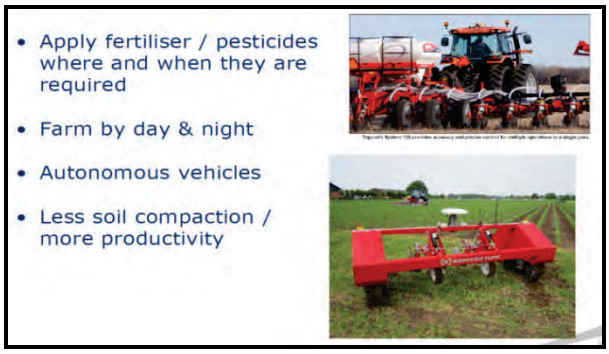


Fig. 30: GNSS for Agriculture

4.4.10 Surveying: Land (Cadastral, Construction, Mapping and Mine Surveying, Marine (Hydrographic and Offshore Surveying), Currently Professional Surveying Receivers use all available GNSS signals (multi-constellation & multi-frequency) & other differential correction technique (e.g. SBAS, RTK, DGPS).

4.4.11 Time Synchronization of Power Grid:

Fig. 31

4.4.12 Monitoring of Structures & Environment: Bridges, Towers, Dams & Reservoirs, Rail & Road Networks, Sky Scrapers & High Rise Buildings, Foundations, Mines & Quarries, Power Stations, Historic Buildings and Landmarks, Landslides, Earthquakes / landslides, Flood Risk and extents.

4.4.13 Disaster Management & Support: Disaster assessment, management and prevention, Monitor possible danger situations that may cause disaster (e.g. monitor flood levels, tsunami prediction, and earthquake), Rapid emergency communication, and Rapid command schedule.

Fig. 32: Assessing disaster

4.4.14 Atmospheric and Ionospheric Studies using IRNSS: Ionospheric Monitoring & Scintillation Studies, GNSS Tropospheric Effects & Meteorology, GNSS Reflectometry (GNSS-R), GNSS Radio Occultation (GNSS-RO).

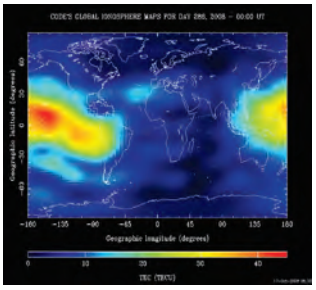


Fig. 33:Global TEC Map

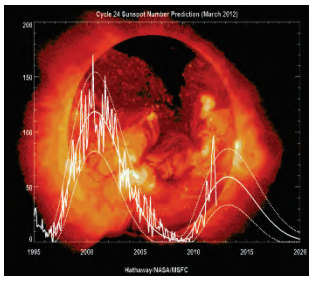


Fig. 34:Ionosphere significantly depends by solar activity

4.4.15 Location-Based Services (LBS)

- **Amenities:** Closest hospital, Filling station, Nearest restaurant, Shopping mall
- **Weather:** Current weather at the location, Temperature, Possibility of rain
- **Topology:** Landform, Height from sea level, Nearest river, Lakes, Mountains etc

- **Entertainment:** Any sport event near the location on date, Theatre halls etc.

5. Conclusion

After all, we need measurements of space and time for almost all our activities and GNSS provides these. For the emerging civil aviation scenario (less than 5 years), all users will need accurate PNT services. All these will be provided by GAGAN IRNSS, which in future do have potential to expand.Hence, GNSS will influence our life more than any other technological advent.

References:

1. Numerous invited talks, presentations & publications done by the author on GNSS, during his long tenure at ISRO as Founder Program Director of Satellite Navigation Programme.
2. Various Presentation made by the author at UOOSA- Vienna on GNSS.
3. Presentation made "Indian GNSS Paradigm" at SCPNT-2015 – Stanford University, California USA, 13th Nov. 2015.
4. A.S. Ganeshan et.al. "First Position Fix with IRNSS", Inside GNSS, July/August 2015, Page No. 48-52.
5. K S Parikh presentation on "Indian Satellite Navigation Program" at 'National Conference on Electronics and Computer Engineering (NCECE-2016)', DIAT, Pune on 21st Jan. 2016.

Electronics as a Force Multiplier in Military Vehicles




SN Yadava[1] **Col. AS Takshak** [2] **HB Srivastava** [3] **Benjamin Lionel**[4]

[1]Sc-'E', PO-II, DRDO HQ, New Delhi.
[2] Addl Dir, DRDO HQ, New Delhi.
[3] OS & Director, LASTEC, New Delhi.
[4] Sc 'G', Head PO-II, DRDO HQ, New Delhi.

Abstract: *Electronics has affected all the major aspects of military fighting vehicles i.e., Fire Power, Mobility and Protection. In this paper, the electronic systems and technologies which have made the military vehicles as force multipliers are discussed in detail. Challenges and related issues are also discussed. This paper also brings out the emerging trends and potential technologies of the future that would change the battlefield scenario.*

1. Introduction

Electronics has invaded every aspect of human life. It has revolutionized the communication technology, resulting in change of human life style and converted the world into a global village. The advancement in electronics has been adapted to several weapon platforms making them a potent game changer. It is no secret that technology drives the tactics in battle. The war tactics of World War II (WW II) have been made redundant due to the advent of cutting edge electronic systems. Military vehicles have adopted these force multiplier technologies resulting in enhancing capability to neutralize the enemy target in quick response without suffering any major hit in combat. This paper elaborates the various electronic systems that have contributed in evolution of military vehicles since WW II till date and have made them a force multiplier in today's battlefield. Integrated Fire Control System [1], Thermal Sights, Laser Range Finders and Designators, Image Tracking, Battlefield Management System, Electronically Controlled Engine [2,3], Electronically Controlled Transmission Unit, Laser Warning Systems and Network Enabled Operations [4] are some of the technologies adopted on contemporary military vehicles.

2. Electronics and Military Vehicles

All the systems of military fighting vehicles can be broadly classified into major categories i.e., Fire Power, Mobility and Protection. The introduction of Electronics has enhanced the performance of all the three parameters and is elaborated further.

3. Fire Power Related Electronics Force Multipliers

Firing capability of Armoured Fighting Vehicle (AFV) plays critical role in battle effectiveness. Figure 1 depicts systems involved in firing from an AFV. The various technologies related to fire power are discussed below:-

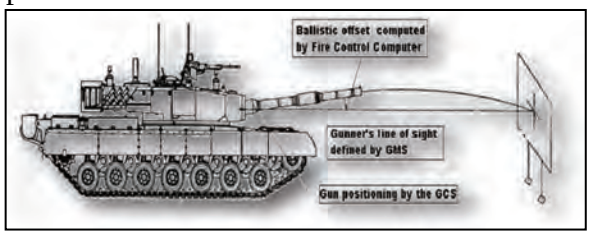


Fig 1. Systems involved in firing.

3.1 Integrated Fire Control System (IFCS) of Modern Battle Tanks

Hitting a distant moving target requires ascertaining its range and, estimating its speed and direction, extrapolating to compute the lead angle, and then imparting the ballistics to the weapon. In the early twentieth century, when tanks came into the battlefield, gunners performed these tasks manually with skills gained during training or aided by small instruments like optical telescopes and stadia line range finders, look up ballistic firing tables, and laying the guns by mechanical screw jack. During World War II, Battle tanks had mechanical sights with a ballistic graticule to impart the requisite offsets to the gun over the Line of Sight. Range estimation was done using a ranging machine gun, which obviously gave out the position to the enemy. This had further limitations as there was no means to compensate for the real-time environmental conditions. Also, it had associated inaccuracies due to the limitations of mechanical linkages of the gun with the sight.

Introduction of Laser Range Finders (LRF) in the late 1960s enabled estimation of range to an accuracy better than ±10m. Also, the advent of synchros, resolvers and later on digital encoders led to replacement of mechanical linkage between weapon and sight by electronic or digital linkages, enabling weapons to follow sights more accurately. Digital technology provides significant improvements to Fire Control System (FCS) by enhanced responsiveness, ballistic computation for different projectiles trajectory and moving target engagement. Accordingly, modern FCS has enhanced the battle effectiveness of Armored Fighting Vehicles (AFVs) in terms of their accuracy, high first-round-hit-probability, thus enhancing their fire power.

Modern IFCS can be defined as a system combination of the Gunner's Main Sight (GMS), Gun Control System (GCS), Commander's Panoramic Sight (CPS), atmospheric and ballistic parameter sensors and fire control computer. The functions of target acquisition, tracking, data computation, and engagement control are all carried out primarily using electronics. Technologies for realisation of modern IFCS include Stabilization of Line of Sight (LOS) using precision Gimbal assemblies, Imaging cameras (visible and / or Infra Red (IR) cameras in the bands of long wave / medium wave or short range infrared), Laser, Ballistic Computation, Multi Sensor Fusion, Data & Image Networking. A simplified block diagram of a typical IFCS is given in Figure 2.

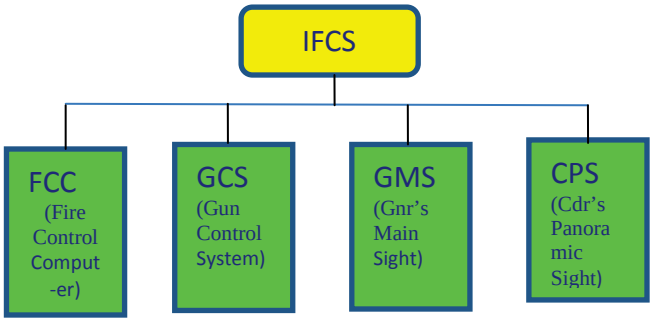


Fig 2. Block diagram of IFCS

The technologies of primary sighting system, namely, Gunner's Main Sight which has a

stabilised mirror head with the day sight, thermal sight and LRF / designator inbuilt in its envelope have matured into a highly advanced Fire Control System. Many developers are integrating fire control computer also in the GMS. Some have even got Inertial Navigation System in-built into the Gunner's Main Sight to aid the crew to reach their destination without any dependence on the GPS (Global Positioning System). Thermal Sights have transformed the battlefield into day/night war theatre and will be discussed next. Stabilised line of sight of the FCSs coupled with the stabilised GCS through accurate resolvers and quick response electronics have made engagement of moving targets from a moving platform with high first round hit probability a reality! Hunter killer mode of operation is possible with the use of CPS integrated with its own LRF and ballistic computer. This gives the ability to the commander to do 360° surveillance and handing over of potential target to the gunner by the press of a button. He can then continue to look for new targets while the gunner is engaging the present target. The advantage of this provision is that the commander can range and track the potential target while the gunner is required to only engage the designated target, enhancing the response time of the AFV to neutralise any potential threat.

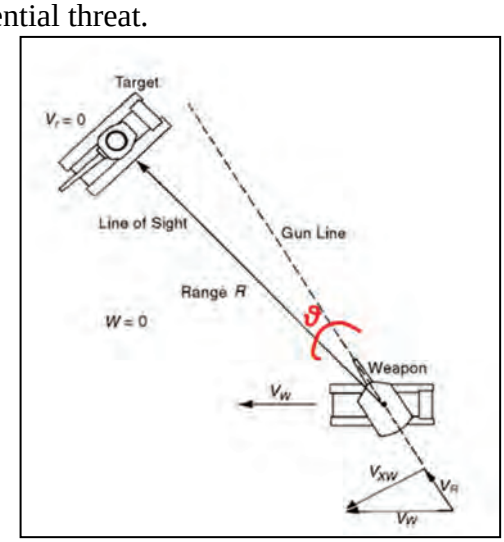


Fig. 3. The Ballistic offset is a result of Offset components in Elevation and Azimuth.

Modern FCSs also have digital interface with all the other payloads on board the AFV and have effective digital communication to transmit voice, data and video signals to the other defined friendly aggregates in the combat team. They have onboard systems that enable guided missiles to home on to the defined target.

3.2 Night Vision Devices

Till WW II, all battles were fought mainly during daytime. The concept of night operations was rarely preferred, considering limitations of illumination of the battlefield and the potential collateral damage. With the advent of photomultipliers, the scenario changed and soon Image Intensifier (II) based systems were introduced for short range vision. However, for long range combat engagement (about 1000m) active IR systems (working in ~900 µm wavelength) came into the battlefield. Very soon, the IR detectors deployed by the opposing forces could easily detect the IR search lights giving out the position of the attacking columns, which necessitated development of 'passive' IR systems, which could sense the radiations emanating from the intended target. The urgency was addressed in the early 1960s when the first passive Thermal Sights (working in 8-12µm) were introduced. This was possible due to the progress made in electronics image processing and display systems. The technologies for thermal imaging systems evolved continuously and have completely redefined the scenario in today's battlefield. Early generation thermal imagers typically contained single element detectors and graduated to linear array. A two-dimensional mechanical scanner was used in order to generate a two-dimensional image. Second generation thermal imagers contained one - dimensional arrays (linear focal plane arrays) with several columns of elements. The two-dimensional

scanner was simplified, as scanning was primarily required only in one direction. Due to scanning in one direction, these thermal imagers still required complex electronics to improve the signal-to-noise ratio. Today's thermal imagers contain two-dimensional Focal Plane Array (FPA) detectors that do not require any scanning mechanism for acquiring the two-dimensional picture. The FPA detector is a significant breakthrough in technology and due to advancements in the optics, electronics, and microprocessor technologies, today's cameras have the ability to engage tank type of targets as far as 5 km or beyond, with equal precision. Today images are digitized, stored, manipulated, processed onboard the camera.

With further advancements, today, Thermal Imaging detectors are classified as uncooled and cooled. In cooled thermal imager, detector is contained in vacuum sealed flask that is cooled by sterling engine cryo-coolers. Cooled types of detectors have higher sensitivity, are faster in response and use small aperture lenses. These are generally used in the GMS and CPS. Compared to this, uncooled thermal detectors, are less sensitive and will require large aperture for signal collection and consequently result in short range thermal imagers. In present day combat vehicles, driver, gunner and commander are all provided thermal sights. These operators are also provided with a day sight (a CCD camera or a direct viewing sight). Since commander is supposed to carry out surveillance, he is generally provisioned with panoramic sights to provide 360 degree situational awareness. Presently all the AFVs are fitted commander's thermal imager with LRF cum day sight with an engagement range of 4-5 km. This capability enhancement has worked as force multiplier for AFVs in the battlefield.

4. Mobility Related Electronics Force Multipliers

Electronic Control Unit (ECU) of engine and Electronic Transmission Control Unit (ETCU) of transmission gear box have enhanced the effectiveness of power pack and ease of operation of AFVs.

4.1 ECU of Engine and ETCU of Transmission Gear Box

Armoured Fighting Vehicles of WW-II and even later versions used mechanically intensive engines and transmissions which had huge limitations in form of their performance, efficiency and power output apart from the challenges of trouble shooting and maintenance. The injection of fuel has decisive influence on engine starting, idling, power, and emissions. The early engines deployed fly weight governors and mechanical distributor injection pump (higher weight, considerable power consumption) to control fuel delivery resulted in poor control of Air Fuel Ratio (AFR), leading to lower thermal efficiency and higher emissions. Today's AFV's engine and transmission are electronically controlled. The main purpose of ECU is to control Air Fuel Ratio, injection timing, waste gate control of turbo charger and other related parameters for optimum performance of engine. Precise control of fuel injection is possible today with Common Rail Direct Injection (CRDI) and use of solenoid valve (instead of injection pump). ETCU is a unit that controls automatic transmission. ETCU may also communicate with ECU or directly interface with the electronically controlled automatic transmissions, traction control systems (TCS). ETCU takes the inputs from vehicle speed sensor (VSS), pressure control solenoid (PCS), torque converter solenoid (TCSd) and other related parameters. Based on the inputs, solenoids are activated to shift the desired gears. The Controller Area Network (CAN) bus

automotive network is often used to achieve communication between these devices. ECU of engine, ETCU of transmission gear box have revolutionized the performance of power pack of military vehicles. ECU fitted engine coupled with ETCU fitted Transmission gear box paved the way for efficient automatic transmission system, enhanced the performance of vehicle and enabled automatic operation with reduced fatigue of vehicle operator. Incorporation of failsafe mechanisms due to overheating of engine and due to loss of pressure in hydraulic lines have helped to avoid catastrophic failure and enhanced ease of vehicle operation. This feature is a real force multiplier as operator / driver can operate the vehicle for longer duration with comfort and handle combat roles more effectively. The simplified input and output parameters of ECU and ETCU is given in Figure 4.

Input sensors		Output
Fuel rack position, Crank position, Fuel , air, coolant temp and pressure	ECU (Processor)	AFR, Injection timing, Boost pressure, Waste Gate opening, Diagnostics, failsafe
VSS, TCS, TCSd, PCS	ETCU (Processor)	Gear shift, Diagnostics, failsafe

Fig. 4. Input and Output of an ECU and ETCU

5. Protection Related Electronics Force Multipliers

Earlier, armour material, thickness and orientation of the armour plates were primary considerations for enhancing the protection level of the military vehicle. Due to the evolving threat, calling for higher level of protection, armour thickness has been increasing progressively leading to increase in the weight of the tank. Higher the weight, lower is the mobility and hence protection is compromised as exposure time of the AFV to enemy fire would be more. Protection with passive armour is inadequate for varied threats in the modern battlefield. Laser Warning and Counter Measure System (LWCMS) is used for passive defence. It detects, analyzes, and locates directions of laser emissions from laser guidance systems and LRF. Then it alerts the crew and launches various countermeasures, like smoke screen, aerosol screen, active Laser Self Defence Weapon (LSDW) with laser dazzler, laser jammer, etc. LWCMS degrade the effectiveness of the incoming missile's sensors and also the missile guidance systems. However, this cannot defeat the unguided and high speed kinetic energy projectiles.

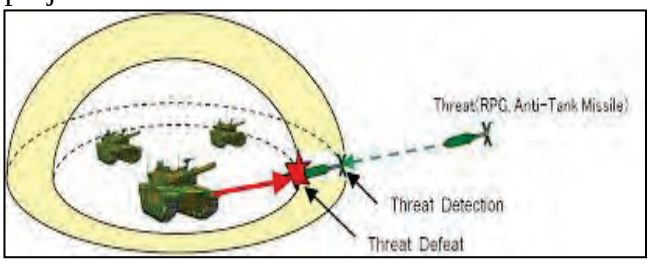


Fig. 5. Active Protection System Concept

Development of Active Protection System (APS) is the current trend to enhance protection. APS consists of highly sensitive radar onboard the AFVs that senses the incoming projectile and triggers a countermeasure that accurately intercepts the projectile at a safe distance from the AFV and neutralises it. The Next Generation Tanks (NGTs) are expected to have less passive armour but with on board APS. The NGTs will also have Remotely Controlled Weapon Station (RCWS) with reduced crew strength.

6. Emerging Trends : UGV And ROV

Electronics has made Unmanned Ground Vehicles (UGVs) and Remotely Operated

Vehicles (ROVs) very effective in applications [5-9]. UGVs / ROVs are used for surveillance, reconnaissance, and Improvised Explosive Device (IED) detection and destruction purposes widely. Other potential uses include breaching of minefields; Un Exploded Ordnance (UXO) clearance; physical security; logistics; fire-fighting; urban warfare; weapons employment; and operations in contaminated zone. A variety of UGVs have been developed that increase mission performance, combat effectiveness, and personnel safety.

If fitted with weapon, UGVs can be used as ground drones for counter insurgency operation and other combat roles. UGVs' performance today is marred by the limited range of operation. Currently, tracked and wheeled UGVs, indigenously developed, can operate in the range of around 10 km. Small ROVs are able to operate in the range of 500m to 1000m in line of sight and confined space. Their range can be extended if they are assisted by Unmanned Aerial Vehicles (UAVs). The UGVs / ROVs discussed so far are tele operated with man in the loop.

AFVs are likely to be unmanned in the future. To start with, these would be remotely operated by combat experienced troops. They would engage in active combat remotely with increased efficiency as they can operate from the comforts and protected ambience of the control room that would be thousands of miles away. Autonomous UGVs (inbuilt intelligence) will be the next reality as military vehicles [10, 11]. They would eventually evolve as 'swarm robotics wherein a group of autonomous vehicles / systems could move together, make intelligent decisions and act appropriately to complete a given mission with minimum human intervention.

7. Generic Vehicle Architecture (GVA)

Traditional vehicle electronic architecture of military vehicles had resulted in highly customised electronic interface of modules leading to high cost of operation and maintenance. GVA is a new evolving standardisation of vehicle electronic architecture which will help the modularity, scalability and maintenance. It is understood that NATO GVA (once established) will be more useful for military vehicle.

8. Challenges

The benefits of electronics in military vehicles are immense. However there are some challenges that need to be addressed in the design phase itself. Harsh environment, shock, vibration and extreme temperature and dust environment needs to be taken care of. Also these challenges are exemplified by network centric requirement such as capture and transport of video for C4ISR application and 360 degree situational awareness. Integration of subsystems, supply chain management and sustenance should be looked into, for smooth operation. Life cycle, obsolescence management for electronics systems and data security is required to be addressed very carefully.

9. Conclusion

Technologies and electronic systems incorporated in modern AFVs, i.e., battle tanks, infantry combat vehicles, and other related vehicles have proved to be game changer. They have enhanced the operation capability manifold and have proved to be force multipliers in the battlefield. The rapid progress in electronics is bound to change the battle tactics further and the days are not far when a fully network centric warfare with remotely operated war machines will participate.

It is foreseen that they will be operated by a combat team that would be handling a host of autonomous ground vehicles, sitting thousands of miles away but have the capability to engage with pinpoint accuracy, like the drones are being operated today! It is not a difficult proposition as the required enabler technologies are already available. Electronic systems customised to the military vehicle platforms are the force multipliers that would help in realising this!

Acknowledgement

The authors are thankful to their Organization, i.e. DRDO and Dr S Christopher, Secretary DDR&D and DGDRDO for providing opportunity to work on these challenging systems of strategic importance. The authors are thankful to laboratory Directors and scientists of CVRDE, VRDE, R&D(Engrs), IRDE and LASTEC working in the field and for day-to-day interaction with them. The authors also thank Indian Armed Forces for their involvement and support in indigenous development of the systems.

References

1. K Bates et al, "Testing Tomorrow's Fire Control Systems Today", IEEE, Systems Readiness Technology Conference 1998.
2. Y Robinson et al, "Experimental Investigation on Electronic Fuel Injection in a Two Stroke SI Engine by Virtual Instrumentation Technique", Intl J of Engg. Ed. Vol 21 No.1, 2005.
3. Max Fuchs et al, "Advanced Design and Validation Techniques for Electronic Control Units", SAE Paper 980199, 1998.
4. GE Intelligent Platforms, "Vetronics Architectures Emerge to Facilitate Network-Enabled Operations", www.ge-ip.com.
5. Gerald R Lane, "Unmanned Ground Vehicle Control Technologies", U.S. Army Tank-Automotive Command, IEEE, 1991.
6. Pekka Appelqvist et al, "Mechatronics Design of an Unmanned Ground Vehicle for Military Applications", Helsinki University of Technology Finland, www.intechopen.com.
7. Phuoc-nguyen et al **"**Reliability and Failure in Unmanned Ground Vehicle (UGV)", Ground Robotics Research Center, University Of Michigan, GRRC Technical Report 2009-01.
8. A. Bouhrauna, et al "Design and Implementation of an Unmanned Ground Vehicle for Security Applications", Proceedings of the 7th International Symposium on Mechatronics and Its applications (ISMA 10, Sharjah, UAE, April 20-22,2010
9. Christof Rohrig et al, "Localisation of an Omni directional Transport Robot Using IEEE 802.15.4a Ranging and Laser Range Finder", The 2010 IEEE/International Conference on Intelligent Robots and Systems, Taipei, Oct 2010.
10. Mitchell M Rohde et al "Point Com: Semi-Autonomous UGV Control with Intuitive Interface", Robotic Mobility Group, Massachusetts Institute of Technology.
11. Jae Cheon Lee et al "Development of Autonomous Vehicles for Urban Driving", ICROS-SICS International Joint Conference, Fukuoka, Aug 2009.

Concept of "Design in India" Integrated with "Make in India" as a Force Multiplier- A Case Study of LCA-Tejas Avionics System

P.N.A.P. Rao
Retd. Outstanding Scientist and Project Director (ADA)

Abstract: *The design, development and production of Indian LCA- Tejas Fighter Aircraft and its induction into service with Indian Air Force as a Force Multiplier with the latest technology has been achieved by the Indian LCA Team by integrating the " Design in India" process with " Make in India" concept. Case study of the design and development of Tejas Avionics System is described in this paper illustrating how such an approach has resulted in increasing the Force Multiplier capabilities of IAF.*

1. INTRODUCTION

Even though India has emerged as the top most destination in the IT and Software Sectors, it has lagged behind in the Manufacturing Sector where China has taken the lead. Keeping this in view, Government of India has launched a laudable program -"Make in India"- to invite firms to manufacture Equipments and Systems in India with the aim of making India a leading manufacturing hub in all areas including Electronics and Defence Sectors where our imports are very high. Even though the "Make in India" Program will lead to increased manufacturing activities in the country, this alone will not be sufficient to achieve the goal of taking India to the Top Five Highly Industrialised nations in the world with attendant increase in employment and GDP. There is a need to enhance Industrial capability in the Defence Sector in India by integrating "Design in India" Program with "Make in India" Program to achieve self sufficiency in the defence sector. This strategy would act as a Force Multiplier for our Armed Forces by enhancing our capability in both design and manufacturing with state of the Art Technology which is tailored to our specific requirements. No nation is prepared to share Force Multiplier Technology with India. In order to attain full Force Multiplier Capabilities it is very essential that India has full Design capability integrated with the manufacturing capabilities in most of the Defence Sectors especially in critical areas. This Article covers some aspects of this subject with case studies from LCA-Tejas Program.

2. NECESSITY OF INTEGRATING "DESIGN IN INDIA" WITH "MAKE IN INDIA"

Analysis of the Manufacturing activities in two major sectors- Electronics and Aircraft -reveals that in most of the cases the "Make in India" Programs have been limited to assembling

Fighter Aircrafts or Electronic Equipments from subsystems imported from abroad with very little value addition. The so called "Technology Transfer" is limited to Manufacturing drawings for assembly and final testing. Obviously no major foreign manufacturer is ready to transfer design data. If India aspires to become a major Industrial Power it is essential that we have the complete competence in all sectors of System Engineering life Cycle from Requirement Capture through Design, Development, Integration, Testing to final manufacture. The System Design should focus on meeting the special and specific requirement of Indian Services. For any Defence System to be used as a Force Multiplier in the ever changing threat scenario, it is essential to have the capability to modify the systems and add additional Force Multiplier capabilities with minimum cost and time. This is possible only if both Design and Manufacturing capabilities are built within the Indian R& D and Industrial Sectors to meet the requirements of Defence Systems.

3. CASE STUDY OF INTEGRATING DESIGN, DEVELOPMENT AND MANUFACTURING IN INDIA- LCA-TEJAS

3.1 Introduction

One of the examples of the Integration of Design, Development and Production activities in India is the Indian Light Combat Aircraft (LCA-Tejas). Tejas is the smallest and lightest multi role Fighter Aircraft of its class with Fourth plus Generation Technologies. With the modern technologies and capability to change weapon configuration to meet the changing roles - Air to Air, Air to Ground and Air to Sea-LCA- Tejas is certainly a Force Multiplier for the Indian Air Force. Initial Operational Clearance (IOC) and its induction into service of Tejas with Indian Air Force can be considered to be a major technological success of Indian Scientific, Engineering and Industrial Community. This is the result of unified efforts of ADA, DRDO, NAL and HAL with participation of a large number of Private and Public Sector Industries as well as Academic Institutions in India.

3.2 Technologies of LCA-Tejas

LCA program had to bridge the technological gap in the Fighter Aircraft field in India where the last design was HF 24 in the early 1960s. Tejas has the following Technologies which can be classified as Fourth Generation Plus: Composite Structure, Unstable Aerodynamic Configuration, Digital Fly By Wire Flight Control System, Integrated Digital Avionics System with Open System Architecture, Full Glass Cockpits with AMLCD Displays, Utility Services Management System with Control and Status/ Health Monitoring of all Systems including Engine, Flight Control and Mechanical Systems. All these Technologies integrated in LCA - Tejas enable it to emerge as a major Force Multiplier in the Indian Defence Scenario.

Figure 1. LCA Technologies

3.3 Methodology of integrating Design with Manufacture as adopted in LCA-Tejas Program

An integrated Team was formed with ADA as Overall System Designer with participation of DRDO Labs, NAL and Private and Public Sector Companies like BEL and HAL. A unique feature of the methodology was that HAL had a major role in design, development and production. This approach helped integration of the Design and Production processes. Another major factor was that Indian Air Force Pilots and Engineers were a part of the Design Team. A National Flight Test Centre (NFTC) was formed with Indian Air Force Pilots and Engineers as an integral part of the LCA Project Team. This enabled continuous in flow of User requirements and Customer review throughout the Life Cycle of the Program minimising rework and changes. Pilot Vehicle Interface (PVI) is a major factor in a Fighter Aircraft Program and participation of the Pilots from NFTC helped in optimising PVI. Flight Testing of LCA was a major responsibility of NFTC

3.4 Case Study of Avionics System Development

In modern Fighter Aircrafts, Avionics System has a major role to play in adding technology and capabilities to the Fighter Aircraft towards the build up of Force Multiplier capabilities. As described below, LCA- Tejas Avionics System is to be designed to have a major role in the Force Multiplier capabilities of Indian Air Force.

LCA-Tejas has State of the Art Integrated Digital Avionics Suite with Open System Architecture and full Glass Cockpit with Menu Driven Displays. This enables the Pilot to obtain any Information on Air Data, Navigation and the Status of the Systems and Weapons. Real time information about the external threat environment obtained through on board sensors like Multi Mode Radar, IR Sensors and EW Suite is presented on a Display enabling the Pilot to assess the threat situation.

Full Avionics System Design was carried out by an Integrated Design Team of all stakeholders. Most of the Hardware was developed in Work Centres in India. Another major aspect is that the Development of all the embedded Software - most of which is Real Time and Safety Critical- was carried out by Indian Design Teams. The Software has more than 3 million lines of Code. An Independent I V&V Team was associated with Software Development and Certification to ensure faults free and safe Software. In fact the one of the major factor which has contributed to the excellent Flight Testing Safety Record of LCA- Tejas till now is the contribution of Avionics System by way of safety design as well as Status and Health Monitoring and generation of Amber and Red Warnings to the Pilot in case of problems in any of the on board system- Avionics, Flight Control, Propulsion or Mechanical. This was possible by the integration of Utility Management System (USMS) with Avionics System. USMS and its integration with Avionics was conceptualised and designed by Indian Engineers. This Integration of all Aircraft Systems and their functionalities through Avionics System is a major design feature of LCA- Tejas which enhances its Force Multiplier Capabilities.

Another feature of LCA is the Project Management in the close association of Certifying Agency-CEMILAC and Quality Assurance Agency- DGAQA. Engineers from both these teams were involved in all stages of design, development, ground testing, integration and Flight Testing. This enabled reduction in development time as all the required inputs from these teams were received discussed and modifications required if any, were carried out in real time.

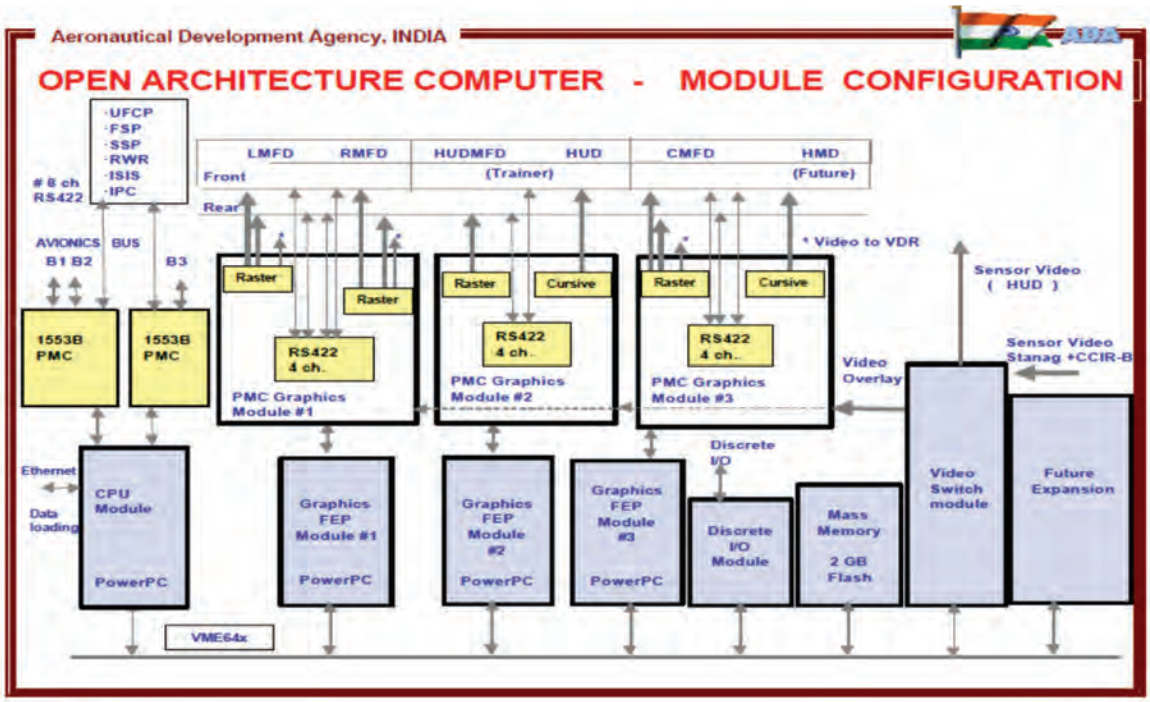


Figure 2. LCA Open Architecture Computer

Figure 3. LCA –Tejas PV2 Glass Cockpit

A Unique feature of LCA Avionics is the Dynamic Testing in a Dynamic Avionics Integrated Rig (DAIR). This enabled the design teams to study the performance of the avionics in all phase of Flight and optimise the software for safe and optimum flights. The result of such extensive testing of all systems including Avionics and Flight Control was that the LCA First Flight on 04 January 2001 was perfect with no faults. All interface and functional problems (both H/W and S/W) were solved on the ground before first flight as all design data was available with the Integration Team.

All the above features which are part of the Four Plus Avionics System of LCA- Tejas has enabled Indigenous Fighter Aircraft to emerge one of the front line Fighter Aircrafts in the world adding to the overall Defence Capabilities of India as a Force Multiplier.

It is matter of pride to the LCA-Tejas team that no accidents have occurred in the more than 3000 Flights so far. This has been possible due to the adoption of fully integrated approach with emphasis on safety aspects in design, testing, S/W development and the incorporation of Status and Health Monitoring of all the Systems through Avionics.

4. Benefits of System Engineering Approach to LCA –Tejas Development:

LCA-Tejas Team adopted the System Engineering (SE) Process to obtain a Integrated Approach to Design Development, Testing and Transition into Production. System Engineering is a “Top Down”, Structured and Inter Disciplinary Synthesis Process leading to the development and operation of a System that satisfies the requirements of the Users and other stakeholders in an optimum manner. It includes Requirement Capture, Architecture Definition, Preliminary Design and Detailed Design, S/W and H/W Development, Testing, Integration, I V&V, transition into Production, Operation and Life Cycle Management including Maintainace. Adoption of SE process helped the LCA team to develop and produce a Weapon System Platform meeting the Requirement of Indian Air Force including Force Multiplier capabilities. System Engineering emphasises Quality, Maintainability, EMI/EMC. It also encompasses produceabilty aspects which help in integrating design with manufacturing. It is recommended all Major Defence Projects adopt this Process. A typical System Engineering Process Model (V Model) is shown in Fig 4 below:

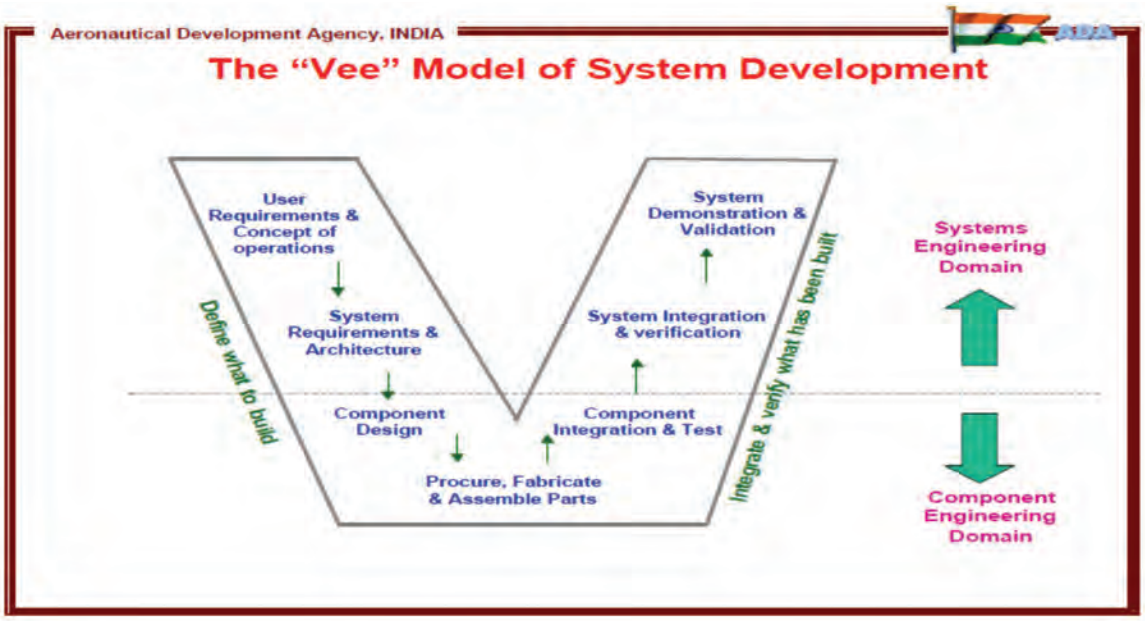


Figure 4. "Vee" Model for System and Software Development

5. BENEFITS OF INTEGRATED DESIGN AND MANUFACTURING APPROACH

As most of the System, Subsystem and Detailed Design was carried in Work Centres in India, detailed knowledge and full understanding of the design and performance of LCA is available in India. LCA Systems are highly Software Intensive and most of Software including System Software was developed in India with full detailed documentation. This is an important aspect as during the development, integration and Flight Testing, significant software changes are needed to meet the Requirements changes and Certification needs.

After induction into Service and during its Service life, a Fighter Aircraft requires major modifications for the following reasons:

1. New Functional Requirements based on the changing threat perception and experience gained during service.

2. Up-gradation of Avionics (Life of Avionics is five to ten years due to obsolescence of Electronic Components)

3. For induction of new weapons on LCA-Tejas.

To implement all changes during the Life Cycle of a Fighter Aircraft System, Hardware and Software changes are needed. In LCA- Tejas this is easily carried out with minimum effort, cost and time because full System knowledge and design documentation of the Systems, Subsystems and Software is available with the Indian Team with full expertise and experienced Engineers are available in various Work Centres. For a nation like India it is essential to have the above capabilities to emerge as a Nation with full Force Multiplier Capabilities and to meet the changing and emerging threat scenario.

Figure 5. LCA- Tejas with full Weapon Load as a Force Multiplier

6. CONCLUSIONS

6.1 India has built up the capability to design and manufacture Fighter Aircraft by applying System Engineering principles and integrating design and manufacturing processes in a smooth flow. This is possible by integrating "Design in India" with "Make in India". This approach has resulted in a Fighter Aircraft for the Indian Air Force which is a Force Multiplier with latest technology, easy adaptation to multiple roles (Air Superiority, Air to Ground and Air to Sea), ease of carrying out up-gradation and integrating new weapons, and ease of maintenance.

6.2 With this approach, up-gradation of Avionics, integration of new weapons and introduction of any new functions in LCA required by IAF to meet new and emerging threats can be easily implemented with minimum cost and time frame, as all design details are available within India. With excellent menu driven Glass Cockpit, excellent Handling Qualities and very good Pilot Vehicle Interface (PVI), LCA- Tejas is definitely a Force Multiplier.

6.3 LCA- Tejas Naval Version with many common features with Air Force version adds to the Force Multiplier capabilities of Indian Navy. This is possible with the Integration of the Design and Manufacturing Capabilities of Indian Organisations and Industries.

6.4 Next generation Fighter Aircraft including Medium Range Combat Aircraft and Unmanned Combat Air Vehicle (UCAV) can be developed in shorter time frame based on the design and manufacturing expertise built in various

organisations within India. When these Aircrafts are developed and introduced into service along with LCA Tejas, they will form formidable Force Multiplier Capabilities for the Indian Forces. This is possible with the Integration of System Engineering, detailed Design and Manufacturing Processes within various organisations and Industries within India.

6.5 All these indicate that India in the verge of becoming a major Power in Aircraft Industry combing advanced Design and Manufacturing State of the Art Technologies.

It is strongly recommended that India prelaunch its National Civil Aircraft Program to design and develop and manufacture a 70-90 Seater Civil Aircraft. This Aircraft will also have a military version for the Indian Air Force, Navy and Army.

Octopod – The All-in-One Airborne Surveillance Pod

Dr. Theo Hengstermann

Optimare Systems GmbH, Bremerhaven, Germany

Abstract: *Starting with a brief introduction about the general design and layout of the Octopod, the specific capabilities and parameters of the integrated sensor systems and their particular contribution to different types of missions and its interaction and representation on the mission management systems Aero Mission or MEDUSA are described. This is done by explaining the different modes of operation and benefits of using different configurations of state-of-the-art remote sensors.*

1. INTRODUCTION

Protection of the EEZ and early detection of any kind of threats in the marine environment is the primary focus of Maritime Domain awareness. This does not only imply the protection of the coastal areas of countries against threats but also protection of their vital interest in their economic zone and the protection of the international shipping routes against terrorists attacks or piracy as well. The particular reasons for the increase of the awareness on the maritime domain are manifold and may cover such aspects like:

- Protection of the security economic zone against any threats coming from outside or any illegal activity
- Protection of the maritime environment against pollution or any other illegal over exploitation by human activities
- Protection of the national fishery grounds against illegal fishing activities
- Search & Rescue.

Within the concept of maritime domain awareness, airborne surveillance plays a vital role. Due to the potential severity of offenses and their partially massive and severe consequences, application of Airborne Maritime Surveillance is much more focused on prevention of potential offenses and deterrence than just on detection for later prosecution. The range of topics, which are widely addressed by Airborne Maritime Surveillance, covers

- Traffic observation;
- Smuggling including human trafficking and drug smuggling, contrabands;
- Anti-Terrorism;
- Illegal Migration;
- Protection of the Offshore Assets;
- Monitoring of the environment;
- …. and many more.

The task of a maritime surveillance aircraft is not just to detect contacts in the area of interest whether on the surface or submerged or to detect any illegal activity or threat against the marine environment. It is to interrogate those contacts and to establish whether they represent friendly/neutral platforms or threat platforms. The ability to detect, classify and identify maritime objects and to handle information effectively in real time is the major key to maritime domain awareness. Beside powerful sensor systems with high sensitivity and stability, above all sophisticated algorithms for data fusion are required to isolate from the sensor data those targets, which potentially represent a substantial threat from the harmless. It is important to note that on basis of the sensor data and the behavior of a certain target, it can be identified as a potential threat; but in nearly all cases, further intelligence (e.g. by EO/IR and visual inspection or even through surface action) is required to get the final proof.

In addition to these, more security related questions, airborne maritime surveillance aircraft also significantly contribute to the safety of the maritime environment. On one hand, maritime surveillance aircraft are widely used to detect any illegal pollution of the sea; on the other, they are a significant part of the contingency measures because of their capability to deliver qualitative and quantitative information on pollution found at sea, thus laying the basis for a rapid and efficient recovery operation.

According to the manifold of different tasks to be followed by airborne assets, it has become more and more common to implement complex sensor configurations together with sophisticated mission management systems to account for the increasing number of possible threats arising from the strongly increasing vessel traffic and exposure of offshore assets due to exploration activities. A situation, which has led to an increasing demand for truly multipurpose maritime surveillance aircraft. One major step towards a real multipurpose maritime mission system is the unique, ground-breaking all-in-one belly mounted OctoPod, which combines up to eight well-proven sensor systems supporting more than 20 different mission tasks.

Due to the belly mounted concept of the OctoPod the cabin is almost kept free from sensor installations, thus leaving the space for other complementary equipment for additional mission capabilities like ESM or ASW. The space may even been used to open the aircraft for other roles like Medical Evacuation.

2. THE OCTOPOD

The cumulated experiences from more than 20 years providing sensors and mission systems for airborne maritime surveillance have finally led to the design of the OctoPod, which as a central requirement should not only provide all necessary components for a multi mission aircraft but also leaving the space for truly multi role capability.

The missions to which the development has targeted for are,

- Airborne maritime surveillance
- Airborne environmental surveillance and oil spill detection
- Search & Rescue
- Airborne land surveillance

With the configuration shown in Figure 1, the OctoPod comprises the following **Core Features**

- **Multi-Functional**
  - Eight core functionalities based on eight selected sensors, which are used cross-sectional over 20 different mission tasks
- **Belly-Mounted**, which results in
  - low effort for aircraft modification & certification and
  - Low impact on the aircraft's cabin
- **Multi-Platform**
  - The vertical pod dimension stays within the ground clearances of the most prominent surveillance platforms
- **Modular**
  - The configuration can be adjusted individually configured from subset to full configuration to meet the specific requirements of the potential customers
  - Removable
  - Low effort for aircraft reconfiguration

Fully Integrated

  - The OctoPod is fully integrated with the mission management systems AeroMission and MEDUSA of the Aerodata company group.

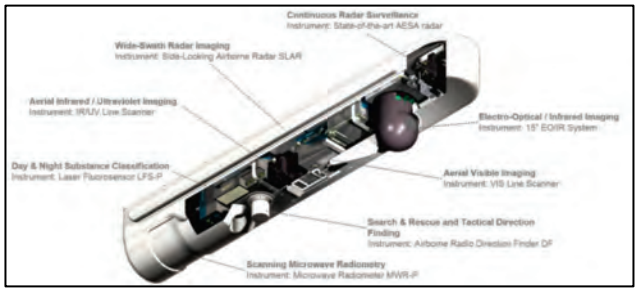


Figure 1. Configuration of the Octopod

2.1 Sensor Configuration of the Octopod

To guarantee the requested performance and the capability for multi mission operation, the OctoPod is equipped with the following sensor suite (Figure 2)

Figure 2. Sensor Suite of the Octopod

2.1.1 Search Radar

The Search Radar is the primary sensor of almost any maritime or ground surveillance mission allows the detection of even small targets at long distances even under harsh environmental conditions.

Due to its wide distribution, there are numerous different radar systems available from quite a number of different suppliers. In case of the OctoPod, the Selex Seaspray 5000E has been chosen, which due to its modern AESA antenna design gives an optimum compromise between size and performance.

The Seaspray 5000E is an X band radar system that combines the Seaspray common processor with a compact AESA antenna mounted on a dual axis mechanical scanning pedestal. The radar provides a full range of maritime surveillance and coherent imaging modes optimized for a wide range of operational scenarios, from high altitude long-range surveillance and target classification to lower level shorter-range surveillance of smaller targets.

To balance the trade-off between swath depth and resolution, multiple levels of resolution are provided: the higher the resolution, the narrower the swath being imaged. The Seaspray 5000E Strip SAR Mode provides a swath depth of 20 nm at the highest resolution of 10 m. In Spot SAR

mode two patch sizes can be selected, 1 km x 1 km patch size with 1 m resolution and 500 m x 500 m patch size with 0.5 m resolution.

Seaspray 5000E provides an ISAR mode with selectable resolutions and integration times for target imaging and classification purposes. Entry into this mode is accomplished by first designating a target and then selecting the ISAR function. Range profiling of tracks is also available to support target classification (Fig. 7).

A MTI mode is provided that permits the operator to detect and display ground and sea surface moving targets. In this mode, the radar detection plots produce estimates of target bearing, range and range rate, with the corresponding derived position reported in latitude and longitude.

MTI plots are output as a plot list and can easily be presented as a layer on top of any other mapping system. Clearly, as indicated, the MTI mode accurately detects and reports vehicle road traffic over a wide area.

Figure 3: Surface MTI Plots overlaid On To a Standard Map

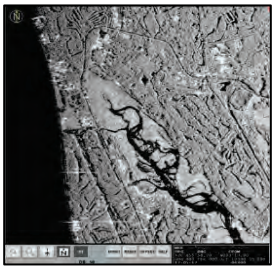


Figure 4: Strip Map SAR

2.1.2 Automatic Identification System

Although not directly part of the OctoPod, each installation also includes an Automatic Identification System (AIS) as part of the mission management system. The performance of maritime search radar can be significantly increased by automatically correlating the radar and the AIS tracks. This correlation is a feature of the mission management system, which also provides sophisticated filter algorithm to remove or highlight particular targets and to structure the radar image by classification of the targets.

2.1.3 Electro-optical/Infrared System

The EO/IR system is the primary system for video documentation and inspection and identification of targets even during the night (Figure 16). The OctoPod is capable of integrating almost any EO/IR system from different supplier up to a size of 15 inches.

2.1.4 Search & Rescue and Tactical Direction Finder

The lightweight, compact and rugged direction finder system RHOTETA RT-600A is specifically designed to receive and interrogate all current international distress frequencies including 121.5 MHz, 243 MHz, 406 MHz, as well as ARGOS and COSPAS-SARSAT encoded beacon signals. The receiver hardware is completely contained in a pot-like antenna mounted on the lower side of the OctoPod. When integrated over the ARINC 429 data busses, the RHOTETA RT-600A 430 can provide the beacon's latitude and longitude along with its unique identifier. The RT-600A direction finder is provided including the broadband options that extends the VHF and UHF frequency coverage.

2.1.5 Side-Looking-Airborne Radar

Far-range detection of oil spills is the absolute domain of the Side-Looking-Airborne Radar (SLAR), which is a cloud-penetrating X-band radar technique of real aperture type. At an aircraft altitude of about 300 m, SLAR systems usually have a cross-track coverage between 60 and 80 km. Oil spill detection using airborne radar is generally based on the principle that oil spills as well as biogenic surface films (even monomolecular films) and hydrodynamic effects may reduce the radar backscatter due to dampening of gravity-capillary waves of the sea

surface. SLAR is an indispensable tool for maritime surveillance. An example of SLAR data displayed in OPTIMARE's MEDUSA Analysis Software Tool is shown in Figure 10.

Due to its high sensitivity against any changes in the roughness of the sea surface, SLAR can also be used to detect small high-speed boats by their wake.

2.1.6 IR/UV Line Scanner

Infrared/Ultraviolet imaging devices like IR/UV line scanners are standard instruments for near-range monitoring of oil spills. These devices are usually sensitive in the thermal infrared (8 μm-14 μm) and the near ultraviolet (320 nm - 380 nm). At an aircraft altitude of 300 m, the swath width of a typical IR/UV line scanner amounts to about 500 m.

Films of crude oil on the water surface can be detected in the thermal IR because (a) oil has lower integral emissivity than water in this spectral region and (b) oil, particularly crude oil, can be heated through absorption of sun light if they are sufficiently thick (A. Fontanel and A. Roussel, 1979).

Reported values of the minimum detectable oil film thickness in the thermal IR range from 2 μm to 70 μm (N. Robbe, 2005). Hot spots, which are generated through absorption of sun light by the oil, are assumed to appear in the thickness range between 50 μm and 500 μm. This at least allows a distinction of areas within an oil spill with different thickness.

Near UV remote sensing of oil spills is based on the fact that the air/oil interface of the oil film has about twice the integral near UV reflectance of the unpolluted sea surface. Assuming that sufficient visibility and daylight illumination are given, very thin sheets of oil can be mapped using near UV sensors. The minimum detectable oil thickness in this wavelength region amounts to 0.01 μm (M.F. Fingas and C.E. Brown, 1997).

False targets such as biogenic slicks, foam or sun glints may interfere. Recent research work suggests that the UV signal measured above an oil spill can be used for fusion with optical thickness data measured with a laser Fluorosensor (N. Robbe, O. Zielinski, 2004). Combined IR/UV devices show the areas of intermediate and large oil film thickness as well as the total extent of the oil spill (Figure 11).

2.1.7 VIS Line Scanner

VIS line scanners have been established as auxiliary tools for various airborne remote sensing applications, like for example, airborne maritime surveillance.

The OPTIMARE VIS Line Scanner (VIS LS) is a ruggedized, lightweight remote sensor for earth observation at visible wavelengths (400 - 700 nm). In maritime surveillance, the system is used for acquisition of highly resolved geo- referenced Red/Green/Blue composite images. These images can be used for documentation and for more exact volume estimations based on oil appearance codes. Some effort has been spent on the development of oil appearance codes, i.e., the interpretation of the color appearance of oil spills in terms of oil layer thickness. Red-Green-Blue (RGB) line scanners combine high mapping accuracy with the acquisition of color information and thus allow more accurate volume estimations based on oil appearance codes. One popular color code that connects color appearance on an oil film to the oil film thickness and which is frequently used is the Bonn Agreement Oil Appearance Code (BAOAC).

Code	Description Appearance	Layer Thickness Interval (μm)	Litres per km²
1	Sheen (silvery/grey)	0.04 to 0.30	40 – 300
2	Rainbow	0.30 to 5.0	300 – 5000
3	Metallic	5.0 to 50	5000 – 50,000
4	Discontinuous True Oil Colour	50 to 200	50,000 – 200,000
5	Continuous True Oil Colour	200 to More than 200	200,000 - More than 200,000

Fig 5: Bonn Agreement Oil Appearance Code (BAOAC) (A. Lewis, 2007)

2.1.8 Microwave Radiometer

Microwave radiometers (MWRs) are passive microwave remote sensors, which are used to map oil layers exceeding a thickness of ~50 μm. Oil spills appear as brighter objects in the microwave region relative to the oil-free sea surface. The reason for this is a positive emissivity difference between oil and water in this wavelength range. Multi-frequency MWRs can be used for measurements of the oil film thickness (Ulaby et al., 1986). MWRs like those that are installed on the German and Spanish Maritime Surveillance aircraft are capable of measuring the absolute oil layer thickness in the range from ~50 μm to ~3000 μm. At an aircraft altitude of 300 m, their swath widths amount to about 500 m. However, there is no limitation with respect to the aircraft altitude. MWR like IR, UV and VIS sensors can be flown also at much higher altitudes. However, it has to be taken into account that with increasing altitude the ground resolution of the image will decrease. Unlike IR, UV and VIS sensors, MWRs are all-weather sensors, which can even look through dense cloud layer. Examples of oil spills measured with the Microwave radiometer are shown in Figs 12, 13.

2.1.9 Laser Fluorosensor

At present remote classification of oil spills is only possible using laser fluorosensors.

Laser fluorosensors (LFSs) for oil spill monitoring are based on high power UV lasers which send short laser pulses (5-20 ns) towards the water surface. The laser-induced fluorescence and back scatter are received by a telescope and separated spectrally into a limited number of monochromatic signals. According to several studies, (J.F. Fantasia et al., 1971; T. Hengstermann and R. Reuter, 1990; T. Hengstermann, 1992; F.E. Hoge, and R.N. Swift), the detected discrete emission spectrum can be used to estimate the oil class and to measure the thickness of optically thin surface films of crude and refined oil. Two German maritime surveillance aircrafts are equipped with an imaging LFS called Imaging Airborne Laser Fluorosensor (IALFS). At an aircraft altitude of 300 m, the swath width of this instrument amounts to ~150 m. In contrast to the German maritime surveillance aircraft, the Spanish maritime surveillance aircraft are equipped with a profiling instrument delivering thickness data and oil classification in the nadir of the aircraft with a resolution of 10 Hz.

The capabilities of the Laser Fluorosensor include

- Detection of laser-induced fluorescence of crude oils, petroleum products and water constituents
- Classification and mapping of crude oils, petroleum products and chemicals spilled at sea
- Detection of crude oils, petroleum products and chemicals floating underneath the water surface
- Measurements of oil film thickness over very thin (optically thin) oil layers
- Distinction of naturally occurring biogenic slicks from oil spills
- Hydrographic measurements (CDOM, turbidity, chlorophyll-a).

An example of measurements of the laser Fluorosensor on an oil spill is shown in Fig. 14.

3. MAJOR MISSIONS

The following section describes typical missions for which the OctoPod has been designed for and gives a description of the typical workflow during each type of mission.

3.1 Securing Evidence

Securing evidence of a given offense is one of the primary tasks of almost any aerial surveillance asset when operated for maritime surveillance, environmental surveillance or border or fishery

patrol, whether the offense has been detected during normal routine flights or is an outcome of response flight.

Very high standards of evidence have to meet the threshold demanded by the courts. The court will need to be certain that the surveillance equipment on board the aircraft is accurate and has been used properly by qualified crew. The crew will need to give credible witness statements in support of any photographic or video evidence, as well as evidence collected from the sensor data or of their own observations. A direct chain of evidence needs to be maintained in a way that the court can be assured that there has been no tampering or contamination of evidence subsequent to the patrol but prior to the court proceedings. This means that the way in which the data have been gathered and processed is transparent, well documented and any precautions has been taken to prevent any tampering in the whole chain of evidence.

Data that are to be provided in case of an observation are:

- Position of the vessel or potential offender
- Tactical situation display marking the position of the ship with respect to possible restricted areas / boundaries of the EEZ
- Time of observation
- Radar Images showing the vessel
- ISAR Image (if available)
- EO/IR Images and videos showing the vessel in detail
- Images providing the reading of the ships name taken with EO/IR or still camera

All Images have to be provided with data annotation of position, altitude, heading, time.

If a potential offense has been detected, all data need to be persistently secured in an archive. If during a mission no offense has been detected, the data should be archived after the mission for a defined period of time to allow an access to the data in case that a potential offense has been detected by means of other surveillance activities e.g. by surface forces or satellite images.

3.2 Maritime Surveillance

Protection of the EEZ and early detection of any kind of threats in the marine environment is the primary focus of Maritime Surveillance. Within the concept of Maritime Surveillance, the airborne segment plays a key role.

Due to the potential severity of offenses and their partially massive severe consequences, application of Airborne Maritime Surveillance is much more focused on prevention of potential offenses and deterrence than just on detection for later prosecution. The range of topics to be addressed by Airborne Maritime Surveillance covers

- Traffic observation
- Smuggling including human trafficking and drug smuggling, contrabands
- Anti-Terrorism
- Illegal Migration
- Protection of the Offshore Assets

The task of a maritime surveillance aircraft is not just to detect contacts in the area of interest whether on the surface or submerged. It is to interrogate those contacts and to establish whether they represent friendly/neutral platforms or threat platforms. The ability to detect, classify and identify maritime objects and to handle information effectively in real time is key to maritime domain awareness. Beside powerful sensor systems with high sensitivity and stability, above all sophisticated algorithms for data fusion are required to isolate from the sensor data those targets, which potentially represent a substantial threat from the harmless. It is important to note that on basis of the sensor data and the behavior of a certain target, it can be identified as a potential threat, in nearly all cases further intelligence (e.g. by EO/IR and visual inspection or even through surface action) is required to get the final proof.

Depending on the type of mission, different procedures apply. While during Scheduled Missions, the focus of the operation is on the detection of potential offenses, during Response Missions the fact of an offense is already given and the focus of the operation is to collect unambiguous evidences for later prosecution of the offender and to support surface forces to intercept the offender.

The high number of targets makes it necessary to apply sophisticated algorithms to detect possible anomalies. By validation of the information coming from the different data sources and by comparison of the behavior of the targets with predefined pattern (speed, direction, position with respect to the boundaries of the EEZ, AIS, vessel size, etc.) potential offenders can be visualized in the tactical situation display. By use of the ISAR images provided by the Surveillance Radar and images from the EO/IR in conjunction with data and images from the vessel database, a potential offender will be identified and the status of its activity is investigated. The typical workflow of a programmed patrol mission is shown in Figure 7.

The primary sensors or elements of the mission system used for this mission are,

- Surveillance Radar,
- AIS,
- EO/IR
- Data from a Vessel Monitoring System (VMS)
- Internal vessel data base of the mission management system
- Tactical situation display with an indication of the restricted areas

In addition to this, also information, which has been collected prior to the mission, may be available.

Figure 6: Tactical situation display showing different types targets on a Moving Map Display. Via context sensitive display the operator is able to get target specific information

In contrast to Scheduled Missions, which follow a given schedule, Response Missions appear asynchronously to the normal flight schedule. Response Missions are carried out if an offense has been detected e.g. through information from a different source of information (e.g. satellite imagery, intelligence reports, reports from surface forces, etc.).

Additionally to this, Airborne Maritime Surveillance is also predestinated to support coordination of surface operations. In this case, extensive communication (voice and data) is required. Sensor imageries, the tactical situation displays and video can be sent to surface forces.

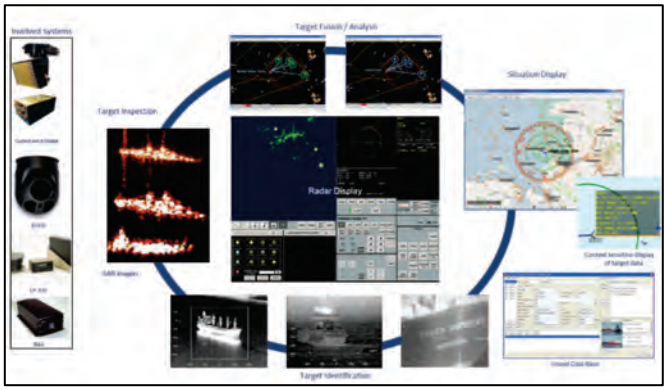


Figure 7: Typical workflow Cycle for Maritime Surveillance mission

3.3 Fishery Patrol

Fisheries and aquacultures are a major earner for many countries and are a major source of food and income particularly in the developing countries. The sector's share of gross domestic product exceeded a value of 78.9 million tons in 2011 (World Ocean Review 2). Given the value of this resource and its importance for the countries' economy, effective maritime surveillance is required to protect these natural assets. Fishery is a limited resource. Most people accept that if we want to sustain our fisheries for future generation, a responsible management of this resource is required. This management includes the operation of an effective compliance regime, of which surveillance is an integral and indispensable part.

In many countries, fishery patrol is organized in a layered model consisting of different layer of information as shown in Figure 8. In many cases, a potential offense may only be detected by fusing the information from the different layers of information as shown in the Figure 8. This means that for the most successful approach there is the need for a networked concept of operation for airborne Fishery patrol operations.

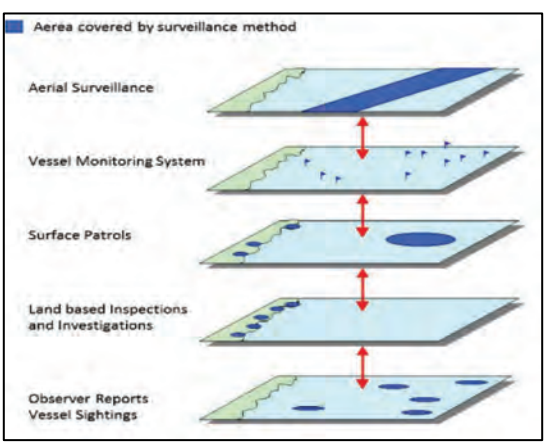


Figure 8: Layered Model Of Fishery Patrol Practiced In New Zealand (Adopted From "Maritime Patrol Review, 2000).

Similar to maritime surveillance two different categories of missions exist: Programmed and Response Patrols, which again may be break down into different sub-categories of missions.

Depending on the type of mission, different procedures apply. While during Programmed Patrols, the focus of the operation is on the detection of potential offenses, during Response Patrols the fact of an offense is already given and the focus of the operation is to collect unambiguous evidences for later prosecution of the offender.

The primary sensors or elements of the mission system used for these mission are the

- Surveillance Radar,
- AIS,
- VMS,
- Internal vessel data base of the mission management system,
- Tactical situation display with an indication of the restricted areas.

In addition to this, also information, which has been collected prior to the mission, may be available (reporting from other information layer according to Figure 9).

By plausibilization of the information coming from the different data sources and by comparison of the behavior of the targets with the expected behavior of a fishing vessel (speed, direction, position with respect to the boundaries of the restricted area, AIS information, vessel size) potential offenders can be visualized in the tactical situation display. By use of the EO/IR in conjunction with data from the vessel database, potential offenders are identified and the status of their activities is investigated. Figure 9 shows the typical workflow of a programmed patrol mission.

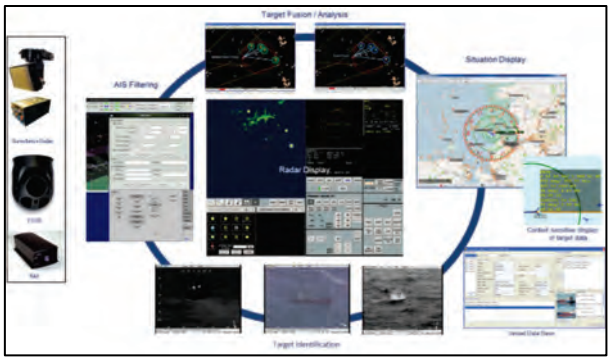


Figure 9. Typical workflow cycle of a programmed fishery patrol mission

3.4 Environmental Monitoring

Airborne pollution control has long become an international affair and a key element for the protection of the marine environment. Legal, ecological and economic effects of marine pollution by ship traffic and platform discharges have been important arguments for many coastal nations worldwide to establish or expand airborne maritime surveillance also to oil spill detection capabilities.

Airborne pollution control allows a spatio-temporally flexible investigation of local characteristics of marine pollution, especially by oil spills, and thus enables response crews to rapidly assess the situation at the pollution site, leading finally to an increased response efficiency. In addition to decision-making support these airborne services also fulfill tasks like deterrence of potential polluters and securing evidence for prosecution. Although in many countries more than 90 percent of the daily operation is related to the two latter aspects, in most countries the pollution detection capability is considered the genuine value in terms of contingency planning.

The scope of a pollution control suite for a maritime patrol aircraft is determined by the requirements of the application concerning detection, mapping, classification, and quantification of marine pollution. Standardized in-flight reporting in conjunction with data downlink for instance by satellite communication is the first element in the chain of evidence, which supports the prosecution.

Basically, there are two different scenarios for Airborne Oil Spill Detection, which have an impact on the system configuration, the mission strategy and the mission profile.

- Accidental discharges of Oil from ships or from Off-Shore Platforms
- Illegal release of oil from ship traffic

In case of accidental discharges, regularly huge amount of oil is discharged to the sea. The primary goal of the mission is to provide quantitative data about the oil spill to allow a most accurate assessment of the current situation and to contribute to the overall situational awareness. Moreover, by use of data taken at different points in time (e.g. during different missions) also an assessment of the dynamic development of the situation can be derived.

Data, which are required to support marine crisis management and in addition to support cleanup-operations are:

- Position and aerial extend of the oil spill or positions if the spill is already broken into different oil patches (Figure 11)
- Detection of Hot Spots for coordination of oil spill recovery (Figure 12)
- Thickness distribution of the oil spill or patches respectively(Figure 11)
- Volume of the oil (Figure 13)
- Drift
- Spreading
- Oil Type to verify if only one or different sources contribute to the oil spill (Figure 14)

For an efficient marine crisis management, it is important that particularly in the very first moment of a disastrous discharge of, oil quantitative data on the situation are made available. The general requirement therefore should be, that at least one aircraft with suitable

equipment on board arrives on scene at least 4 hrs after the emergency call has arrived and that at least after 6 hrs first quantitative data are available in the emergency center.

The primary sensors for the approach of the oil spill are the 360^0 Surveillance Radar and the Side-Looking-Airborne Radar (SLAR). While the SLAR shows the oil in an extended area on the water surface, the 360^0 Surveillance Radar provides an overview on the ship traffic. Due their wide coverage, these sensors provide a synoptic overview of the situation, showing the oil slick on the sea surface, ships and offshore installations.

To help the operator to distinguish between the different Radar targets and to structure the overall situational awareness, each target may be identified and labeled using AIS data. With powerful filter algorithms provided by the AIS tool of the Mission Management System, the operator can distinguish e.g. between the response vessels and other ship traffic or identify target which may cause additional threats e.g. tanker etc. in an emergency situation (Figure 10).

Depending on the situation, also the EO/IR system may be used in order to visually verify a certain target or to collect evidence of a particular observation (Figure 16).

According to the updated flight plan from the situation overview near range mapping of the oil spill is carried out. The main goal of this phase of a mission is to collect quantitative data from the oil slick. A possible flight path to cover the entire oil spill considering also wind data is shown in Fig. 15.

The following sensor systems are involved in this phase:

- SLAR — Overview (Figure 10)
- IR/UV/VIS — Position, Area, rel. Thickness Distribution (Figure 11)
- MWR — Thickness Distribution in abs. Units, Volume Calculation, Hot Spot Detection and –Localization (Figures 12, 13)
- LFS — Oil Type Classification, Thickness Measurement of Thin Oil Films (Figure 14)
- EO/IR — Securing Evidence, Documentation (Figure 16)

If there are already data available from previous missions, the dynamic parameters of an oil pollution like drift and spreading are derived. This requirement also underlines the necessity for a multi mission data handling on board of the surveillance aircraft.

Beside the sensor data, which prove that a given observation presents a violation in terms of substance type, volume etc. additionally video documentation from the potential polluter will be taken. These videos will allow the identification of the potential polluter e.g. by reading the ships name (Fig. 16).

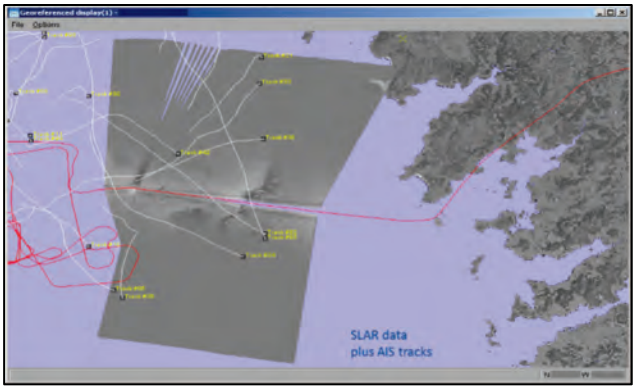


Figure 10: SLAR Image overlaid on a Satellite Imagery, flight track (red line) and ship tracks (white lines) calculated from AIS data

.

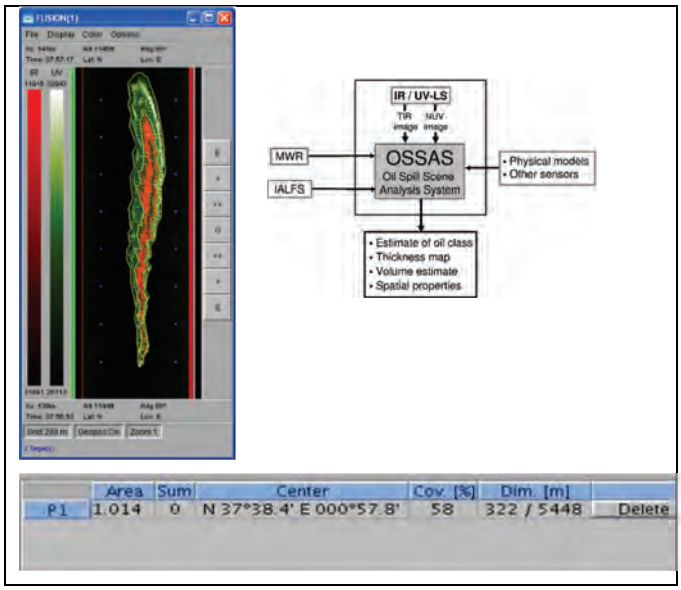


Figure 11: Calculation of the Position and the Areal extend of an oil spill using the data of the IR/UV Line Scanner. Fusion of the data from the UV and from the IR already allow a first assessment of the relative thickness distribution of the oil spill on the sea surface. Calculation is done without any necessary interaction of the operator through the OSSAS.

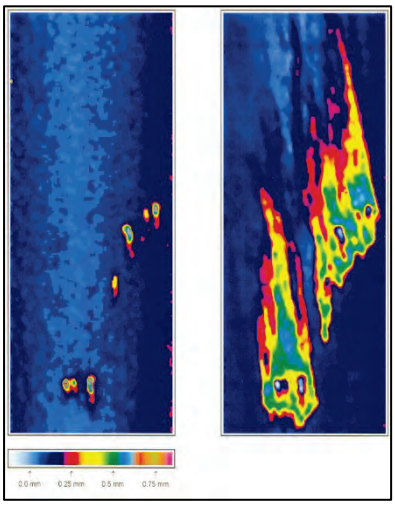


Figure 12: Hot Spots with the main concentration of oil detected with the microwave radiometer

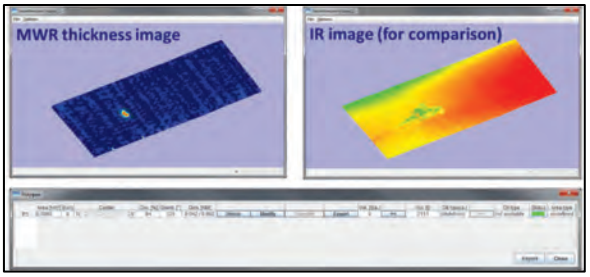


Figure 13: Calculation of the Volume of an oil spill by means of the Microwave Radiometer. In the case SHOWN, the total volume of oil that has been spilled to the sea was about 3000l. Calculation of the Microwave radiometer leads to a volume of 3111l again confirming that most of the oil is located in small patches.

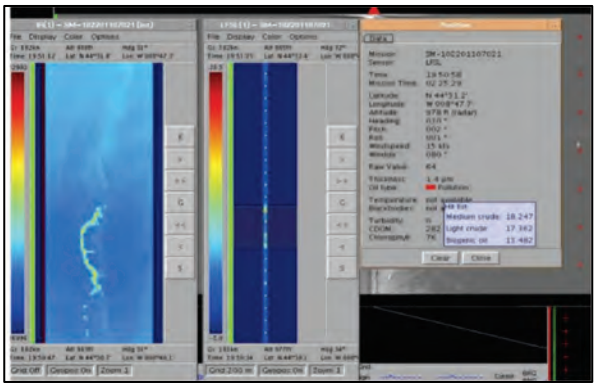


Figure 14: Classification of the Oil Type of a Real Oil Spill as Medium Crude Oil (Left). Classification Scheme of Lfs (Right)

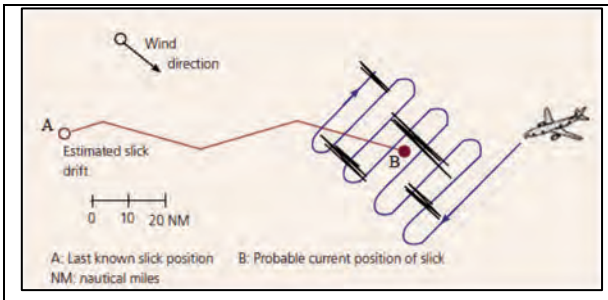


Figure 15: Possible flight track on an oil pollution Taken from Aerial Observation of Oil Pollution a Sea, Operational Guide, CEDRE)

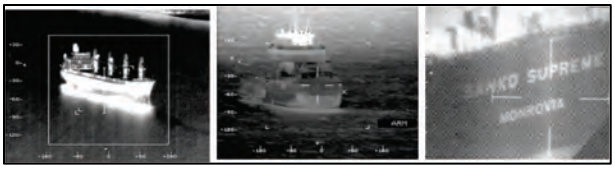


Figure 16: Securing evidence after an observed violation by video documentation of potential polluter

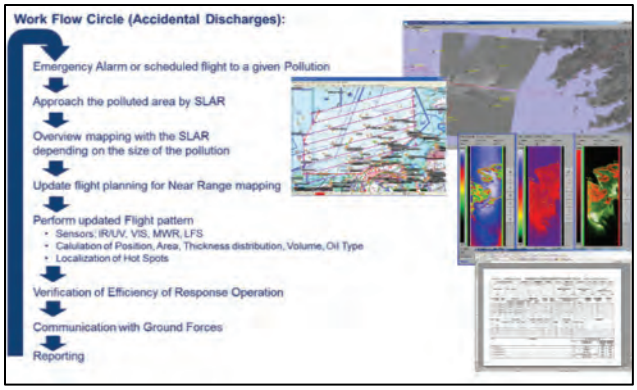


Figure 17: Mission Work Cycle for Maritime Pollution Detection Mission in case of Accidental Discharges

4. SUMMARY

Airborne maritime surveillance has long proven to be an indispensable part of modern concepts to encounter the manifolds threats in the maritime environment and laying the fundament for comprehensive maritime domain awareness. According to the manifold of different missions and mission tasks to be followed by airborne assets, it has become more and more common to implement complex mission system environment together with a set of sophisticated sensor systems on board of the aircraft to account for the increasing number of possible threads arising from the strongly increasing vessel traffic and exposure of offshore assets due to exploration activities. This led to an increasing demand for truly multi-mission systems covering the whole bandwidth of the different missions and mission tasks.

One major step towards a real multipurpose maritime mission system is the unique, groundbreaking all-in-one belly mounted OctoPod as it has been introduced in this paper. Its modular layout allows tailoring the configuration of the OctoPod exactly to the requirements and needs of the customer. The unique design of the OctoPod even allows using the Pod cross-sectional among different aircraft of a fleet giving the most flexible and cost and space economic solution for these applications.

Bibliography

1. Grüner K., Reuter, R. and Smid, H., “A new sensor system for airborne measurements of maritime pollution and hydrographic parameters“, GeoJournal, Vol. 24, No. 1, pp. 103-117, 1991.
2. Zielinski, O., “Airborne Pollution Surveillance Using Multi-Sensor Systems.” Sea Technology, Vol. 44, No. 10, pp. 28-32, 2003.
3. Robbe, N., Hengstermann, T., “Airborne Oil Spill Remote Sensing: Why Multi-sensor Technology is Key for Maritime Surveillance.” Hydro International, April 2008 Issue, Volume 12, No.2, ISSN 1385-4569, 2008.
4. Robbe, N., Hengstermann, T., Remote sensing of marine oil spills from airborne platforms using multi-sensor systems. Proceedings of the Water Pollution 2006 Conference, Bologna, Italy, 2006.
5. Fontanel, A. & Roussel, A., La détection des nappes d’hydrocarbures sur la mer. Oceanis, 4, pp. 673–691, 1979.

6. Robbe, N., Airborne Oil Spill Remote Sensing: Modelling, Analysis and Fusion of Multi-spectral Data. Ph.D. thesis, Institute of Experimental Physics, University of Hamburg, 2005
7. Fingas, M.F. & Brown, C.E., Review of Oil Spill Remote Sensing. Spill Science & Technology Bulletin, 4(4), pp. 199–208, 1997
8. Robbe, N., Zielinski, O., Airborne remote sensing of oil spills – analysis and fusion of multispectral near-range data. Journal of Marine Science and Environment, (C2), 2004
9. Lewis, A., Current Status of the BAOAC (Bonn Agreement Oil Appearance Code). A report to the Netherlands North Sea Agency Directie Noordzee, 2007
10. Ulaby, F.T., Moore, R.K. & Fung, A.K., Microwave Remote Sensing: Active and Passive, volume III. Artech House, 1986.
11. Fantasia, J.F., Hard, T.M. & Ingrao, H.C., An investigation of oil fluorescence as a technique for the remote sensing of oil spills. Technical report, DOT/Transportation Systems Center U.S. Coast Guard, 1971. Report TSC-USCG-71-7.
12. Hengstermann, T. & Reuter, R., Lidar fluorosensing of mineral oil spills on the sea surface. Applied Optics, 29(22), pp. 3218–3227, 1990.
13. Hengstermann, T., Untersuchungen zur Laserfernerkundung mariner Ölverschmutzungen. Ph.D. thesis, Department of Physics, University of Oldenburg, 1992.
14. Hoge, F.E. & Swift, R.N., Oil film thickness measurement using airborne laser-induced water Raman backscatter. Applied Optics, 19(19), pp. 3269–3281, 1980.
15. The National Compliance Unit, Review of Maritime Patrol Requirements, Ministry of Fisheries of New Zeeland, 2000
16. Aerial Observation of Oil Pollution at Sea, Operational Guide, CEDRE
17. The Future of Fish – The Fisheries of the Future, World Ocean Review 2, 2013

Harnessing Technology to Meet Coastal Security Challenges

Comdt K C Singh
JD Com (P&P)
Coast Guard Headquarters

1. Introduction

1.1 Oceans play an important role in the politico-economic and strategic affairs of a maritime state. Thus India is regarded by many strategist as one of the highly advantaged peninsular maritime countries, which sits astride the interjection of vital Sea Lines of Communication (SLOCs) passing through the Arabian Sea, Indian Ocean and the Bay of Bengal. Considering the volatile geopolitics of the Indian Ocean Region (IOR), presence of strategic chokepoints critical to our energy needs and overall maritime security paradigm, it is incumbent upon us to ensure that our national interest in the maritime domain is protected at all times. Besides safeguarding our economic and trade interests in the IOR, it is equally important to prevent any security breach along our porous coastline.

1.2 The conventional maritime interests in the Exclusively Economic Zone (EEZ) include security of offshore hydrocarbon reserves, non-conventional energy potential, and other living and non-living resources of the sea, including fish and the mineral wealth on the seabed. However, considering the dependence of our economy on ocean trade, safety of SLOCs and Maintaining, general good order in our maritime zones has also emerged as priority areas.

1.3 The weightage being assigned to the maritime trade and shipping is amply reflected in the national vision of developing port and boosting coastal trade through the "Sagarmala" project. The shipping industry is accordingly being promoted and ports of all sizes and ownerships are being created to meet cater for envisaged increase in the maritime trade. It may well be appreciated that a significant increase in the shipping traffic density in our maritime zones is on the cards. In addition to the merchant marine, numerous coastal freighters and traditional/ mechanised sailing dhows also contribute significantly to the congestion of our maritime environment.

1.4 The Indian fishing industry is also the sixth largest in the world with a fleet strength of almost 300,000 boats of various shapes and sizes, which land their catch at one of the six major fishing harbours, 41 minor fishing harbours and 180 odd fish landing sites along the coast. Other than these known landing areas, most traditional boats, engaged in near shore operations, land their catch at opportune creeks/ fishing landing centre or open spaces.

1.5 These factors, when examined in totality, pose a complex surveillance challenge for the Indian maritime agencies. Besides the increased probability of inadvertent accidents/ collisions the cluttered maritime domain, also provides an opportune disguise for possible infiltration by nefarious elements. Additionally, challenges like seaborne smuggling; armed robbery/ piracy, unregulated fishing, straying of fishermen across IMBL also have a significant bearing on our coastal security Concerns. It is apparent that identification of a rogue vessel amongst the numerous innocuous ships/ boats thus remains a serious challenge to our surveillance efforts.

1.6 It may be evident from the above prologue that the ill-defined and complicated maritime environment poses a big challenge for maritime security in general and coastal security in particular. Situational awareness being the key, emphasis is on sustained surveillance. However, the vast sea-areas of interest, which becomes highly opaque in adverse meteorological conditions, cannot be kept under physical surveillance by ships an aircrafts on 24x7 basis. Besides being a considerably expensive proposition both in terms of Capital and Operational costs, these efforts are also limited by the vagaries of weather. Moreover, differentiating friend from foe in the maze of traffic comprising neutrals exercising their freedom of navigation is a huge challenge. Any of the tens of thousands of fishing boats that return back from sea each day, to any point along the coastline, may be a threat vector. Similarly the thousands of container ships and cargo vessels that call at our ports, or transit through sea areas of our interest either along our coast or along the established SLOCs, can be a potential threat. Physical checking of each and every passing/ transiting boat/ ship is unviable. Besides being time consuming and risky, it also reduces the effective time on patrol of the deployed units thereby limiting the surveillance effort.

2. Chain of Static Sensors: Phase-I

2.1 Introduction

Securing the country's coastline and protecting our maritime interests thereof requires a comprehensive approach, which effectively dovetails the available technology into the operational philosophy to accrue the maximum dividend from the limited resources at disposal of the maritime security agencies. The Chain of Static Sensors project is one such example, wherein technology has been enmeshed in the surveillance matrix to enable automated detection and verification of vessels/ boats plying in our coastal waters and sharing, fusion, and analysis of accumulated data in real time so as to present a common operating picture to all stake holders**.**

2.2 Background

The seeds of the present coastal security network were probably sown soon after the Kargil war, wherein a Group of Ministers (GoM) was set up to suggest measures on reforming the national security apparatus. The GoM on reforming the national security system post Kargil conflict recommended that "A Chain of Static Sensors may be set up in the form of shore radar stations, in areas of high sensitivity and high traffic density'. In order to implement the GoM recommendations subsequently a working group constituted by the MoD recommended the installation of Radars on light houses at 38 places along the coast of India. The need for a comprehensive coastal security mechanism, once again became the focus of public debate and political attention after the unfortunate incidents of 26/ 11, which in turn paved the way for implementation of India's first comprehensive Coastal Security Network.

2.3 Operational Role

2.3.1 The Chain of Static Sensors had been steered by the Indian Coast Guard and executed by M/s BEL, Bangalore with active and whole hearted support of the Directorate General of Light Houses and Light Ships (DGLL)/ MoS. The network is designed for round the clock electronic and optical surveillance of areas of high sensitivity and high traffic density along the Indian Coast upto 25 nm and 15 nm respectively. The system is configured for automatic monitoring of all vessels transiting/ operating within the defined detection ranges. The data with respect to the detected targets is further verified/ corroborated through Automatic Identification Systems (AIS) feed being contributed by the National AIS Network of DGLL.

2.3.2 The purpose of Coastal Surveillance Network is to provide an integrated picture of target movements in the sea, around the mainland and the islands along the coast line of India. This provides the user the full Situational Awareness of the coverage area and helps to take measures to identify and neutralize possible threats/ contacts of interest through positive interdiction.

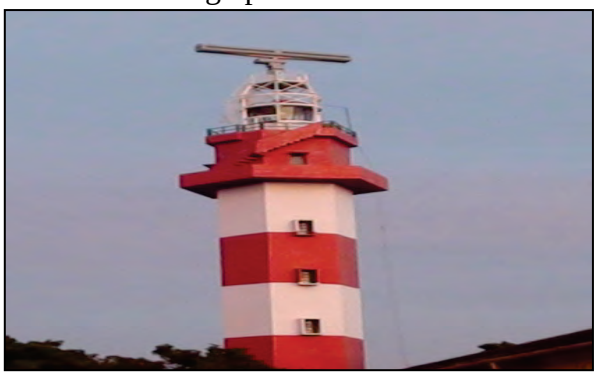


Fig. 1. Sensors installed on lighthouse

System Architecture

2.3.3 The project involved setting up of Radar Stations at 36 locations on mainland, 06 locations in Lakshadweep Islands and 04 in Andaman and Nicobar Islands. These Radar Stations have been established either on the existing light houses of DGLL or on masts erected on the DGLL land. Each Radar Station is linked up to the nearest Indian Coast Guard Stations/ District Headquarters known as Remote Operating Stations (ROS) through leased lines/ VSAT overlay.

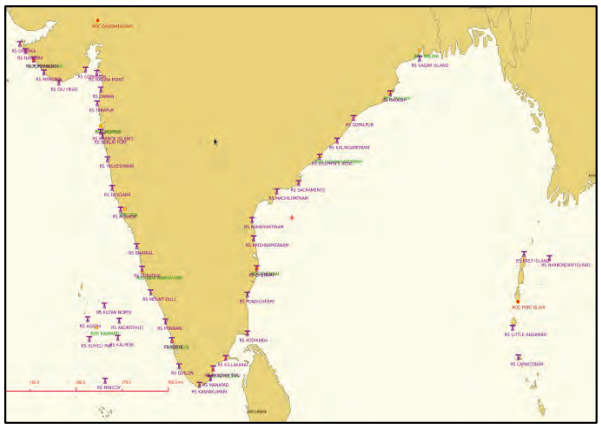


Fig. 2. Radar Stations: Phase-I

2.3.4 The ROS is further linked up to the Regional Operating Centers (ROC) collocated with Coast Guard Regional Headquarters at Gandhinagar, Mumbai, Chennai and Port Blair. Feed from all, ROCs is then ported to the Control Centre at Coast Guard Headquarters at New Delhi.

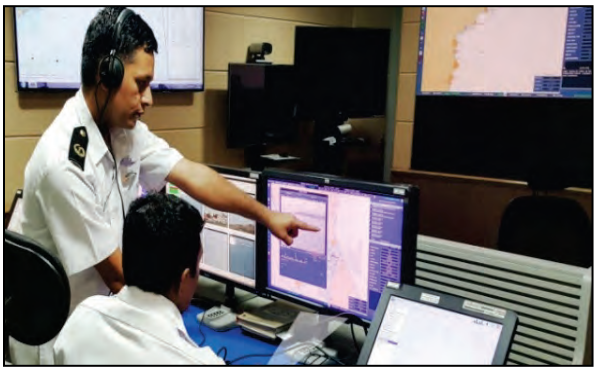


Fig. 3. Remote Monitoring from Control Centre

2.3.5 The system covers latest surveillance equipment viz. Frequency Diversity Radar, Electro Optic sensors (CCD Day Camera, LLTV and Thermal Imagers), VHF sets, Met equipment, AIS, and Networking equipment with V-SAT

overlay as redundancy, in line with the surveillance systems established world-wide.

Fig. 4. Sensors installed on lattice towers

3. BENEFITS

The Maharashtra and Gujarat clusters of the project were commissioned by the then Hon'ble Raksha Mantri in Aug 2012 and today almost the entire project has been implemented successfully. This project is a perfect example, wherein the indigenous networking and software capabilities were effectively utilized to integrate and leverage the state of art sensor technology available worldwide. The system software, since it was first operationalised has undergone several iterations and has now matured into a robust and flexible tool, which is being utilized for triggering, planning and coordinating various operations on a daily basis by the Indian Coast Guard. The benefits of the network are also being reaped by the Indian Navy through the National Command Control and Communication Network (NC^3I). The effectiveness of the network and our capability to conceptualize and execute a national project of this magnitude has also been noticed by our maritime neighbors in the IOR and the model is being emulated by most of these countries. At one hand this project has provided the much needed fillip to our coastal surveillance matrix, at the same time it has emerged as an effective technology demonstrator tool for the country, which is now materializing into possible business opportunities for our indigenous defence production establishment.

4. PHASE-II OF THE PROJECT

4.1 As the Phase-I of the Chain of Static Sensors comprising of 46 Radar Stations was envisaged to provide electronic surveillance around the area of high sensitivity and high traffic density along the Indian coast, numerous natural landing places along the Indian coastline, which were not covered by the Phase-I necessitated the requirement of additional Radar Stations to ensure near gap free electronic surveillance of the entire coastline. Accordingly, Phase-II of the project was envisioned to achieve near gap free coverage of entire coastline.

4.2 As part of Phase-II of the project, it is planned to establish complete array of sensors at 38 locations in addition to 46 locations being established in Phase-I. Further, integration of feeds from the VTMS of Gulf of Kutch, VTS of Gulf of Khambat and ICSS system of Chandipur-Balasore Complex of DRDO is planned.

5. CONCLUSION

With implementation of the Phase-II of the project and its backward integration with the existing Phase-I, the Chain of Static Sensors Network is expected to become the fulcrum of our coastal surveillance matrix and play an important role in optimizing the response of our security agencies. This project in tandem with other similar initiatives like the 'Fishing Vessel Tracking System' would metamorphose our coastal security outlook from reactive to pro-active.

Technologies in Internal Security

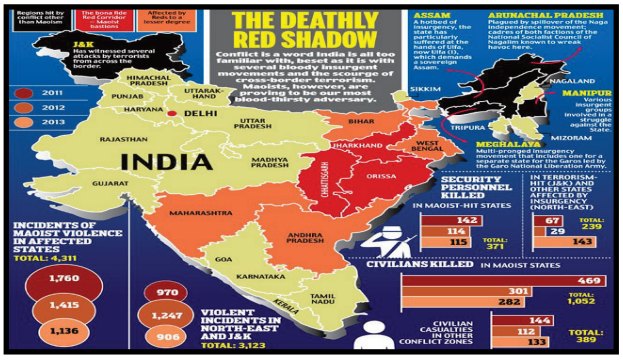
P M Heblikar
Former Special Secretary
Government of India

Dr K Ramchand
Former Director
Centre for Air Borne Systems, Bengaluru

Abstract: *Technology must become an important weapon for Security Forces (SF) in Counter-Terrorism operations (COIN). Domination through extensive use of technology should become the mantra for managers of national security infrastructure in India. Technology should not become an adjunct but an integral part of all national security calculations in India. Technology solutions, both hardware and software, are available in India. They need to be harnessed to meet not only our contemporary requirements and also future threats and challenges. The "Eye in Sky" proposition takes into account the requirements of SF in COIN and also those employed in different forms of border guard duties and maritime vigilance. Internal security lies within the purview of States and Union Territories and these are "first responders" to all forms of threats and challenges to law and order and stability. Appropriate technology for use by the States and Union Territories need to be developed in consultation with them. The States and Union Territories are equal stake holders in national security and require technology to sharpen their responses. A two-way dissemination of knowledge, information, experience and data is necessary. DRDO is a technology innovator in this sense and its role is cut out in internal security issues.*

Technology as force multipliers

Technology must be developed and harnessed into becoming an effective counter terrorism instrument. This must become the "mantra" for the future and be able to successfully challenge not only the existing threats to India's national security but also those with greater and dangerous potential. Obviously, these dangers will assume even sinister shape throwing a major challenge to India. Critical elements of such threats currently emanate and exist in our states and union territories



Foreign hand in destabilization of India's stability has been a constant factor since Pakistan's

abortive bid to annex Kashmir in 1948. As decades progressed, the arc became even wider and deadlier; with Pakistan playing the anti-India card from several countries from across India's international borders. China too funded and directed such efforts.

An analysis of the security environment over past several decades will reveal that almost the entire country have witnessed or experienced multiple levels of threats and challenges at different times.

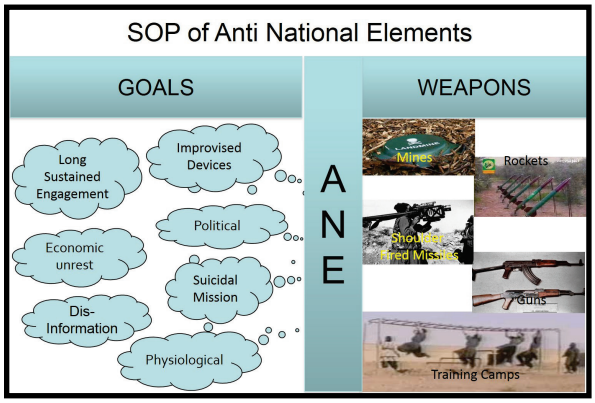
India has an exceptional record in tackling insurgency, militancy, political violence, left wing extremism and terrorism. The woes of the security managers have been compounded by the entry of non-state actors and rise in low intensity conflicts where latest weapons of destruction are used. Despite the track record, there have been several major lapses as witnessed in the recent attack on the Pathankot Air Force Base (Jan 2016).

It is true that India does not have a national security doctrine. Since 1947 there has not been a comprehensive and pro-active policy of national security management that has been totally futuristic and encompassing and not a panic reaction. It will be interesting to note that following Independence, India conducted 4 in-house reviews and 1 inter-ministerial report that looked at certain aspects of national security management. Of the five documents, one involved China, one was terrorism related and rest Pakistan centric. Besides there are several other in-depth assessments and task force reports on same subject including the Naresh Chandra Task Force Report (2012). A bulk of these have looked at India's external defense issues and therefore focused less on internal threats. This brings to the fore, two major challenges in our approach to national security. The first emanates from the fact that our institutions of governance, both domestic and global are based on sector-specific knowledge and management systems. They are unable to collaborate in delivering

multi-disciplinary and multi-sectorial responses. The second challenge lies in changing the enduring notion that national security, which we now understand, should be understood in a much more comprehensive manner rather in narrow military terms. Both challenges need urgent redresses. The Defense Minister has recently told a strategic journal that a national security doctrine is being prepared under his direction. This is welcome news and hopefully includes internal security issues as well. It is important to note that the distinction between defense and internal security is getting blurred with unavoidable and increasing deployment of the military in other than war duties. Technologies must also similarly adapt to meet challenges in the internal security space.

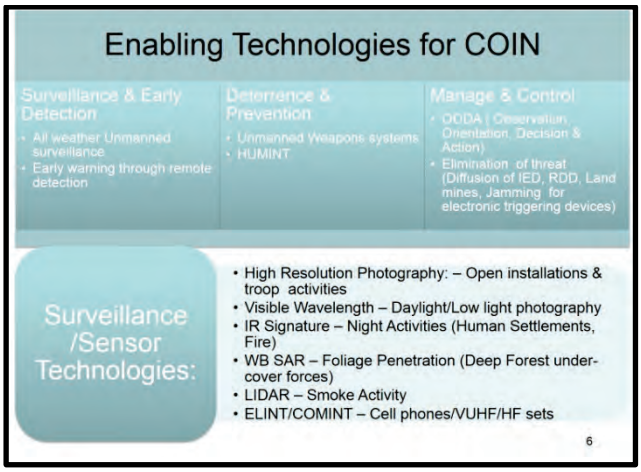
Use of Indian technology, both hardware and software, in government and private sector, in countering internal security threats is the order of the day. These threats have in the past been rural based especially in the forest areas of dozens of our states and union territories across. Despite billions of rupees expended in meeting these challenges, the scenario has not improved in any appreciable manner.

A bulk of our Counter Insurgency Forces (CIF), comprising mainly of the Central Armed Police Forces (CAPF), operate in several insurgency infested theatres such as in the Northeast region, Jammu and Kashmir and the Left Wing Extremist (LWE) dominated areas. In this, they are supported by the State Police Forces.



A bulk of these areas are forest/jungle bound, where the insurgents or Anti-National Elements (ANE) hold sway.

The CIF face several serious disadvantages in their operational duties. Technology or domination through technology must become a force multiplier.



It is important that the ground troops have access to real time intelligence gathered by **eye-in-sky** coverage.

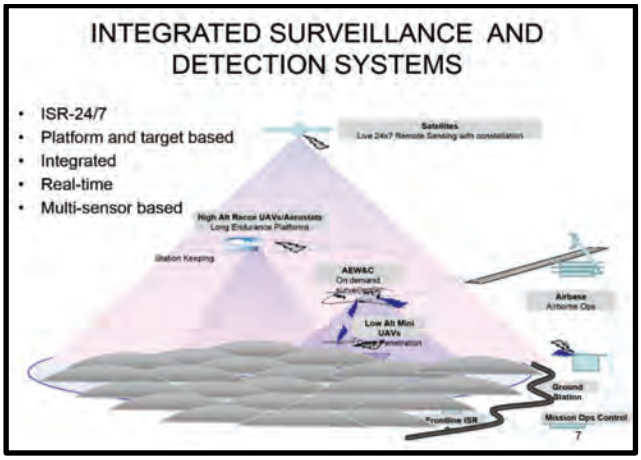
This will enable them to secure their fighting bases, sanitize the Main Supply Routes (MSR), enable road opening parties (ROP) or foot patrols or mobile patrols to obtain advance information about presence of Human Elements or ANE en-route, detect Improvised Explosive Devices (IED) and other tactical activities like ambush or raid.

Information may also be collected about movements of ANE from one place to another, ANE camps, telecommunication, movements of vehicles and information of tactical value that will assist or human intelligence acquired by the CIF.

The eye-in-sky can be either land based or aerial platforms that are capable of wide coverage of ANE dominated areas. Aerial platforms too are of several types that have applications that penetrate thick foliage, detect thermal images and locate embedded IEDs.

There are other technology solutions for fighting in rural areas as also for Fighting in Built Up Areas (FIBUA). Technology to dominate Counter Insurgency Operations (COIN) is required to be developed in a holistic and planned manner instead of becoming a panic reaction or in a piece meal fashion.

The Border Guarding Forces, under the Home Ministry, have an awesome task operating in inhospitable environments and tackling infiltration, human smuggling, cattle smuggling and other forms of illegal activities. The same technology recommended for CIF or COIN should be made available to them as well.



Satellite based technology for border surveillance with infrared facility is important.

This should not be difficult for India as it has its space network and the use of satellite based devices will add exponentially to thwart activities of ANE in the snow clad areas of J&K and also in the Indo-Himalayan belt. Spy-in-sky will help the Border Security Force (BSF) in unearthing tunnels emanating from across the Indo-Pakistan border.

Our security managers have several other options available for induction of technology into their operational plans. One major step is to create a template to end to the "culture of working in

isolation" or "silo" mentality and interact institutionally with the government's scientific community to develop synergies for present and future. This should be like-wise between the scientific community and the security agencies. Agencies like the Defence Research and Development Organization (DRDO) must collaborate in a proactive manner to bring to the fore technologies that can be shared and developed for the security agencies, CIF and even the Coast Guard that is struggling to come up protocols to meet its requirements. The private sector is another area for serious collaboration and needs to be drawn into this scheme. Importantly, the states also need to be brought into this ambit. It must be remembered that a bulk of law and order problems occur in their jurisdiction and they are required to deal with it as first responders. The fruits of technology must benefit them in many ways. Neither the states nor the scientific agencies know about each other in a focused manner, time has come for agencies like DRDO to step into the breach and disseminate knowledge on variety of its products.

The Union government has been spending considerable money on modernization of central police forces and also on the state police forces. Technology must find a role in this strategic program. There is a deficit of technical manpower within the CAPF and others which can be met by the MOD through release of short commissioned officers, both men and women, and also by open market recruitment.

The MOD and MHA should also look at creating more technical think-tanks to not only generate awareness but a reservoir of knowledge and cutting edge technology. The private or corporate sector is awash with latest technology, this must be harnessed in a suitable manner.

Dependence on "Made in India" technology is an absolute must to meet our requirements. This must be encouraged by the "Make in India" program of the central government. Time has come for a review on use of foreign technology in our strategic sector, unless we remove this crutch, we will not grow into an effective industry and develop tools accordingly. This cannot be done overnight but in a planned manner. We also must at developing the confidence and ability to detect, deter and destroy enemy actions before they unfold. Technology must be at the forefront of this game plan.

FORM IV

Statement about ownership and other particulars about newspaper (Magazine) Indian Defence Research & Technology (IDRT)

(to be published in the first issue every year after the last day of February)

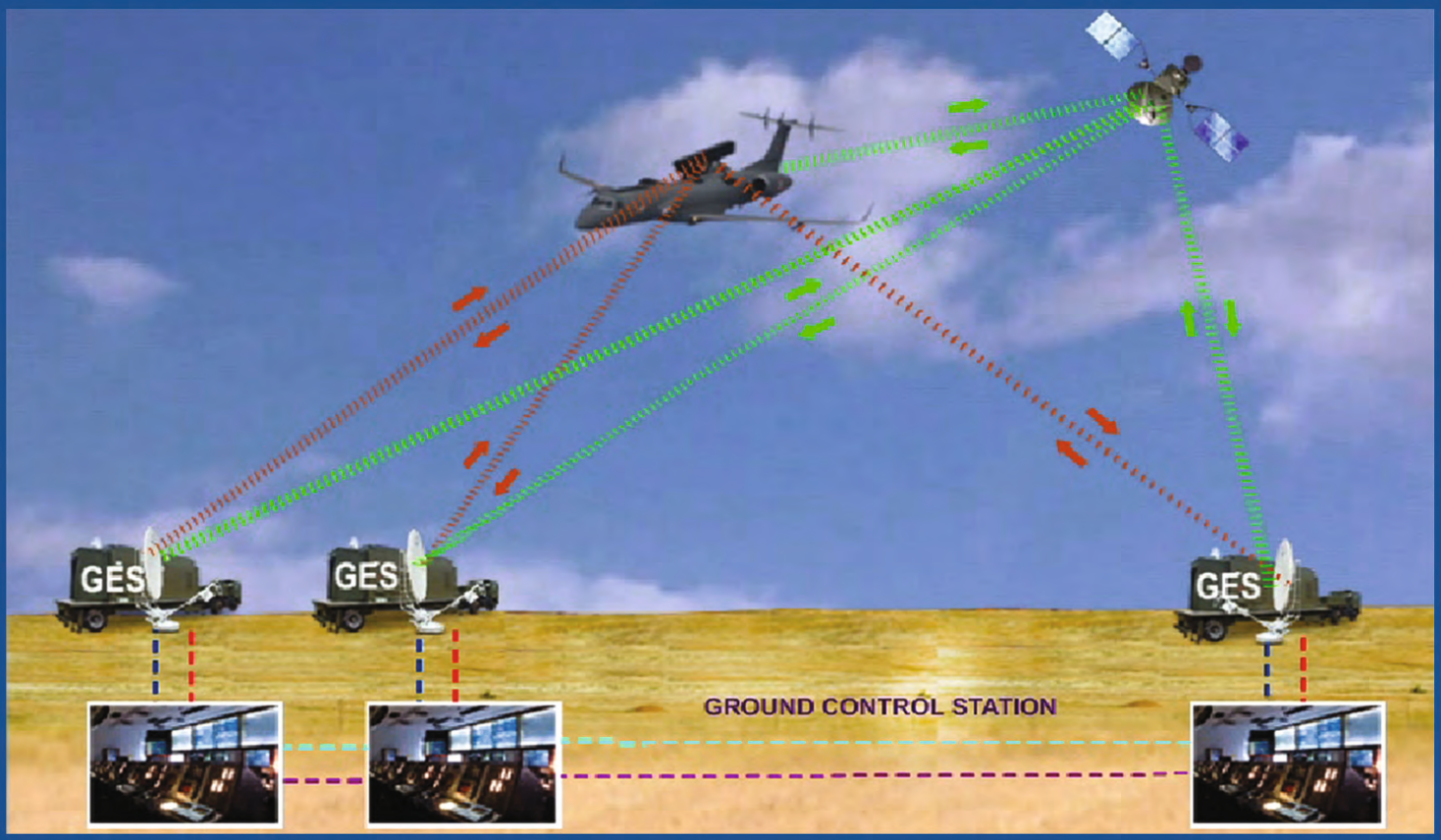
1. Place of publication	Hyderabad
2. Periodicity of its publication	Annual
3. Printer's Name Nationality Address	DESIDOC, DRDO INDIAN METCALFE HOUSE, DELHI -110054
4. Publisher's Name Nationality Address	AK CHAKRABARTI, President, IDST INDIAN Institute Of Defence Scientists & Technologists, DLRL campus, Chandrayangutta, Hyderabad – 500005
5. Editor's Name Nationality Address	BS BANSAL Secretary General, IDST INDIAN Institute Of Defence Scientists & Technologists, DLRL campus, Chandrayangutta, Hyderabad – 500005

6. Names and addresses of individuals who own the newspaper and partners or shareholders holding More than one per cent of the total capital. **NIL**
Name
Nationality
Address

I, AK Chakrabarti hereby declare that the particulars given above are true to the best of my knowledge and belief.

Date: Feb, 2016

AKChakrabarti
Signature of Publisher



Centre for Airborne Systems (CABS)
Defence Research and Development Organisation (DRDO)
Ministry of Defence, Government of India
Bengaluru - 560037 India
Tel: +91 80-25049002/9003 Fax: 91 080-25222326 Email: director@cabs.drdo.in

Designed and printed at DESIDOC, Delhi