COMMUNICATIONS:
A DECISIVE CATALYST FOR
JOINTNESS
Message

The recent announcement of the Chief of Defence Staff (CDS) by the Hon’ble Prime Minister from the ramparts of the Red Fort is an important milestone in achieving the vision of jointness. The creation of the CDS will significantly enhance collaboration between the three Services. It will usher an era in which we meet our National security challenges comprehensively, effectively and efficiently.

The theme for DEFCON 2019, ‘Communications: A Decisive Catalyst for Jointness’, aptly and succinctly reflects the intent to further jointness. To collaborate effectively, the three Services need to develop the capability to effortlessly communicate with each other. The Corps of Signals has provided infallible communications to the Indian Army over the ages. I must now compliment them for taking this initiative towards achieving joint communications. I am certain that this will lead to unprecedented economy of scale and will galvanise interoperability between the three Services.

DEFCON has over the years provided an excellent platform for stakeholders including the Armed Forces, Research and Development organisations and the Indian Industry to partner with each other. I am sanguine that this year will be no different. I am also confident that the Indian Industry will take up this challenge in consonance with the ‘Make in India’ initiative. Wishing the Corps of Signals and Confederation of Indian Industry (CII) the very best for the success of DEFCON 2019.

“JAI HIND”

Rajnath Singh
Raksha Mantri
Message

The Indian Armed Forces are undergoing rapid transformation to meet both existing and future challenges. The Services Headquarters are progressively evolving frameworks and structures to gravitate towards jointness. In this context, I wish to highlight the critical role played by communications towards achieving integration between the three Services.

DEFCOM is a unique platform which brings together stakeholders to deliberate, discuss and understand the requirements of the Armed Forces and match the same with industry capabilities. Indigenous adaptation of rapidly evolving commercial Information and Communications Technology (ICT) must take into account the requirements and concerns of the Armed Forces. I am glad to note that this year DEFCOM 2019, will seek to examine the important theme of, ‘Communications: A Decisive Catalyst for Jointness’.

I am certain that cooperation between the Armed Forces, Think Tanks, academic institutions, R&D establishments and the Industry through the medium of this forum will yield great dividends. I would also encourage the Industry to participate wholeheartedly in this event and to come up with solutions for furthering joint communications. I wish the Corps of Signals and CII all the very best for successful conduct of DEFCOM 2019.

“JAI HIND”

Shripad Yesso Naik
Raksha Rajya Mantri
Message

The quintessential nature of war demands that the three Services fight as an integrated and cohesive force. The recent announcement of the appointment of Chief of Defence Staff (CDS) by the Hon’ble Prime Minister is a landmark step towards achieving jointness. For fructification of jointness in its true spirit, it is imperative that the three Services seamlessly communicate with each other from the strategic to the tactical level.

The seminal theme for DEFCON 2019, ‘Communications: A Decisive Catalyst for Jointness’, is both topical and apt in light of the myriad security challenges our Nation faces. Joint operations integrated by communication networks is a pre-requisite for prosecuting war both effectively and efficiently. Towards this end, there is a need to reflect on operational, technical, organisational and Human Resource (HR) aspects for evolving a joint communications framework to unbridle Tri-Services synergy.

We compliment the Corps of Signals and Confederation of Indian Industry (CII) for setting the stage for truly insightful deliberations. I am sanguine that this collaboration between the Indian Armed Forces, Research and Development organisations, Industry and Academia will lead to key insights and tangible outcomes. Wishing the Corps of Signals and CII all the best for the successful conduct of DEFCON 2019.

“JAI HIND”

[Signature]

Bipin Rawat
General
Chief of the Army Staff
The importance of **Jointness between Services** for military operations has been explicitly highlighted by recent global and regional experiences. The existing triumvirate approach of the Services needs to be bridged by adopting requisite changes in doctrines, organisational structures, optimisation of resources, acquisition processes, operational philosophies and training methodologies. There is also a perceptible need to graduate from cooperation and coordination based approach to an integrated approach under a unified authority to realise effective Jointness.

The transformation towards Jointness stipulates transcending organisational barriers, culture and ethos to evolve a pragmatic framework to accomplish stated goals. **Communication** will serve as the key in unshackling the barriers hampering our tryst with Jointness and would definitely be the underlying ‘ether’ that permeates Jointness. The **primacy of information flow and decision making** in prosecution of joint operations will pivot on **seamless communications** and **integrated networks** between the Services.

I am sanguine that the theme for **DEFCOM 2019 ‘Communications: A Decisive Catalyst for Jointness’** would provide us a holistic perspective about the conceptual framework for Jointness and a comprehensive insight into the role of Communication in empowering Jointness. The collaborative forum of DEFCOM 2019 would definitely afford the Indian Armed Forces, Research and Development Organisations, Industry and Academia an invaluable opportunity for close interaction and pave the way for evolution of Joint Communication Framework and Communication Support Structures and Methodologies.

**“TEEVRA CHAUKAS AND JAI HIND”**

Rajeev Sabherwal
Lieutenant General
Signal Officer-in-Chief and
Colonel Commandant Corps of Signals
Message

DEFCOM 2019 comes at an inflection point in the evolving frameworks and structures of the Services towards achieving ‘jointness’. In light of the recent announcement of the appointment of the Chief of Defence Staff by the Hon'ble Prime Minister, the theme for this year’s edition - ‘Communications: A Decisive Catalyst for Jointness’ is very apt.

As the structures of the forces become highly integrated, it is crucial that power of Information and Communication Technology (ICT) is harnessed fully to achieve operational efficiency. The role of the industry, in this process, becomes ever more involved and important to realise the capabilities that our Armed Forces require. With technology evolving at a rapid pace towards Artificial Intelligence, Virtual Reality and Augmented Reality, the Armed Forces and Industry will need to deliberate, discuss and understand the myriad challenges and opportunities arising in the landscape of IT and Communication that would facilitate achieving jointness seamlessly.

DEFCOM 2019 will anchor all stakeholders in the ICT domain to generate key insights and tangible outcomes for the Armed Forces and Industry as well.

I wish DEFCOM 2019 all success!

Chandrajit Banerjee
Director General, CII
Contents

1. **Joint Communications for Enabling Conventional Kinetic Operations**  
   *Maj Gen C Mani and Lt Col Vikrant Sharma*  
   11

2. **Emerging Platforms for Control in Joint Networks**  
   *Harpreet Singh*  
   24

3. **Conflict in the Instantaneous Age**  
   *Brig Ashish Chhibbar and Brig Vivek Verma*  
   29

4. **Achieving Synergies in Defence Forces Through Network Centric Warfare System**  
   *Deepika Gupta, Rupesh Rawat, Devesh Mishra and Nitin Gera*  
   40

5. **Collaborative Defence R&D: Indian and International Perspective**  
   *Gopal Bhushan and M Madhusudan*  
   48

6. **Systems Approach Imperatives for Designing the Unified Secure & Resilient Digital Communication Infrastructure to Empower the Joint Operations**  
   *N Kishor Narang*  
   58

7. **Spectrum Management for Tactical Battle Field Networks**  
   *Brig Navjot Singh*  
   75

8. **Reorganisation of Indian Spectrum Administrator**  
   *Maj Gen LB Chand, VSM (Retd)*  
   80

9. **Cyber and Electronic Warfare: Technology Enablers and Challenges**  
   *Maj Akhilesh Singh*  
   96

10. **Tri Services Training in Joint Environment**  
    *Col Deven Makhija*  
    105

11. **Computational and Correlational Data Analytics for Increased Military Effectiveness**  
    *Brig A Shridhar*  
    112

12. **The Role of SDR as an Enabler in Joint Operations**  
    *Col Rohit Nandan Prasad*  
    117

13. **Threatscape Segmentation: Network Invigilation for Realizing Vulnerable Assets using Neural Analytics (NIRVANA) to Mitigate Zero Day Attacks**  
    *Lt Col Vivek Bardia, Lt Col Gaurav Upadhyay, Lt Col Raja Vijit, Lt Col Akshay Sati and Lt Col Yogesh Sati*  
    123

14. **SATCOM—Last Mile Secure Connectivity to Difficult Terrains of Tactical Battle Area**  
    *MR Sujimol, Anita Panday and K Shahana*  
    132

15. **Mobile Communications using Modified 4G LTE and Futuristic 5G for Joint Operational Environment**  
    *Col A Oberoi*  
    139
16. Developing Synergy and Jointness in Cognitive and Social Domains  
   Col K Pradeep Bhat (Retd)  
   151

17. A Framework for Implementation of Smart Documents for Armed Forces  
   Maj Kunal Pal and Dr CRS Kumar  
   155

18. Technology for Standardization of Sensor Data from Legacy Heterogeneous Sensors in Tactical Surveillance Application for Joint Operations  
   Vandana, Sanjay Motia, Pradeep and Anoop Kumar Rai  
   169

19. Private LTE Networks for Defence Critical Communications and Digital Defence 4.0  
   Philippe Agard, Public Safety and Defence Segment Leader  
   179

20. Communication as a Decisive Catalyst for Jointness  
   Lt Col Prabhmeet Singh Manik, SM  
   186

21. Machine Type Communication & Internet of Everything (IoE)  
   Col Rajesh Kapoor  
   193

   Col Munish Tuli and Lt Col Aashish Joon  
   197

23. Joint Enterprise Cloud for Armed Forces  
   Lt Col Sumit Gupta, SM  
   202

   Lt Col Sudipto Roy  
   208

25. Enhancing Cyber Security Posture by Leveraging Technologies Like Big Data, Artificial Intelligence and Block Chain Technologies  
   Lt Col Apurva Bhatnagar  
   219

26. Practical Solution for Secure Network in a Quantum Computing ERA  
   Anindita Banerjee and M T Karunakaran  
   232

27. Future of Cryptography: Quantum Key Distribution through Micro-Satellites  
   Col Kapil Jaiswal  
   247

28. High Performance Network Forensics and Anomaly Detection on Commodity Hardware  
   Kunal Sadalkar, M Hemavathy and M Akila  
   256

29. HR Strategies in Support of Joint ICT Structures  
   Brig Ramesh Balan  
   261

30. Utilizing Decentralized Technology for HRM Advancement  
   Avnish Singh Jat, Rajkumar Pandey and Akshay Singh  
   268
Joint Communications for Enabling Conventional Kinetic Operations

Maj Gen C Mani and Lt Col Vikrant Sharma

Abstract—As the armed forces strive to modernise, paucity of resources will necessitate optimising through first deciding on the capability needed to be achieved to meet the threat environment. Capability based planning will need to supplement and eventually supplant the current threat based planning paradigm. The acquisition of a network centric warfare capability that seamlessly integrates the sensor-decision maker-shooter grid must therefore be a national priority. Relevant scenarios for joint operation/mission range from low intensity operations, Humanitarian Assistance and Disaster Relief (HADR) Operations to high-intensity combat operations like Amphibious operations, Air Land Operations (ALO) / Battle, Air Transport Operations, Maritime Air Operations (MAO) etc against broad spectrum of adversaries ranging from organised militaries to belligerent regional powers to violent extremist organizations. It is important that services/ agencies taking part in operations coordinate all activities across all instruments of power from the earliest stages of the preparatory build up and planning process.

1. INTRODUCTION

1.1 General

1.1.1 Warfare at the national level consists of coordination, orchestration and synchronisation demanding complete integration of all elements of national power. In most of the advanced democracies in the world, where civilian control over the armed forces is completely established, the role of a single point military advisor to the highest political decision making entity of the state is institutionalised. Peace loving India has succumbed to the realities of its extremely volatile neighbourhood and the political hierarchy has finally approved appointment of Chief of Defence Staff (CDS) for the three services. The idea to have a CDS is essential for defence reforms, jointness, multi-disciplinary coordination, economical use of resources and standardised procurement.

1.1.2 This decision is expected to give an impetus especially to jointness and integration among armed forces. The existing structure for cross-service cooperation is weak and efforts for jointmanship are proceeding slowly, resulting in duplication of efforts, wastage of resources and delay in decision making.

1.1.3 Modern warfare calls for simultaneous and seamless application of all elements of warfare, kinetic or otherwise, synergising the capabilities and resources of the three services. All five domains – land, air, sea, space and cyber space are to be exploited with maximum effect. New and emerging concepts, technologies and techniques must also be employed to use force cohesively and in an orchestrated manner. Joint planning & application, joint training, joint doctrines, compatibility in equipment & procedures and last but not the least joint communication is a prerequisite.
1.1.4
Next step required to make CDS effective is creation of Integrated & Joint Commands. Theatre commands are the key to transforming the armed forces as joint forces. Same name, same regions but different HQ leads to diverging strategies. This prevents jointness and seamless performance in times of conflict or war. Without Integrated or Joint Commands the services would not be able to transform into a single, war fighting machine. Theaterisation of commands will further lead to creation of a HQ with joint communications, intelligence, surveillance and air defence systems.

1.2 Aim

1.2.1
To establish the requirement of joint communication as an enabler for conduct of joint operations.

1.3 Scope

1.3.1
This paper has been laid out in the following parts:-

(a) Part-I: The Indian Experience of Inter Services Cooperation.
(b) Part-II: Communication Planning For Joint Operations.
(c) Part-III: Barriers To Joint Communication.
(d) Part-IV: Way Ahead- Integrated Communication & Communication Management

2. PART - I : THE INDIAN EXPERIENCE OF INTER SERVICES COOPERATION

2.1
The Indian Armed Forces have time and again proven their mettle in military as well as non-military actions in local, regional and multi-lateral operations and exercises. The Indian Army had covered itself with glory during World War-II, but could not repeat its performance in 1962. Galbraith in his letter to Kennedy was quite right when he stated that Indian tactics had not evolved from World War-II and was ineffective against a China steeped in guerrilla warfare. The Chinese had perfected the art of guerrilla warfare after fighting with the Kuo-Min-Tang for 22 long years. The Indians performed exceedingly well when facing frontal attacks as at Bum La, Nuranang, Gurung Hill or Rezang La. The lack of high angle artillery weapons affected the quality of fire support. Ammunition which had to be resupplied by air using reusable parachutes mostly failed to open or landed in gorges and crevices from where they were almost impossible to recover. The Chinese on the other hand were well equipped with howitzers and mortars. The most critical factor was the lack of offensive air support. Keeping the IAF out of the war when all the advantages for employment of air was held by India was ill considered. However, the overwhelming qualitative and quantitative force superiority and the quantum difference in infrastructure development on the two sides could have had only one result.

2.2
In 1965, suboptimal utilization of air assets reflected the lack of joint planning and the ineffectiveness of joint organisations for tactical air support on the battlefield. Indian air support first arrived at 5.30 PM on 01 Sep almost 12 hours after it was demanded by the Chhamb Brigade Commander, by when it was impossible to distinguish friend from foe. The demand for air support was itself inexplicably delayed. Ideally, air support should have been available
at dawn, since the attack had commenced just before first light. This could be condoned since India was taken by surprise at Akhnur. What is inexcusable however, is the lack of air support in the Punjab sector when the orders for go ahead with the operation was given on 03 Sep, three days before 11 Corps attacked the Ichogil canal. A far more grievous error was to neglect taking out of Pakistan airbases and radars once the attacks on Punjab had been launched. Instead the Pakistan Air Force (PAF) got the first blow in demolishing 10 aircraft on the runway in Pathankot. Fortunately, for India, the other airfields at Adampur, Halwara and Jamnagar were not attacked synchronously and hence suffered relatively lesser losses. The Navy too was not employed, despite the attack on Dwarka by the Pakistani Navy. The fact that India’s only aircraft carrier was carrying out routine maintenance again calls into question the lack of foresight as this routine maintenance could easily have been postponed. Lack of response to the bombing of Dwarka Port further emboldened Pakistan by making them believe that the Pakistani Navy’s writ ran on the Arabian Sea. However, a conscious decision of the Defence Minister to restrain the Navy for fear of escalation appears to be the real reason.

2.3
1971 witnessed better joint planning. In East Pakistan, however, there were 11 IAF squadrons against just one squadron of the PAF. While fears of Chinese intervention might have been the reason for this, it was an overkill. Thinning out of IAF resources for utilization on the Western Front could have been considered. A more synergized application of airpower in the Jaisalmer and Barmer sectors could have resulted in greater destruction of the Pakistani mechanized Forces. The Longewala battle too was fought only by the four Hunter aircraft at Jaisalmer air base. Better force application could have been achieved if airfields at Uttarlai, Jodhpur and Nal had been synchronously used. The naval power was well utilized, but a synergized application of the IAF and the Navy in the bombing of Karachi was absent.

2.4
In 1999, the self-imposed constraint of not crossing the LoC ensured that combat power was not employed optimally. The limitation of not crossing the LoC resulted in curbing the effectiveness of the IAF. The Army had to suffer much more casualties as its approaches were restricted. By any standard these casualties are inordinately high especially in an environment where the Pakistan Army formally did not enter the conflict and the PAF was kept out of the picture. This highlights the lacunae in surveillance, targeting and Post Strike Damage Assessment (PSDA), due to shortage of effective sensors that could be deployed in high altitude areas. The shortage of modern communication, interception and direction-finding equipment further, reduced the synergistic application of army and air power. The Indian Navy carried out an effective blockade of the Karachi port adding to its political isolation but did not really affect the conduct of operations.

2.5
Therefore, when viewed critically it appears that lots more needs to be done to move up the value chain of cooperation-coordination-jointmanship-integration. The lack of joint planning and implementation is a serious lacunae that can only be addressed by revamping the existing individual Service specific structures and empowering the Chief of Defence Staff (CDS). While this will inevitably take time, communications are a fundamental enabler to integration and need to be addressed on priority.
3. JOINT KINETICS OPERATIONS PLANNING

3.1 Lack of jointmanship can be likened to running a three-legged race with all the three legs going in three different directions. The principles for joint planning have the following imperatives all of which can be empowered through joint communications planning:

(a) Unity of Effort.
(b) Concentration of Force.
(c) Economy of Effort.
(d) Freedom of Action through a directive style of command.
(e) Clearly defined objectives that are understood across all echelons of command permit concentration of kinetic effects. This will also inject the requisite flexibility to the command elements and enable them to take the initiative within the overall contours laid down by the Joint Task Force (JTF) commander.
(f) Security of plans are an imperative in this era of information warfare. Multiplicity of Service specific networks will only increase the points of vulnerability.

4. PART-II: COMMUNICATION PLANNING PRINCIPLES FOR JOINT OPERATIONS

4.1 The principles for joint operations planning reflect the challenges for the three Services in a complex and uncertain security environment. Communications as evident are critical to conduct of such operations. In our context the challenges are in ensuring cross cultural awareness of the respective communication procedures and ensuring a clearly understood and recognised lexicon for joint communication procedures. The challenges are perhaps best exemplified in the conduct of amphibious operations. Superimposed on the Service specific communication system is the additional requirement for command and control of the Amphibious Task Force (ATF) over the Amphibious Operations Area (AOA). Some of the planning considerations are given below:

(a) Communication planning for ATF should be compatible with tactics and techniques employed by each service as part of overall force. Operations are characterised by peculiar nature of operations on land, sea and air involving dissimilar forces. Communication setup planned must assure effective exercise of command, control, coherence and coordination of fire support.
(b) Elements of the ATF may operate across widely separated areas for a particular phase of the amphibious operation. Communication requirements for every phase, therefore needs to be planned in detail. A measure of duplication will be an inescapable requirement and merit employment of additional resources. The communication plan should also ensure operation by the force without undue interference between various elements.
(c) Separation of individual ships and forces as a passive measure of def against air & missiles increases the requirement for long range radio communications. Accordingly, allocation of communication equipment on board ships must be considered carefully in the light of naval and landing force requirements. The communication
equipment allocated for the control of or use by helicopter borne forces must be planned with particular consideration of nature of the terrain and distance which may exist initially between area of operation ashore and the amphibious task force.

(d) The geographical location of the amphibious objective area may dictate the need for special and alternate means of communication to cater for fading especially in HF long range communications.

(e) Plans must ensure that the command, tactical and administrative communication requirement of all elements of the amphibious task force are met by specific technical provision of communication circuits and radio nets and that these provisions are fully coordinated and integrated.

(f) **Communication During Planning Phase.** Communication planning must be integrated and same should be ensured at the very commencement of the planning phase between all major participants from three services at the command level. Preservation of communication security is essential to plans, and maintenance of same is of paramount importance since initially planning headquarters are separated by large distances.

(g) **Communication During Embarkation Phase.** Before embarkation commences plans must provide for adequate integrated communications between naval, ground and air forces to be embarked. The Landing Force Commander (LFC) normally will be assigned the responsibility of provision of communications in the embarkation area. Plans must also provide for establishment of communications in the Pier or Beach Areas to control embarkation. Early liaison and coordination must be established between corresponding Naval and Landing Force elements to ensure efficient communications during embarkation.

(h) **Communication During Rehearsal Phase.**

(i) In order to test communication systems, equipment and techniques the overall plan should provide for full scale rehearsal of communications arrangements for all elements of the task force. Communication security requirements during the conduct of rehearsals may dictate adoption of the following precautionary measures:

(aa) Use of min power for transmission.

(ab) Change of frequencies and call signs. However, the security desired must be weighed against the ambiguity which might result during subsequent phases of the operation as a result of this change.

(i) **Communication During Movement To The Objective.** Plans for communications during the movement to the objective, will require naval forces to provide all external and inter ship communications. The use of communication facilities particularly radio is severely restricted to prevent disclosure to the enemy of the locations, movement and intentions of the ATF. The ATF Commander
promulgates the EEP status during the movement to objective area. Communication plans must cater for these restrictions and provide for the handling of important messages within the imposed limitations. Communications within various movement groups of the ATF will be provided by helicopters, visual means or superimposed on peace time VHF and UHF radio networks in consonance with the degree of radio silence in effect.

(j) Communication For Naval gunfire support. Plans for communications during the Naval Gun Fire Support will require naval forces to provide all external and inter-ship communications. It would require communication integration with army artillery units, air force fighter squadron and attack helicopters etc. Unless planned the desired softening of enemy positions on beach area may not be achieved which may delay or hamper progress of assault phase.

(k) Communication During Assault Phase. During the assault phase primary reliance must be placed on radio and radio relay communications. Communication plans of both naval, air and landing forces should provide for sufficient channels of communications during the ship-to-shore movement to permit the exercise of command, control and coordination which is required at all echelons. Communication plans of the landing force should cater for the rapid deployment and development of landing force communication system ashore in order to ensure facilities to respond to the needs of the tactical situation as the assault progresses. It should be suitably integrated with follow on naval forces, air force and logistic elements for the desired shore based support in the AOA.

(l) Base Development and Garrison Communications.

(i) Higher HQs may plan to carry out base development and setting up garrison ashore at the earliest. Communication personnel and equipment from three services shall be embarked and landed with the landing force in order to begin early installation of a planned advanced base communication systems. When such plans exist, all usable elements of landing force communication system ashore should be included in the program for development of the advanced base communication.

(ii) These plans may also provide for the establishment of external communication ashore for use upon termination of the operations and after departure of the ATF Commander from the objective area. A joint mobile communication unit for this purpose may be assigned to the landing force commander for embarkation and early establishment ashore.

(m) During planning, equipping and training for the amphibious operation, commander must bear in mind that during landing and assault the enemy may attempt to deny successful communication by own forces by means of jamming. Steps must thus be taken to minimise the effect of enemy jamming or interference. These measures include:-
(i) Use of alternate freq and call signs.
(ii) Development of plans for locating (DF) enemy jamming stations.
(iii) Provision of specialised training for operators from three services in anti-jamming procedure.
(iv) The use of authentication procedures.
(v) Provisions for other means of communication such as beamed super high frequency, infrared, visual, boat/ helicopter messenger.
(vi) Offensive action to locate and to neutralise or destroy enemy jamming stations.

5. PART - III: BARRIERS TO JOINT COMMUNICATION

5.1
The foregoing attempts to bring out the complexity of planning communications for a joint operation. The existing state of integration has significant obstacles to achieve seamless communications some of which are described below.

5.2
Theaterisation of Commands. With CDS in place theaterisation should see the light of the day. Without this, redundant efforts are being made by each service to ensure communication for its respective elements. This is leading to poor optimisation of resources and budget. Lack of integration of service specific data networks like ADN, Navy net and AFNET are primarily due to a lack of will as technical solutions exist to integrate at any of the layers of the OSI model.

5.3
Inadequate involvement of Commanders. More often than not the communication planning is assumed to be in place without giving terms of reference. If terms of reference are laid then the requirements do not meet the desired capability. Capability is independent of technological demonstrations and is an important aspect of communication planning. Also, communication planning is an important aspect of operational planning and should be adequately addressed. Steps like these may hamper joint communication at an operational level.

5.4
Cultural Awareness. Lack of knowledge of strengths and weaknesses of sister services communication capabilities is a serious flaw in joint planning. Mere visits, sharing of literature and few courses will not bring out the jointness as desired. Non-standardisation of policies and procedures is also a setback to joint communication planning.

5.5
Security Issues. Lack of Joint Communication Planning affects the communication security issues due to lack of standardised security setup in terms of common algorithms, common crypto devices and common/ compatible protocol. In turn lack of security can jeopardise the operational plan.

5.6
Lack of Joint Exercises. Lack of/ limited number of Joint Communication Exercises at the tri service level leads to non-familiarity, lack of knowledge of practical aspects and lack of focus with respect to interoperability, familiarity of equipment and procedures for joint operations.
6. PART - IV: WAY AHEAD:
INTEGRATED COMMUNICATION & COMMUNICATION MANAGEMENT

6.1 Integrated Communication

6.1.1
Integrated communication once established will address a range of issues in order to support the achievement of consistency in information flow throughout the levels of joint operations and respond to the expectations of various stakeholders in the JTF. Integrated communication also requires the alignment efforts of all communication agencies within the JTF and communication between the JTF and other actors for the sake of consistency, credibility, and ultimately effectiveness in support of mission accomplishment. Integrated communication facilitates JTF HQ internal communication for Command and Control (C2), staff routine, troop information, and training. Integrated communication vertically involves reliable and seamless communication of the JTF HQ Commander and his staff with Higher HQs and subordinate commanders to issue, receive and clarify direction and guidance, including plans and orders. In the horizontal dimension, communication processes will involve JTF to promote JTF objectives and enhance awareness, understanding, and support of JTF operations.

6.2 Communication Management Anticipated at the Joint Operational Level

6.2.1
It is a leadership responsibility to implement superior communication guidance so that it becomes effective throughout all levels of mission. Integrated communication must build on helping the JTF senior leadership achieve their objectives through effective command and control and situational awareness. In this respect, it is of utmost importance to understand that although personnel with assigned joint integrated communication tasks may act on behalf of the commander, the ultimate responsibility for JTF communication rests with the senior leadership. Communication specialists must get actively involved in all analysis, planning, execution/management, and assessment/evaluation activity. Communication specialists should be key actors in the senior leadership's decision-making process. Integrated communication incorporates several processes that need to be taken care of by the senior leadership and appropriate assisting functions in order to be implemented consistently and become effective. These processes should materialise in so-called 'communication management tasks'.

6.3 Communication Management Tasks

6.3.1
The following tasks describe the scope of communication management for operations/situations involving more than one service:-

(a) Command and Control (C2). This constitutes a communication dependent activity in itself. Designated superiors of JTF wield power and exercise authority and direction over subordinates through communication to convey orders, instruct and motivate, explain the tactical situation and present a role model. Communication is a leadership function to support unity of effort of the JTF. Commanders are the supreme communicators and drivers of integrated communication. Those involved in communication management should be authorised to issue direction and guidance to exploit communication
capabilities and functions and to ensure integration of communication with operational analysis, planning, execution and assessment.

(b) **Communication Strategy.** Situational awareness and understanding the Communication Strategy are inextricably entwined. Analysis of the Communication Strategy enables the identification of requirements, opportunities and risks, and provides the baseline for the assessment of effects. For joint operations it is a cross-dimensional, trans disciplinary and continuous task, which needs to be performed by a highly qualified tri services signals staff. Analysis results must be translated and operationalized in order to optimally exploit communication capabilities and functions as well as operation planners, and finally the Commander. Analysis of the Communication Strategy includes a variety of different subjects such as the communication media, IT, leadership, military C2 structures and social networks, and it also significantly overlaps the other areas, e.g. political propaganda and information infrastructure. Therefore, Communication Analysts should involve various Subject Matter Experts (SMEs) and evolve communication strategy to facilitate materialisation of strategic objectives.

(c) **Communication for Effect Development**

(i) An effect is the physical and/or behavioural state of a system that results from a kinetic or non-kinetic set of actions. An effect can be thought of as an intermediate state between the current prevailing state/situation and the military objectives that support the end-state. Effects provide a bridge of reason between end state and actions undertaken, the context for inter-service/interagency collaboration and the basis for continuous assessment of the success of an operation. In order to assure this functionality, it is important to accurately convey the meaning of desired effects to all involved in planning, execution and assessment. Effects statements should therefore describe the conditions resulting from desired changes in the operational environment in a comprehensive way. Effect statements should not infer how the effect is to be realised. Effects must be measurable and allow to quantify observable system and attribute changes. Finally, effects must be feasible, i.e. achievable in terms of timing and resources, and assignable to a functional lead for their creation.

(ii) Within the framework of Integrated communication setup, the same principles must be observed to describe effects to be achieved in the communication domain. The most important requirement in this respect is that effects contributed through integrated communication must refer in particular to Communications and Information Systems (CIS) and Command and Control (C2) Systems, in order to fully integrate relevant communication aspects in the planning process. The development of effects in the integrated communication in support of operational objectives is a key task that collectively involves
analysis, plans and operational personnel. It must be based on a profound understanding of the communication requirements envisaged, the mandate and mission objectives, as well as the available capabilities. It is for this reason that development of effects for the integrated communication need to be guided from a JTF commander’s perspective and fully integrated with and phrased as operational effects. A suitable org comprising of representatives from three services should be constituted to include all relevant functional and capability expertise and viewpoints.

(d) **Contribution To Targeting.** All kinetic actions are affected by communications. Negative effects from failure in communication can result in collateral damage, fratricide and especially civilian casualties damaging support for the JTF’s mission and attracting attention of international community and media. For this reason, the potential effect of effective and secure communication setup should be taken into consideration from the outset of the joint targeting cycle. Communication analysts and planners, Info Ops and signals staff, should be included at every level of the targeting process.

(e) **Communication Activity Planning.**

(i) Activity planning constitutes the lower end of operational planning. Its aim is to examine the range of possible (and probable) cause-and-effect relationships between kinetic actions and desired effects. Effects in communication domain may be defined as desired conditions created in the Joint Communication Setup as a result of various communication related activities. Communicators need to carry out an analysis of situation and end state desired in order to identify the actions needed to cause the desired effects. Subsequently, the signals staff must identify and continuously review the resources to be used in the conduct of each military action. Further, the staff must determine whether any communication resources might be necessary to support other non-kinetic actions.

(ii) It is likely that while the joint planning staff will provide guidance on the actions, it will be the decision of each service to develop actions in more detail and allocate the resources. Activity planning requires organisational setup to develop and de-conflict possible actions that can be conducted by the relevant service level to create identified effects in the Integrated Communication Setup.

(f) **Coordination.** Coordination is a key task and main responsibility of Communicators from three services to promote the integration of communication in all aspects of operations planning, execution and assessment. Therefore, appropriate joint signals staff needs to manage the appropriate involvement considering and keeping in view existing communication capabilities and functions in support of joint operations. Effective and efficient communication requires harmonisation and synchronization of communication procedures.
Joint Communications for Enabling Conventional Kinetic Operations

(g) **Communication As A Driver.** Driving and shaping JTF operations requires dynamic and prompt measurement of effectiveness of communication planning. It aids in designing and appropriately adjusting desired effects of communication and related activities to achieve these effects. This task needs to be closely linked to the continuous analysis of the rapidly changing situation and existing communication setup, which provides the baseline for change and activity planning thus facilitating JTF msn.

(h) **Training & Education.**

(i) Integration of communication in all plans and activities and advancing the new mind-set towards awareness and perception of the Integrated Communication requires the assistance of communication specialists during staff planning process and working routines as well as general communication training for personnel from tri services. Internal signals leadership and tri services signals staff development programs should enhance the accountability of communicators to the JTF and contribute to overall mission success. It is the commander’s responsibility to ensure that properly trained personnel are empowered through training and education opportunities in order to facilitate these requirements. Subordinate Signals Cdr at the highest level in each service need to involve education and training programs that support the development of the mind-set of integrated tri service communication.

Each and every member of the JTF must acknowledge the fact of presently not being able to communicate effectively and lack of interoperability and implement this in their plans and actions for shaping the JTF’s operations.

(ii) Joint Signals Staff education programs would also serve the purpose of promoting situation awareness, information exchange, transparency, and a common understanding of the Commander’s intent related to Integrated Communications. Cross-service individualised training should be considered extremely important as it will help communication and coordination amongst all staff elements. It is a primary responsibility at each service level to ensure such courses are subscribed to and in a joint manner plan more such courses to build professionalism for provisioning of joint communications and also achievement of a better understanding of individual service expectations.

(i) **Literature.** A very important measure to ensure common communication procedures between services is to have common literature that has been agreed to and published in both English, Hindi and Roman Hindi at a common press. Being able to think, read and act alike is a prerequisite for establishment of communication interoperability and laying down of concrete procedures for joint operations. A very good example of the same is refuelling of helicopters. It might appear to be a straightforward task but involves several interrelated aspects adhered to by each service.
(j) **Organisational Changes.** At the Apex level there is also a requirement of establishment of Staff involved in Communication Management. Ideally, the SO-in-C should function under the CDS to do justice to the word ‘Chief’ in his appointment title since he is already vested with providing land line communications to all the three services. With the appointment of the CDS hopefully he would be allowed to do his job. This will ensure the existing JCES will perform roles other than spectrum management. Alternately, it could be expanded to a *Joint Communication Directorate* composed of a *Joint Director and Joint Signals Staff* selected from three services. A functional *Joint Communication Coordination Working Group (JCCWG)* may be set up under Joint Communication Directorate to carry out necessary study of current and future battle requirements and facilitate activity planning, coordination and project communication related requirements that have a bearing on joint operations. Proposed organisation with authority and defined role is as recommended below:-

(i) **Director Joint Communications**

(aa) **Role:** The Director Joint Communications will assist the senior leadership in all aspects of integrated communication. He will coordinate communication aspects with strategic authorities and direct all internal and external communication processes of the JTF at the operational level on behalf of the commander. He will coordinate communication efforts with neighbouring commands and other organisations and stakeholders in theatre.

![Joint Communication Directorate](image-url)
(ab) **Authority:** The Director should be granted the authority to require consultation between JTF agencies (organisations or commands and their representatives) for all issues related to JTF communication. Within his responsibility for integrating internal and external communication processes he should also be authorised to directly address all members of the JTF HQ as well as communication specialists of subordinate commands.

(ii) **Deputy Director Joint Communications.** His role and authority mirrors that of the director. In addition he exercises command over the Joint Signals Staff and Joint Communication Coordination Working Group.

(iii) **Joint Signals Staff**

(aa) **Role:** Assist Director Joint Communications for all intent and purposes. Mirror the role of Director at lower level of competency. Their focus is on coordinating desired communication support and disseminate directions on behalf of Director.

(ab) **Authority:** The staff should be granted the authority to require consultation between JTF HQ staff elements and communication specialists of subordinate commands.

(iv) Support Staff from three services

7. **CONCLUSION**

7.1

As we try to get better at joint communication, we need to remember that Rome wasn't built in a day. There are many gaps between what we currently do well in this arena and all the things we would like to do well in pursuit of a fully mature vision of strategic communication. It follows from this insight that there should be a logical progression toward closing gaps and building capabilities related to this area.

7.2

Reforms in this area emphasise guidance, leadership, and strategic direction coming from the top. I also advocate top-down progress in this area, but when we speak about joint communication at tactical and operational levels the emphasis should also be for the prospects for bottom-up progress in this area by each service as well.

**REFERENCES**

3. USI Journals.
4. *India STRATEGIC Journals.*
Emerging Platforms for Control in Joint Networks

Harpreet Singh
E-mail: harpsin@cisco.com

Abstract—We have seen great leaps in digital technology in the recent years. Smartphones, cloud computing, multi-touch tablets, these are all innovations that revolutionized the way we live and work. Technology is evolving at an enormous speed, and it is forcing organizations to adopt these technologies and innovate to stay in business. The new technologies leverage the existing ones, and build on them, while some are completely new. Regardless of the origins, these technologies are designed to bring agility and automation in the world of IT, while dealing with the challenges of securing the IT infrastructures. We shall cover one such innovation in this article viz, Software Defined Networks, that leverages multiple underlying technologies, and try to address its relevance to jointness, which is the theme of DEFCOM this year.

1. SOFTWARE DEFINED NETWORKS (SDN)

1.1 The Open Networking Foundation describes Software-Defined Networking (SDN) as an emerging architecture that is dynamic, manageable, cost-effective, and adaptable, making it ideal for the high-bandwidth, dynamic nature of today’s applications. This architecture decouples the network control and forwarding functions enabling the network control to become directly programmable and the underlying infrastructure to be abstracted for applications and network services.

1.2 When we apply this definition to a campus network with different types of users with varying privileges and security policies, the requirement of a Software Defined Network at the campus level calls for a central policy engine that would define the privilege levels of a user/device at the time of granting access to the network. A Software Defined Network would also require the central controller to define policies, and communicate them to the underlying network devices to be able to enforce those policies.

1.3 Software Defined Networks generally use the overlay network technologies like VXLAN to connect disparate networks and provide segmentation between the various types of users. Creating an overlay network on the underlying physical infrastructure also provides the flexibility of connecting any user to any access port on the network, and enforce the same set of security policies for the users, regardless of whether they connect to the network a wired port, or over a wireless network, or even through a VPN connection.

1.4 These networks can be augmented using technologies like Network Behavioral Analysis to detect traffic anomalies, any data hoarding attempts, or even communication to Command and Control servers, and block network access to malicious/compromised users/devices.
1.5

Technologies like MPLS have been used to segment different user types on the WAN by creating virtual routing and forwarding tables. Although this is a secure and scalable way of segmenting users on the WAN, these technologies do not provide any isolation or segmentation within the same LAN. All users/devices on the same subnet or LAN segment are handled in the same manner and hence a single compromised user can impact the entire LAN segment. Software defined technologies in the access networks, can utilize the overlay network topologies to segment users within the same LAN segment thereby providing an additional layer of security and segmentation.

1.6

Traditional networks use IP address to identify a packet and the policies are enforced at the access layer when the user connects to the network, or when the user reaches the Data centers to access applications. The packets on the network are identified solely on the basis of IP addresses, and there is no classification/distinction of packets that belong to different user groups within the same IP address pool. Overlay technologies like VXLAN allow additional tags to be added to packets, which can be used to identify the origin of the packets and enforce policies based on this additional information in the packets. This allows the packets to carry their identity like an ID badge all the way on the network, and policies can be enforced at any point on the network.

1.7

These technologies can be used to control network access to the users depending upon not only the user credentials, but also based on the type of devices that are being used to access the network. The network access can also be controlled based on the type of software that is being run on the devices, and also depending upon the security posture of the host depending upon predefined security policies or even conducting run-time VAPT before allowing network access. Since the entire functionality is based on the software defined concept, the rich APIs provided by the control points can be leveraged to add additional elements in the authentication workflow and take decisions based on additional inputs that are hitherto unknown to the vendor community.

1.8

Having a controller based network also ensures that there is a central node where all data is aggregated, that can be correlated to gain insights into the overall network behavior rather than get discreet view of health of individual devices. The controller also acts as the central console to provide functions such as configuration management, image management, and push security policies in a coordinated and cohesive manner to all managed devices.

1.9

The network devices can stream information to the controller about the traffic that flows on the network in the form of metadata, or even the utilization of resources on the devices, or other control plane packets. This rich telemetry information can be processed using Artificial intelligence and machine learning algorithms, coupled with the IT best practices fed into the system as policies, to provide actionable insights into the network health. These prescriptive recommendations enable the network administrators to proactively detect and remediate incidents on the network. The metadata information can be combined with additional feeds such as threat intelligence feeds to contain risk, and rapidly detect and mitigate threats. Figure 1 below explains the SDN model.
1.10

Cisco is leading this innovation in the SDN world, and apart from the software defined innovation in the Data center like Application Centric Infrastructure, and Software Defined Wide Area Networks (SD-WAN), Software Defined Access (SDA) as a technology can enable organizations realize the benefits of policy-based automation, end-to-end secure segmentation, complete network visibility, automation capabilities to reduce provisioning times and improve resolution times and enhanced security on the network.

2. RELEVANCE OF SDNS TO EFFECTIVE JOINTNESS

2.1

Against the backdrop of the Jointness imperative, the problem of designing, planning, managing and operating the networks of the three services significantly gets complex. Apart from the need to factor in the nuances of service-specific parameters, operating practices and protocols, we also need to consider the following constraints.

(a) In general, the three services uses different networks for its usual operations than it does for C3I and intelligence requirements. Different service networks have different security protocols, but controlling the protocols, message exchanges and how applications interoperate are the key means to maintaining control over the networks.

(b) Military networks employ a wide variety of technologies. The communications technologies deployed for air, land and sea operations have operational and security requirements that exceed most commercial communications operations. In addition, these service units need to meet strict security oversight and take into account the tactical context and the need-to-know paradigm.

(c) In commercial networks, network tiers are not as firmly defined and separated as in military networks, and commercial organizations have more complex systems for identity management built on top of their networks; in contrast to the more controlled and rigorous
military approach. Additionally, there is more use of high-end and indigenous encryption in military networks than in commercial networks.

2.2

Software Defined Networks can provide a firm hierarchy of network access that is flexible and can be adapted to changing requirements of the organization. When isolated networks (A, B & C) connect to share information and resources using a common IT infrastructure (J), IT administrators have to deal with challenges to ensuring end-to-end segmentation and policy based access control on the network. Figure 2 is illustrative.

2.3

Software Defined access can help achieve that effectively in such environments. The concept of software defined access can be extended to the remote islands which also have the requirements of consistent policy enforcement and segmentation across user groups. Technologies like SD-WAN can be utilized to extend the segmentation in a seamless manner across the points of interconnect of these networks, to ensure that. Policies are consistent not only across one network, but across the entire eco-system.

The following technical benefits can be derived from a SDN deployment described in this document.

(a) By simplifying the design, planning and management of joint networks, they become more flexible in responding to changing operational requirements.

(b) Joint networking which need complex configurations can be enabled by SDN. We need to define interfaces and software inter-operability points.

(c) We can ensure dynamic policy control to meet stringent security requirements. This could also be more responsive and kept simple to ensure it is soldier-proof.

**FIG. 2: FLEXIBLE HIERARCHY OF NETWORK ACCESS**
(d) Military operations are fluid and require rapid deployment of monitoring resources across networks. Flexibility in configuration through software ensures dynamism in deployment of network monitors and choice of metrics.

(e) Since device complexity is removed, management of a large number of devices becomes simpler and across inter-operable boundaries of multiple vendors.

(f) Field Data centers with servers and network elements could make use of SDN technology to allow for network virtualization, increased network security through common configuration, a higher degree of component interoperability, and reduced energy consumption.

(g) We also believe that the network will be cheaper to design and procure as the components become more generic, requirements are similar for components, interference between components could be reduced and over-provisioning of components could be reduced.

(h) Resources may be reallocated on demand, such as in increase of calculation resources or extra bandwidth.

3. CONCLUSION

3.1

On the flip side, SDN requires careful consideration of security imperatives and considering that military networks are likely to be specifically designed, it is unlikely that this commercial technology could be implemented “off the shelf,” but would rather need to be adjusted, and modified to match the needs of the specific service implementation. Joitness requires a high degree of open architectures with flexible, inter-operable and extensible architectures. SDNs meet that requirement.
Conflict in the Instantaneous Age

Brig Ashish Chhibbar and Brig Vivek Verma

Abstract—The first few years of the twenty first century have witnessed the transition from Information Age to Instantaneous Age, where change is extremely rapid, unexpected and unprecedented with the cyberspace domain being transformed into the most lethal and preferred domain for war fighting. Mega corporations of the instantaneous age wield enormous global influence, wealth and technological advantage and are the new Power Centres of conflict. India with its large demographic and digital dividend is at the centre of major powers rivalry and needs to play its cards very deftly and close to its heart. The time to act is now and here.

1. PART 1: SETTING THE STAGE

1.1 Wealth and War

1.1.1
Alvin and Heidi Toffler in the book ‘War and Anti-War’ surmised that the war follows the wealth. A fact that India was raided by marauders during the medieval times and was colonized by the European powers was all aimed at depriving India of its wealth. The petro-dollar conflict has kept the West Asia embroiled in a multidimensional conflict to date. The emergence of information as the new domain and data as its wealth-ware has almost made it imperative that this ‘new oil’ will shape the future conflicts contours.

1.1.2 Advent of Information and Communication Technologies (ICT) has introduced a new pillar to the existing Trinity model propounded by Clausewitz of Government-Military-Economy. The wars up to World War II followed the traditional model wherein defeating of armies or removing the head of state was essential to capitate the nation to surrender. The reliance was on colonizing and then systematically draining the nation of its wealth through creation of trading hubs and strategic logistic chains based on roads, railways and shipping, thus controlling prices and production. While the World War II saw the vanishing of colonies but it ensured that the strategic structures remained undisturbed. This was replaced by a neo-colonist model in form of Marshall and Molotov plan being practiced by the United States of America (USA) and the Soviet Union as part of their Cold War competitive strategy to build alliances and new supply chains for resource diversion. The quest to dominate created rivalry across all domains from nuclear to space and deep sea but it was technology which was spearheading the real contest. Military Technological Revolution (MTR) was practiced by the Soviet Union while the United States rechristened it as Revolution in Military Affairs (RMA).

1.1.3 Some of the technologies shaping the discourse before the end of Cold War in US were Strategic Defence Initiative (SDI) (commonly referred as Star Wars programme) and the development of network systems by the Defense Advanced Research Projects Agency (DARPA). However, the collapse of Soviet Union prompted
Pentagon to scale down SDI and promote internet as it saw the promise in unlocking its value as part of the globalization push aimed towards a model of revenue generation and connect control. The marriage of Internet with communication platforms not only increased its penetrative power across the governance and people but it also brought the people and governance structure to the fore-front of the frontiers to be guarded. The common citizen who was outside the security discourse net was brought into it. According to Gao Heng, the ‘Battle of Depth’ was put in place. The power of information with the people in the democratic and despotic countries gave them the sense of empowerment and in the words of Gene Sharp an ‘alternative’ and ability to shape the destiny of nations which saw its manifestation during the Arab Spring in 2010 and Facebook-Cambridge Analytica scandal in 2018.

1.1.4
Information has redefined the Trinity model of Clausewitz and has given rise to a quad model with people as their fourth pillar and information overhang across all pillars. The evolution of the above model brings to fore following implications (Refer Figure1):

![Changing Nature of Warfare](image)

**Fig. 1: Changing Nature of Warfare**
(a) People and economy are closely knitted and with no defence mechanism built with them will be the first to be targeted.

(b) People and government have close linkage. Hence, affecting people affects the government almost instantly.

(c) Information overhang plays on the ‘Observe and Orientation’ loop of the Observe Orientation Decide and Act (OODA) loop thus adversely affecting the decision and response mechanism.

(d) The volatility, uncertainty, complexity and ambiguity (VUCA) provided by the information platform makes it a low-cost option of controlling and contesting the battle space.

(e) The game will be played in a non-contact mode in both lethal and non-lethal manner where data handling systems will add to the efficiency of weapon systems.

2. PART 2 – EVALUATING THE ENVIRONMENT

2.1 Instantaneous Age

2.1.1

We are presently living in the Instantaneous age. The transition from Information age to Instantaneous age happened during the first few years of the 21st century. The Instantaneous age is characterised by a number of tectonic shifts, each making the age more unique, unknown and unprecedented from the previous known ages of hunter gatherer – agriculture – industrial and information. Firstly, the scale of progress and change has transformed from linear to exponential and logarithmic. A cursory study on emergence of new technologies and businesses in the last decade or so will more than prove this statement. Secondly, wealth generation by utilising natural resources like manufacturing and supply of oil and minerals has more or less stagnated. Real wealth generation is being achieved by monetising artificial resources like data and intelligence. Thirdly, there has been a shift in a nation’s power centre. Earlier, the power centre of a state were its leadership and government. Presently, mega corporations and private enterprise which have a global presence and generate enormous wealth and intellectual capital are the new centres of gravity of a state. Fourthly, ideas and intellectual property are the most critical capital and resource of a state. Major breakthroughs in AI technology have proved time and again that the code or algorithm is more powerful than the machine. A US $35, Raspberry Pi based Artificial Intelligence (AI) system developed by a doctoral graduate of University of Cincinnati was able to defeat a US Air Force trained pilot in combat simulation in June 2016. Fifthly, easily available off the shelf technology and equipment can empower individuals and weak organisations to target and cause harm to major states and organisations. The attack by Houthi rebels to successfully target and destroy oil processing facility at Abquaiq and Khurais in Saudi Arabia on 14 September 2019 is an example of this type of strategic empowerment at low cost. Lastly, instantaneous age is giving rise to a new global world order where mega corporations of global scale are creating enormous wealth and causing disruptions and paradigm shifts in previous age based industry and employment bases across the globe. The wealth which was earlier being generated in decades is now being generated in years and months by neo age Mega Corporations founded in a short time span by new age tech gurus and innovators, most of whom are teenagers or in early twenties.

2.1.2
These Mega Corporations yield enormous power, overcome and stifle competition, own the entire eco system and pick flags. There is an all pervasive culture of winner takes it all attitude. Nation states who have a large number of these Intellectual property (IP) and niche technology based Mega Corporations in turn wield enormous influence and prosper while states who are serviced by these Mega Corporations reap the benefits of digital empowerment at low capital cost but lose out on indigenous technological advancement, flight of home grown and in house generated data and more or less become entirely dependent and at the mercy of the digital eco system created by these Mega Corporations.

2.1.3
United Nations Conference on Trade and Development (UNCTAD) in their “Digital Economy Report 2019” has clearly brought out this tectonic shift in wealth creation in the 21st century. It states “Digital advances have generated enormous wealth in record time, but that wealth has been concentrated around a small number of individuals, companies and countries. Under current policies and regulations, this trajectory is likely to continue, further contributing to rising inequality”.

2.1.4
A comparison of the market capitalisation of world’s top 20 companies in 2009 and 2018 adequately proves the above statement. In 2009, the top 20 companies in the world comprised of seven companies in the oil and gas and mining sector, three companies in technology and consumer services sector and three companies in the financial sector. In 2018, eight companies of the technology and consumer services sector, seven companies of the financial sector and only two companies of oil and gas and mining sector comprise the world’s top 20 companies. What is more surprising is that four of the top ten companies in 2018, namely Amazon, Alibaba, Facebook and Tencent did not feature in the top 100 companies in 2008.

---

3 Ibid, page iv
2.1.5
Among the world's 70 highest valued digital platforms, bulk are based in USA followed by China. US digital companies have a 70% market capitalisation share of the world in this sector with the US hosting more than half of the world's top 100 websites.

2.2 The Age of Mega Corporation

2.2.1
The Mega Corporations need a very specific and niche eco system to create and sustain them. Herein also lies their vulnerability. Some of the key ingredients of this recipe are given in succeeding paragraphs.

2.2.2
Peace, stability and rule of law are the most essential ingredients for setting up and sustaining a Mega Corporation. High end niche human skill set is the most important asset of these type of new age industries. Such a skill set will never be available in any one region or part of the globe and needs to be suitably incentivised and motivated to relocate from different parts of the world and become part of the newly raised company.

2.2.3
Secondly, high end digital infrastructure in terms of power, storage, data sets and computational resource with high speed internet access is a key necessity. Thirdly, a thriving Science, Technology, Engineering and Mathematics (STEM) knowledge eco system with large numbers of English speaking STEM graduates and research and development institutions in the geographical vicinity add immense value and potential to new mega corporations. Fourthly, funding which was a major requirement in earlier years is no longer an issue due to large number of venture capitalists and angel investors looking to grab a piece of the pie in the formative years. Fifthly, governmental incentives in terms of tax breaks, custom duty exemptions, corporation friendly policies, lenient bankruptcy laws and ease in doing business go a long way in fast scaling up of the company as well as increasing the risk taking appetite of the Mega Corporation.

2.2.4
Lastly, once a Mega Corporation is locally well established and has been able to carve out a niche space for its products and services in the hugely competitive global market, there is a need for the government to promote global standards, policies and laws which best serve the Mega Corporation's interests as well as its intellectual property. Then only will the Mega Corporation really fulfil its global ambitions and start creating an exclusive eco system which results in massive wealth generation and strategic leverage.

2.2.5
Since a Mega Corporation requires a very specific type of eco system to sustain and generate wealth, a disruption in a part or whole of this eco system will result in the Mega Corporation greatly losing out on its wealth creation and strategic leverage.

2.2.6
Firstly, disruption of peace and stability in the country where a Mega Corporation is based will result in a flight of skilled manpower as well as capital. Secondly, Mega Corporations are exceedingly vulnerable to new changes in technology that completely and suddenly overthrow existing technologies, revenue generation models and practices. Introduction of taxi aggregator services like Uber and Ola and its effect on local taxi businesses is an example of the above. Thirdly, infringement of Intellectual Property and copying/stealing
of proprietary technology or knowledge will result in the Mega Corporation losing out on their major leverage to generate clientele and wealth. Fourthly, restrictive trade barriers, local laws and policies enforced by countries which host the major clients or generate maximum revenues will also greatly affect the corporation in the long run. Fifthly, change in global standards, laws and trade practices which directly impact the business and revenue models of Mega Corporations. Sixthly, fragmenting the global supply chains and processes and lastly, launching investigations, lawsuits and substantial fines/ penalties on leadership and mega corporations also add to the list of vulnerabilities.

2.2.7

If a country is able to create a Mega Corporation which is capable of giving reasonable competition to an adversary’s Mega Corporation in similar fields then, the winner between the battle of corporations will eventually decide on the net leverage enjoyed by a particular country in the global arena of niche technology.

2.3 India in the Instantaneous Age

2.3.1 Indian cyberspace is growing at an astonishing rate with a projected internet population of 730 million by 2020. We have the third largest internet population after USA and China and our internet population grew six times from 2012 to 2017 at an astonishing Compounded Annual Growth Rate (CAGR) of 44%. It is projected that by 2020, 75% of new internet users would be from rural India and the country will boast of 175 million online shoppers with 75% of e-commerce transactions happening on mobiles.

2.3.2

The ITU in its statistical report titled “Measuring the Information Society Report Volume 2 2018” has done analysis of ICT infrastructure of 192 countries including India. The report focuses on three major areas namely mobile services, fixed services and government policy. The report provides some interesting observations, namely:-

(a) The mobile subscriber base in India is less (87.3%) in comparison with Asia & Pacific (104%) and world (103.6%). In spite of this, India has the second largest mobile phones and smart phones in the world. It is therefore evident that the only available market for mobile phones and smart phones in the world is India.

(b) Our internet access to households and individuals is lacking and needs to be fast tracked.

(c) The quality of our internet access in terms of broadband speed is poor with more than half of population having access speed of 10 Mbit/sec or less. In comparison, rest of the world’s more than 80% population enjoys access speeds of 10Mbit/sec or more. The above is an indicator of poor quality of infrastructure.

2.3.3

The Digital in World and Digital in India report 2019 by Hootsuite shows some interesting trends concerning social media usage, e commerce activity and mobile usage patterns in India. Details of the same are as under:-


(a) Compared to our population, we have on an average lesser number of internet as well as active social media users. However, we are the fastest in the world in increasing our internet population (Adding 97,885,001 user in 2018 alone) and second fastest in growth of active social media users (Adding 60,000,000 in 2018 alone).

(b) Indians have shown an astonishing appetite for internet and social media platforms and this offers enormous opportunity to the government as well as ICT industry.

(c) Our poor literacy figures are a cause of grave concern as lack of literacy (which can be considered synonymous to cyberspace literacy) can result in large number of population falling prey to fake news, cybercrime/ frauds and financial scams.

(d) In spite of having poor internet speeds, Indians generate the maximum data in the world and spend more time on the internet than the world average.

(e) Facebook and You tube are the world’s most widely used social media apps. India has the largest user base of Facebook in the world with the highest growth (YoY). In addition, we have second highest growth of Instagram users. Our You Tube channels have some of the largest subscriber bases in the world. This all indicates that India is a major revenue provider to global social media companies.

(f) India uses more internet linked banking and financial services than the global average. This is a very healthy trend and needs to be encouraged. However, due to our poor literacy percentages, a large number of our internet accessing population becomes susceptible to social engineering and financial cyber frauds and crimes.

(g) Indians have shown remarkable digital optimism. They have tremendous faith towards digitization and use of internet and cyberspace to improve services, provide transparency, root out corruption, optimize governance and distribution of governmental benefits and enhance overall quality of life.

2.3.4
All the above information points towards one major fact that India is a major stakeholder in the global ICT arena and has the potential as well as leverage to create Mega Corporations, give competition to existing Mega Corporations and generate enormous wealth and prosperity by leveraging its ICT potential including availability of a large talent pool of English educated STEM workforce and cheapest rates of internet access, cloud platform services and electricity.

3. PART 3 - PLAYING THE GAME

3.1
The 2018 US Defense Strategy and 2019 Chinese White Paper on Defence clearly looks at the way the competitive strategy is going to be played. While the United States seeks to play the game of dominance, China has been calibrating its asymmetric response as a part of its professed ‘Unrestricted Warfare’. The first phase of the conflict has unveiled itself as part
of the trade-tariff-technology war between the US and China where the Washington has accused Beijing of predatory economics and stealing of technologies. According to McKinsky estimate the AI business potential is between $3.5 trillion and $5.8 trillion annually across nine business functions in 19 industries. This constitutes about 40 percent of the overall $9.5 trillion to $15.4 trillion annual impact that could potentially be enabled by all analytical techniques. Xi in his keynote speech at the 19th National Congress of the Communist Party called for “deep integration between [China’s] real economy and advanced technologies including the internet, Big Data and artificial intelligence.” That pledge came on the heels of the July 2017 release by the State Council of its “New Generation Artificial Intelligence Plan,” a three-step development programme to make China the world leader in artificial intelligence innovation by 2030, generating more than $150 billion in annual revenue from its core AI industry and more than $1.5 trillion from related industries. China’s goals may be ambitious, but it has put in motion the plan to raise its overall artificial intelligence technology and applications to the most advanced level in the world by 2020. In a span of one year from 2016 to 2017 the start-up AI investment in China grew by 11 per cent attracting 48 per cent of the total investment as compared to 38 per cent start-up investment by US businesses. Moreover, China has also overtaken the US in terms of registering AI patents, based on “artificial intelligence,” “deep learning” and “machine learning.”

3.2
According to 2017 Price Water Cooper (PwC) analysis, in the total global impact on GDP outcome due to AI investment China outshines

---

10Ibid.
11Ibid.
the US by garnering 26.1 per cent or $7 trillion with the US coming distant second with 14.5 per cent of GDP or $3.7 trillion. India is way behind with an impact of 10.4 per cent of GDP or $0.9 trillion. (Refer Figure 2). It is quite evident that the 2018 National Defense Strategy assertion of long-term strategic competition with China foundation stone has been laid by the wealth gap creation which adversely affects Washington dominance.

3.3 **Courtesy: PwC Analysis**

Tariff-technology war brought about by the US is a well calibrated strategy to kill the running horse. Washington with its leverage is trying to stifle the Chinese gallop in AI and 5G the future of technology.

3.4

In such a high stake competitive space where considerable traction and lead has been taken by US, China as well as other technology savvy countries like Japan and UK, what are the alternatives available to India and what should be the role of Defence Services in the overall game plan is the moot question which needs to be deliberated and answered.

3.5

Firstly, the primary objective for India is to garner space and elbow room for itself in this exclusive pie, where majority portion rests with US and China. Thus, a whole of nation’s approach is critical in order to reduce the lead and increase the speed of chase. Whole of nation’s approach can only work when the vision, goals and objectives are clearly defined, demarcated and monitored at each and every step.

3.6

Secondly, the market size, scale of data generation, demography dividend, large English speaking STEM population and growing aspirations and Gross Domestic Product (GDP) of the nation needs to be leveraged to generate traction and increase share of involvement in the global digital eco system.

3.7

Thirdly, India needs to create a large number of Mega Corporations in niche technological areas of AI, blockchain, robotics and big data analytics in order to reap the digital dividend of next generational deep impact technologies. These Mega Corporations can only be created if the right eco system as elucidated above is created for them to thrive and create space in the global marketplace. One major factor in our favour is that next generational technologies use the algorithm or code along with vast quantities of data sets as the primary resource for creating products and services. The availability of skilled manpower as well as large volume of data is a major leverage available with us which needs to be optimally exploited.

3.8

Fourthly, India is situated in the middle of the world’s most violent zone and faces all available threats and challenges to its peace and security. The challenges range from nuclear showmanship to conventional conflict, cross border terrorism, left wing extremism, maritime security and piracy. Having a peaceful and rule based environment is the most essential ingredient for creating and sustaining the Mega Corporation. Herein lies the challenge for our Defence Forces.

3.9

Fifthly, in spite of rapid progress made in the last couple of years, India still has a comparatively poor digital infrastructure, power grid and cyber security posture. The same needs to be fast tracked.
Sixthly, need to propagate indigenous technologies and products for home consumption within India as well as becoming the number one choice for ICT product and services in the neighbourhood, especially within the Bay of Bengal Initiative for Multi-Sectoral Technical and Economic Cooperation (BIMSTEC) region is a must in order to become a major regional player.

Lastly, there is a need to play a more proactive role in international fora, especially those pertaining to promulgation of standards and defining global norms, laws and policies in the cyberspace dimension.

**3.12 Understanding Warfare in the Instantaneous Age**

**3.12.1** Rupert Smith, a retired British General Officer and author of the book 'The Utility of Force: The Art of War in the Modern World', asserts that “we are living in a world of confrontations and conflicts rather than one of war and peace; one in which the clear categories of security and defence—the basic purposes for which force is used—have merged”\(^{12}\). He goes on to argue that a paradigm shift in war has occurred. This paradigm shift is from interstate industrial wars to war amongst the people. War ‘ends’ are now focussed on societies and not states with media platforms bringing the fighting into our living rooms. These conditions have made conflicts timeless with fighting directed at not losing the force rather than achieving the military objective. Additionally, emerging threats are exploiting new technology and finding new uses for old technology, with opposing sides frequently being non-state actors. He argues that war is no longer a massive event that achieves well defined political objectives.

**3.12.2** Notwithstanding, the armies across the world are trying to fathom the future course of warfare based on the evolving technologies. Over a period of time there has been a shift in the operational doctrine from ‘massing of forces’ to ‘massing of effects’ with quantum reduction in physical contact between adversarial forces. The pace of technological reforms in the fields of stealth, stand-off precision targeting, networked Intelligence Surveillance and Reconnaissance (ISR) and autonomous systems have compelled major powers like the United States, Russia and China to initiate defence reforms. The traditional battle space of land, seas, air and outer space is overlapping with non-battle space like technological space (Cyber and electromagnetic space), social space (politics, economics and culture) and cognitive space of human mind. Virtually every space is being contested with battlefield significance. Chaos and complexities added by the non-state actors and mega corporations are affecting security discourse. The reliance of competitive strategy on the use of non-lethal means, asymmetric measures and non-contact response options has pushed the boundaries of conflict across multiple domain using ICT.

**3.12.3** Thus, Non-Contact Warfare seeks to employ all elements of national power across multiple domains to target enemy’s population, sovereignty, government structures and economy through kinetic and non-kinetic means with a view to intimidate, paralyse or denude its politico-military response capabilities and enable winning without fighting. In the era of competitive geo-politics, Information Warfare

will play the lead role in shaping battle space across the continuum of conflict to deceive, deny, disrupt and disorientate the governance structures. It will endeavour to create crisis in decision-making where the probability of armed forces being sucked into a subsidiary role may increase. Hence, the challenge for the armed force will be to remain relevant to engage across multiple domains.

4. PART 4–CONCLUSION

4.1
Conflicts in the instantaneous age will be constant, hybrid, cross domain and interspersed with moments of extreme violence followed by periods of relative peace, calm and tranquillity. These never ending conflicts will tire out individuals and nations, create islands of peace, wealth and prosperity around oceans of depravity and violence.

4.2
The instantaneous age has given rise to the era of Mega Corporations, who wield enormous wealth and power across the globe. The nation with large number of these corporations gains economically and strategically with a deep technological divide created between the haves and have-nots. Bulk of the conflicts in the instantaneous age are to create, sustain and leverage the wealth and power of Mega Corporations as these companies pick flags and demonstrate patriotism and loyalty towards their parent country.

4.3
India is at the cusp of a massive digital revolution and has emerged as a major stakeholder in the global cyberspace domain. It is trying hard to make up for lost time and wants to grab a sizeable portion of the global digital eco system pie commensurate with its size, stature and ambition. However, it also lies in the middle of one of the most violent hot spots in the world which makes the task of creating, sustaining and leveraging Mega Corporations exceedingly difficult and challenging.

4.4
An attempt has been made to define the contours of instantaneous age and reasons for conflict and competition in this rapidly changing and evolving era along with options available to India for leveraging its demographic and digital dividend. The strategic game being played in this age is highly complex and fast paced and its outcome will result in major effects which will be felt by generations to follow.
Achieving Synergies in Defence Forces Through Network Centric Warfare System

Deepika Gupta¹, Rupesh Rawat², Devesh Mishra³ and Nitin Gera⁴
E-mail: ¹deepikagupta@bel.co.in, ²rupeshrawat@bel.co.in, ³deveshmishra@bel.co.in, ⁴nitingera@bel.co.in

Abstract—Convergence in Information and Communication Technology (ICT) is transforming military operations by providing commanders with information that is unprecedented in quantity and quality. Secure and jam proof communications between the defence forces in ground, air and sea are essential for executing successful battlefield missions. As the future of war is dependent on information technologies, Jointness of defence forces acts as a decisive factor in determining the outcome of a war. This paper elaborates on the Network Centric Warfare and usage of cutting edge communication technologies such as Software Defined Radios (SDRs) on surface vessels, airborne platforms, ground mobile entities and in Ground C4I segments and further its exploitation for enhancing Net Centric Command, Control, Communication, Computer, Intelligence, Interoperability, Surveillance, Reconnaissance (C4ISR) capabilities for Defence Forces. It also proposes 3D (Tri-services) Network Centric Warfare (NCW) System architecture and high level solution for development of NCW including C4ISR capabilities.

1. INTRODUCTION

Innovation in military is being reinvigorated as a modern concept despite being conceptualised a long time ago. The basic question that needs to be answered is that when innovation is needed in defence, during peace time or during war time, which can provide them realistic scenarios with necessary triggers to move away from established methods of operation.

1.1

The modern warfare is rapidly shifting from human warfare to the age of information warfare. The revolution of information technology in the field of warfare has provided major thrust for this shift. The Indian armed forces are one of the most battle-hardened and combat rich force in the world [1]. Lack of Jointness has been recognized as one of the major weakness and there is an imperative need for an acceptable, pragmatic and implementable Joint warfare structure, system, organization and doctrine for armed forces.

1.2

Jointness is defined as cross-service cooperation in all the stages of the military processes, from research, through procurement and into operations [2][3]. It is also defined as integration of strengths of three wings of military in a coordinated effort to achieve a common goal [4]. It can prove to be a major catalyst in gaining decisive battlefield versatility and confronting uncertainty as joint forces are inherently more flexible and have expanded capacity as compared to stove piped forces [5].

1.3

Jointness also capacititates a new doctrine of warfare known as Network Centric Warfare (NCW) [6] [7] [19]. NCW is an information superiority-enabled concept of operations that generates and increases combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization [6] [7].
The success of NCW is based on the idea that information is only useful if it enables more effective action. Success key of NCW is not technology but people who will use it – the human dimension, which is based on professional mastery and mission command requiring high standards of training, education, doctrine, organization and leadership. It is about the way people collaborate to share their awareness of the situation in order to fight more effectively. The purpose of an information management strategy is to improve human ability to find data and to understand it. The focus required is the minimum information that needs to be exchanged, how to capture that information and how to best display it.

To realize net-centricity, there is a requirement to network all airborne platforms, ground sensors and ground C4I system in a single looped Main Net Centric Network through secure IP and Non IP communication technologies. The system will enable disparate units to share critical information, including data from the battlefield and make speedier decision making.

“Network Centric Warfare is the best term to date to describe the way we fight in the Information Age. NCW translates Information superiority into combat power by effectively linking knowledgeable entities in the battlefield”

RELATED WORK

It is universally accepted that integration and coordination among forces in this new era will be most needed. Various study reports have been published by defence personals across the world. Various committees have been formed and they provided their consent of the importance of joint operations [4] [8] [15] [16].


Synergy between defence forces has many bottlenecks such as different organizational structure, difference in operational tactics, communication gap which in turn increases the uncertainty among forces while joint operations.

The solution for fighting with these bottlenecks is making such a system which networked all the elements of engaged defence forces and provide the information according to needs of specific arm such as Army, Air Force or Navy. The system should be intelligent enough to identify the situation and then transform them as needed by specific forces. Intelligent networked information technology will enable the defence forces to work in more integrated and cooperative manner.

The suggested intelligent Network centric warfare system shall enable the forces to perform joint operations in more cooperative manner with more flexibility and in more
effective way as assembling of forces and sharing information is happening in real time among all the heads of deployed wing of force. This system shall also enhance the resources exploitation capability of forces as duplication of resources for various purposes shall be easily identified by the system because of its networked architecture.

2.6

The capabilities associated with network centric warfare [9] [19] and operations are imbedded in the intersection of the four domains. The physical and information domains provide the infrastructural and informational foundation for information sharing. People perceive information (which is the cognitive domain) and turn it into knowledge; knowledge leads to situational awareness. The entire process takes place in the social domain, which is essentially the convergence of the information, physical, and cognitive domains. It is here that people interact collectively and collaboratively to solve complex problems. This interaction leads to shared situational awareness.

3. NETWORK CENTRIC WARFARE (NCW) SYSTEM

3.1

As discussed above, the NCW system defines an intelligent infrastructure to provide real time monitoring of situation awareness across different heads of defence forces. This system shall use existing technologies like optical fibre for high speed bandwidth and future technologies like software defined radio for connecting different end elements of defence force.

![Diagram of NCW Domain Dependencies](image)

**Fig. 1: NCW Domain Dependencies**
This system incorporates advanced technologies such as Advanced Decision Support Technologies, Tactical algorithms and most importantly intelligent end user display interface. Components of NCW systems are as following:

(a) Networking Media
   (i) SDR based Networking
   (ii) Optical Fibre based Networking
   (iii) SATCOM Network

(b) C4I2SR Technology Framework
   (i) Intelligent End User Display
   (ii) Advanced Tactical Technologies
   (iii) Decision Support Technologies
   (iv) Training & Debriefing

(c) Security Framework
   (i) Secure and jam Free Software defined Radios as Non IP media
   (ii) Encrypted data transfer over IP media

4. PROPOSED SYSTEM ARCHITECTURE

4.1
In this work, we discuss a coherent system framework mainly for tri-services which is able to present a more efficient battle space awareness built on the ability to integrate intelligence, surveillance, reconnaissance and information. All components are connected with the help of IP and Non IP based communication technologies. A high level architecture diagram is given in Fig 2 [10]. NCW system is the core part of this information sharing architecture. Data of various end nodes of different forces are shared with NCW system for centralized processing. A theatre view of extended situation awareness shall be available at 3D strategic NCW ground centre. This processed information shall be distributed to end user as per their operational philosophy with the help of Intelligent Display Technology.

4.2
NCW system will be based on open architecture concept and common generic data format thus enables interoperability with existing system and does not hamper the innovation of any particular head of defence forces. Internally all defence forces are self-sufficient and independent to operate. However, each head can use the information generated from the 3D strategic ground centre which is transformed as per the end user operational philosophy. The main focus of this system is to generate a Theatre View for performing joint operation by sharing real time information [19].

“NCW is therefore an increasingly necessary theory of war to ensure that critical information gets to those who need it fast, whether it is those on the battlefield or those making the decisions at HQ [20].”
4.3 3D NCW Strategic Ground Centre Capabilities

4.3.1 The 3D NCW Strategic Centre in Ground will have high end computing application capabilities which will interface with ground C2 system, surface and airborne platform through SDR and also integrate with legacy systems of Indian armed forces. Following are the major functionalities of Ground based 3D NCW Strategic Centre.

(a) **Reception and transmission** - of data, image and video from SDR fitted surface and airborne platforms in a MANET, other ground C2 system and sub systems.

(b) **Theatre View SA generation** - Perform correlation, association and fusion of tracks as per data received from sensors including target extraction through Image and Video Processing and Analysis.

(c) **Extended Tactical Situation Awareness** - Picture Generation
(d) **Search and Rescue (SAR)** - It can be effectively utilized to provide valuable search and rescue support through direct communication with non-traditional joint players such as the coast guard, local enforcement and rescue crews.

(e) **Intelligence Gathering and Targeting** - The key to military power is targeting and the key to targeting is intelligence relating to the potential enemy's intentions, dispositions and the likely pattern of his operations. Intelligence is vital for identifying the enemy's crucial vulnerabilities, weaknesses and strengths, which in turn will help in devising an effective strategy. A force needs precise intelligence if it is to employ precision weapons. Intelligence also has a direct bearing on the attainment of effect and managing change.

(f) **Mission Planning** - In net centric operations, mission planning is to integrate military minds, analyse the elements of battle, coordinate between simultaneous operations, re-plan operations on time, evade the conflicts of resource and maximise the effect of operation. It includes a decision module, which will have an expert system, assessment system and deduction system. Mission planning system tool includes Flight, Route and Airdrop planning, Weapon Delivery, Target area planning, Radar predictions, Threat analysis, Route fly through etc.

(g) **Offensive Action** - In conventional wars, offensive action was the prime means of seizing the initiative and establishing moral ascendancy over the enemy. This entailed control over the purpose, scope and intensity of operations while placing premium on early action. In unconventional or sub-conventional conflict, the initiative may not be with the state and pre-emptive action without proper.

(h) **Surveillance and Reconnaissance** - Surveillance and reconnaissance operations involve the collection of information from space-based, airborne, surface and ground sensors regarding the activities, forces and resources of an enemy or potential enemy. Surveillance is a systematic and repetitive gathering of information by photographic, radar, infrared, electronic, acoustic or visual means. Information gained from surveillance would be used for strategic decision making and building data bases. Aerial reconnaissance involves the visual/photo observation of specific targets, interests and areas at a particular time to gain information about the activities, resources and intentions of an enemy.

(i) **Situation Awareness (SA) rendering** - The composite picture generated is rendered to the services based on the individual context and relevance.

(j) **Artificial Intelligence (AI) based inference engine for Intelligence gathering and Targeting**

(k) **Real time training and debriefing**
4.4 Challenges

4.4.1

There is not even a single iota of doubt that Jointness is a much needed innovation in military. However, Civilian motivation is one of major challenges in adopting the Jointness in military especially in case of India [17]. The services should not have engaged in a bureaucratic battle over budgetary questions. Country’s vast size and different physical terrain is a crucial element while implementing the Jointness. Training needs, operational tactics are diverse across the tri-services [18]. Jointness shall provide freedom to each head for their progressiveness and evolveness. Trade-off analysis between Jointness and self-innovation in each head must be done before adopting such system. Jointness shall not hamper the revolution in the forces itself.
5. CONCLUSION

5.1

This paper has described the NCW system, a solution for a distributed monitoring and control system for the Jointness of defence forces. We have elaborated the broad level system architecture, showing that with the help of existing network technologies and systems, in addition with advanced and intelligent technologies, tri services information can be shared and synchronized operation can be performed. Triforces shared picture allows the joint force commander to employ right capabilities at the right place and at the right time. This philosophy shifts the view of command and control community from the system centric view to the Network Centric View. NCW system shall strengthen inter services cooperation with independent-ness of self-evolvement to ensure the innovation in each head of forces.

"Jointness is future military innovation."

REFERENCES

1. Annual Report [2018-19], Ministry of Defence, India
4. Fighting Separately: Jointness and Civil-Military Relations in India, Journal of Strategic Studies
8. Achieving Synergies in Defence, Vinod Anand, Senior Fellow, IDSA
10. John J. Daly, Dr. Andreas Tolk, Modeling and Simulation Integration with Network-Centric Command and Control Architectures. Paper 03F-SIW-121, 2003 Fall Simulation Interoperability Workshop
18. Lieutenant General V K Kapoor, PVSM (Retd), An Operational Perspective of Network Centric Warfare in the Indian Context
19. Modern Militaries and a Network Centric Warfare Approach Jonjo Robb, Jan 9 2014
Collaborative Defence R&D: Indian and International Perspective

Gopal Bhushan\textsuperscript{1} and M Madhusudan\textsuperscript{2}

\textsuperscript{1}Outstanding Scientist and Director, JCB, DRDO, India
\textsuperscript{2}Assistant Professor, Department of Library and Information Science, University of Delhi, Delhi, India

E-mail: \textsuperscript{1}g.bhushan@hqr.drdo.in, \textsuperscript{2}mmadhusudhan@libinfosci.du.ac.in

Abstract—Technology is a foundation that offers new possibilities to produce, store and spread knowledge. While science, engineering and research and development are fundamental to a country's growth, the defence research and development is a necessity for country's sovereignty and security. The indigenisation of defence technology is not only an enabler to a country's self-reliance but also a pivot to a country's emergence as a regional or global influence in geo-political tug of war.

The research at basic and applied levels leading to product development for civil or military purposes is pursued by countries in volume and content as per their affordability and resourcefulness. While collaboration among various entities within the country such as government and private research agencies, academia, industry and state-owned establishments is rather straightforward, International collaborations, which could jump-start the process of technology development and technology/product acquisition, are tedious and long drawn. Countries through international collaboration focus on areas which are strategic in nature, however, the technological advanced countries do not easily part with such technologies which are important for their national security and supremacy. International collaborations also face the brunt of global export controls which restrict the trade of military goods and defence technology acquisition.

This paper narrates the role of indigenous defence research and development in a country's vision of being independent from the uncertainties of arms dependency on foreign countries. This paper also provides a perspective of Defence Research and Development (R&D) and the emergence of Indian Defence R&D; bilateral and multilateral engagements and an overview of global military export-trade controls. It also describes how an innovative defence R&D in India has catalysed the growth of domestic aerospace, defence and civil industry and brought a realisation that having an own defence R&D agency is must for a country's long-term strategic sustenance. This paper brings out the fact that no country can produce everything on its own and need to pursue a prolific international cooperation for R&D edge and inclusive growth of domestic industry. It has been concluded that defence R&D capabilities of India are seeing trajectorial growth and which has contributed in India's ascent towards being a regional power.

1. INTRODUCTION

1.1

With rapid technology development and diminishing boundaries between countries, security has become a dominant concern and key global challenge that confronts all nations\textsuperscript{1}. Kofi Annan, UN Secretary General said, “Depending upon wealth, geography and power, we perceive different threats as the most pressing. But the truth is that we cannot afford to choose. Collective security today depends on accepting that the threat which each region of the world perceives as the most urgent are in fact equally so for all. In our globalised world, the threats we face are interconnected and whatever threatens one threatens all”\textsuperscript{2}. The military imbalance in
90s’ resulted in nations demanding advanced and expensive weapon systems and as their defence budget reduced and defence industrial base withered, re-thinking paved the way to re-alignment among nations. The realisation that foreign collaboration was critical for leaping forward and without international support, self-sufficiency, self-reliance, indigenization and the strategic edge over adversaries would be difficult; countries explored bilateral and multilateral alliances. R&D, which was considered the responsibility of government agencies, became global and networked. This led to countries working globally to leverage capabilities of others to achieve own sustainable development. Countries forged International R&D alliances with industry, Science & Technology (S&T) agencies in government and private, academia etc., though within their strategic objective of achieving self-reliance.

2. ROLE OF INDIGENOUS DEFENCE R&D

2.1
Countries realised that military capabilities are not only essential for war fighting, but their ready availability and indigenisation was more essential to deter and dissuade as also to enhance the strategic configuration of military power. R&D across disciplines especially in defence thus has been recognised as one of the key instruments of a country’s foreign policy, significantly by the developed nations3. Space countries pursue indigenous military R&D as per their needs and available domestic resources for their long-term sustenance and view the spending on Defence R&D as an investment on their own security and industrial growth4.

2.2
The significant aspects of collaborative network approach are that they recognise the importance of working across International governments defence research agencies, foreign private defence companies and foreign academia5. However, the Defence technology being strategic in nature, countries do not easily part with advanced technologies. Having own defence research agencies therefore has never been an option for countries but a necessity for nation who wish to hold an edge over adversaries. It is more so in the case of India, which is emerging as a regional superpower and is reasonably self-assured in defence research, development and manufacturing. The self-sufficiency gives confidence to countries to pursue strategic defence R&D and manufacturing partnerships with India. A typical Defence R&D organisation provides strength through knowledge creation and technological superiority to the country. It complements the country’s civil security, public safety and welfare with dual use technology and products as well.

2.3
In India, the Defence Research Development Organisation (DRDO) is the sole government owned defence R&D organisation which caters to the needs of indigenised research, design and development of defence technology and weapon systems of the country. Likewise, the technological advanced countries have identified the core-areas and non-core areas and prioritised them as per their strategic importance to the country. The core-areas are pursued by the government research labs while non-core areas are outsourced to industry and private enterprises that do research, develop, manufacture and export of arms, weapons and dual use items belonging to non-strategic areas under the watchful eyes of the government agencies.

2.4
DRDO which is a fully government owned R&D organisation carries out defence R&D in
its laboratories followed by manufacturing in state owned Defence PSUs and private defence sector. In USA, the AFRL (Air Force Research Lab), ARL (Army Research Lab) and NRL (Naval Research Lab) carry out the defence R&D innovations and futuristic defence research and development. In Israel, it is DDR&D (MAFAT); in UK the DSTL (Defence Science Technology Laboratory); DGA in France; DAPA/ADD in South Korea; FOI in Sweden; DSTO in Australia; DSTA in Singapore, and, DRDC in Canada, and so on. All these organisations have one similarity, to make the country a self-reliant by establishing a very accomplished defence R&D infrastructure, capable of producing the state-of-the-art military goods in the country.

3. EMERGENCE OF INDIAN DEFENCE R&D

3.1

It is a well known fact that India’s requirement of arms is growing but it is still unable to produce them\(^5\). The lack of defence production industry has made India the world’s second largest arms importer and it is spending billions of dollars annually. But where imports are not possible, as in the space, cyber, missile and nuclear realms, India’s indigenous capabilities are notable. The five biggest spenders in 2018 were the United States, China, Saudi Arabia, India and France, which together accounted for 60 per cent of global military spending. India’s military spending rose by 3.1 per cent in 2018 amounting to USD 66.5 billion. To meet the ambition of cutting down the import of military platforms such as fighter aircrafts, helicopters, warships, combat vehicles, etc.\(^6\), and at the same time maintaining readiness for its colossal security needs and not relying entirely on import, India needs a solid and reliable indigenous R&D set up which not only has the capacity to design, develop and manufacture world class war equipment but most importantly can also visualize the nation’s strategic needs even before such need come into existence\(^6\).

3.2

In India, among all government owned civil S&T agencies, the DRDO is the only defence research agency under the Ministry of Defence that supports Indian Armed Forces with advanced technology and military hardware. India, until mid-1970s, acquired all its military equipment from foreign sources and undertook very limited indigenous development and manufacturing. It was realized that to strengthen country’s position and to secure national interests, India needs a strong and technologically advanced defence agency in the country to setup the defence technology ecosystem. This conviction shaped the growth of India’s Defence Research and Development Organisation (DRDO).\(^7\) DRDO was established in 1958 with a limited role of advising the Indian Armed Forces. Today, DRDO is credited with empowering India in the emerging geo-political balance.

3.3

DRDO, gradually over the period of time moved from design and development of small-scale weapon development projects to the development of large military platforms. 80s and onwards, DRDO embarked upon mega projects such as Integrated Guided Missile Development Program (IGMDP), Main Battle Tank (MBT-Arjun), Light Combat Aircraft (LCA), Airborne Early Warning and Control System (AEW&C), Submarine, Artillery Rocket System, Radars, Electronic Warfare (EW) System, Assault Bridges, Underwater Systems etc. DRDO kept adding an array of varied programmes in Nations’ defence preparedness and self-reliance\(^8\). Further, several world class S&T laboratories with system engineering bases were established. The Indian Armed
Forces are being continuously provided with state-of-the-art systems, weapons, platforms, delivery vehicles, sensors, special foods, medicines and life support technologies\(^8\). Despite the technology denials enforced by USA and other countries, DRDO continued to pursue high-end R&D in its laboratories\(^9\). Over the years DRDO's efforts have brought growth to country’s defence ecosystem spanning across industry, academia, private and PSUs\(^10\). DRDO also conspicuously has come closer to discharging DARPA like mandate albeit with lesser autonomy and more constraints\(^11\).

3.4

With gradual economic growth of the country, the budget of DRDO also saw an upward trend leading to diversification of R&D portfolio, supported by a large pool of scientists and engineers\(^8\). DRDO’s contribution on account of intellectual wealth under government’s “Skill Development” and “Make in India” initiatives have been very generously noted by the government. To support design and developmental efforts, a small percentage of DRDO's annual budget is also devoted to sponsored research in basic sciences through DRDO’s various Research Boards and blue-sky research endeavours. Through Technology Development Fund (TDF), DRDO supports Industry to create an eco-system in the country in promotion of self-reliance in defence technology\(^12\).

3.5

The pace of indigenous R&D in the country is still very slow. Considering the growing stature and a significant economic, political and military role that India will have at the world stage, it is prudent for the country to identify long-term R&D direction, strategy and national policy to support the defence ecosystem\(^13\). India’s investment in the Defence R&D is very modest in comparison to countries like, China, Russia, and the USA\(^6\).

4. INDIAN DEFENCE INDUSTRIALIZATION AND INTER-LINKAGES WITH DRDO

4.1

In post-independence India there was a zero - defence industrial base. The first Industrial Policy Resolution which was drafted in 1948, announced defence among a range of sectors in which the public sector would be the main source of production and manufacturing. The policy was revised in 1956, according to which private sector was not to be involved in the munitions, aircraft and shipbuilding industries, and to boost indigenous manufacturing, government-built ordnance factories and Defence Public Sector Undertakings were set up. Realizing that domestic defence production had not progressed as expected, in 2001, government opened private participation and allowed 26% FDI in the defence sector\(^14\). However, the entry of domestic and foreign industry in the Indian defence market did not change the narrative very much. What ailed the private sector was the lack of access to technology from western countries due to export control and restricted trade of military technology, infrastructure support, funding, and confirmed orders\(^5\).

4.2

To obviate the problem, MoD/GoI further liberalized the Aerospace and Defence sector to private and foreign industry and encouraged them for investing in Defence R&D through various modes of acquisition viz., “Buy India/ Buy Global and Make in India/Make Global” and through the new concept of “Strategic Partner”. India currently procures approximately 70% of its defence equipment from abroad but aims to
reverse this balance and manufacture 70% or more of its defence equipment in India\textsuperscript{15}. There is however a need to promote investment in the defence sector both in R&D and production.

4.3
The production of DRDO developed systems has also added a new dimension to the growth of Indian defence industrialisation. DRDO’s relation with Indian industry has been long standing. It partners with Ordnance Factories, DPSUs, major private industries, and approximately 1000 MSME’s. It has established a self-reliant defence industrial eco-system and collectively all have contributed in the growth of knowledge and intellectual wealth of the country. The total production value of DRDO developed products which have been cleared for induction into Indian Armed Forces has reached a staggering in excess to rupees 2.56 lakh crore\textsuperscript{8}. DRDO’s engagements with Industry also involves R&D cooperation which ranges from research, design, development to production and post-production support for sustenance, maintenance, and upgrades of DRDO developed products and upgrades bought from abroad. DRDO amalgamates backward-forward integration by involving private and public-sector production partners from the early stages of the project (forward integration) and by tapping and developing academia and private R&D to help DRDO with incremental R&D i.e., add-on development after technological feasibility is established in the laboratory (backward integration)\textsuperscript{7}.

4.4
DRDO’s Transfer of Technology (ToT) is another avenue for the industry to access the advanced technologies, processes, quality standards and access to T&E facilities. ToT helps building a sizeable domestic industrial base and reduces imports dependency without which DPSUs and private industry have largely been left to assemble knock-down kits produced under license from the foreign maker. With the growth of India’s defence R&D and manufacturing, the country is now seen as an evolving global hub of defence R&D and manufacturing. It has opened another avenue which is the export of defence products developed in the country.

4.5
Export of defence products plays a major role in building country-to-country relations and strengthening its regional presence from the angle of security imperatives. The defence exports have the potential to bridge trade deficit and bring quality realization and competitiveness among domestic manufacturers as well as international companies. The advantage of exporting DRDO developed products which have gone through extensive user trials and user acceptance process before being deployed in the Indian Armed Forces clearly demonstrates that performance wise these systems have been bench marked with competitive international systems. The systems which have been identified for export among many others include tactical missiles, armaments & ammunition, radars, avionics, EW systems, SONAR, light weight torpedoes, communication systems, and EO system. The export of defence goods is an opportunity to expand the visibility of country’s R&D capabilities and earn return-on-investment. Offset is another important opportunity available to domestic industry to enhance export capabilities.

4.6
Within the buying and selling realm of defence, the Defence R&D cooperation is seen as a pivot in a long-term sustenance of county-to-country relations. The Government of India also emphasizes to leverage foreign defence ties to
deepen technology-embedded engagements through research collaboration, academia interaction and JV. Propelled by the globalization of S&T, the international collaborative activity has also evolved in volume and content. DRDO also undertakes defence R&D collaborative projects to overcome technology gaps and expedite the development process.

4.7
The international cooperation is seen as a means of transforming the narrative of buyer-seller to equitable partnerships which are unique, critical, and transformative. Also, as DRDO’s technological capabilities rise higher, more countries seek to collaborate with DRDO. Asian and Latin American countries have expressed desire to work with DRDO to support them building a strong technology capability base in their countries. The "Make-in-India" has also caught the fancy of many foreign countries that are encouraging their defence companies to partner with DRDO and Indian companies for in-country development and manufacturing. The organization has thus become pivotal to India’s foreign policy and national security. DRDO is conscious to keeping its International cooperation within the permissibility of India’s political appropriateness and geopolitical gains.

5. GLOBAL MILITARY EXPORT-TRADE CONTROLS AND INDIA

5.1
Post 1974 and 1998 India’s nuclear tests brought a new paradigm in country’s quest for indigenisation of defence R&D and domestic production capabilities. Country faced arms embargo and trade sanctions led by the USA. The government agencies, DRDO, ISRO, DAE, certain DPSUs and private industry faced global hostile conduct because of nuclear tests which India carried out. Despite India’s stature of a responsible country which adheres to the norms of non-proliferation and respects international technology-denial regimes which control global defence technology order and prevent the spread of materials, equipment and technologies that could contribute to the development or acquisition of WMD. DRDO was the most affected agency in the country due to international trade sanctions. Many high valued and technologically challenging development programs which DRDO was pursuing at that time with the international partners came to stand still. The sanctions could not however deter DRDO. It continued with high-end research and development initiatives and established several world class S&T laboratories and system engineering bases. It re-established its core strength in (a) design, development and limited series production (b) innovative R&D and technology development; (c) development of strategic and tactical systems; (d) research in life sciences to support man behind the machine; (e) optimizing the combat effectiveness; (f) test and evaluation facilities.

5.2
The removal of sanctions took mammoth efforts of the Government of India by synergizing both political and diplomatic channels. However, it was not until recent admission of India into three out of four multilateral regimes that India is now being treated differently. The admission of India into three regimes i.e., Missile Technology Control Regime (MTCR), Wassenaar Arrangement (WA) and Australia Group (AG) have made India to be recognized as a responsible state and at par with member countries. India was accepted into MTCR club in June 2016 as its 35th member, became 42nd member of WA in Dec 2018 and in Jan 2018, India was admitted into AG as 43rd member. The Nuclear Suppliers Group (NSG) is the only...
non-proliferation regime of which India is not a member yet, mostly due to China’s objection to India’s bid. With these developments and India’s recognition as a country which is committed to the cause of non-proliferation, DRDO and similar S&T agencies stand to gain the access of advanced and niche technologies which were hitherto outrightly denied.

5.3
Subjectively, multilateral regimes do not favour automatic approval of transfer of any control item to its members, however as a member of multilateral treaties exudes the confidence of being a responsible country and committed to non-proliferation ethics. Lately, another impediment that is looming large on India is US’s Countering America’s Adversaries Through Sanctions Act (CAATSA), which was signed into law in August 2017 by the US President and went into effect in January 2018. CAATSA mandates to punish those entities which are engaged in significant transactions with the defence or intelligence sectors of Russia. DRDO’s international agreements are always equitable in technical contribution and funds and lays down basic rules of cooperation in terms of administration, IP sharing, information sharing, third party involvement, deliverables and post development aspect of commercialization, etc. A Master Agreement provides an overall governance to specific Project Agreements and Information Exchange Agreements which are signed subsequent to the signing of the umbrella agreement i.e., the Master Agreement.

6. BILATERAL AND MULTILATERAL ENGAGEMENTS OF DRDO

6.1
At government level, the Defence R&D collaboration is considered a strategic alliance between countries and is pursued under the ambit of Government-to-Government dialogue. In Indian context, the DRDO takes the lead in forging defence R&D partnerships with foreign defence research entities in government/private sectors. Proposals/discussions are pursued with the full involvement of MoD and Foreign Ministries from both sides. The other commercial routes are global tender/RFP which is preferred in outright purchases, consultancy and design auditing; Joint Ventures (JVs) for co-development and co-production.

6.2
DRDO has International engagements with about 40 countries. Traditional partners are Russia, USA, Israel, France, Germany, UK, Italy, Canada, Singapore, Sweden, Republic of Korea, Brazil, Czech Republic, Hungary, etc. Some new countries are Spain, South Africa, Vietnam, Australia, Chile, Japan, Malaysia, Egypt, and countries from African continent. DRDO’s international agreements are always equitable in technical contribution and funds and lays down basic rules of cooperation in terms of administration, IP sharing, information sharing, third party involvement, deliverables and post development aspect of commercialization, etc. A Master Agreement provides an overall governance to specific Project Agreements and Information Exchange Agreements which are signed subsequent to the signing of the umbrella agreement i.e., the Master Agreement.

6.3
A Security Agreement provides security coverage in the protection of classified information which could be exchanged through Project/Information Agreements. DRDO’s major international collaborative projects are, the Brahmos, India-Russia Cruise Missile under the JV arrangement, in which DRDO has the major equity stock holding of 50.5% and Russian has 49.9% stakes; Israel-India/DRDO co-developed LRSAM (long Range Surface to Air Missile for Indian Navy) and MRSAM (Medium Range Surface to Air Missile for Indian Air Force). The LRSAM and MRSAM systems are jointly developed by DRDO and IAI Israel under G-to-G agreements; with Brazil, the acquisition of Embraer aircraft and integration of DRDO’s developed AEW&C System; with Russia, DRDO has hosts of technology development programs and leasing of Russian T&E facilities; with the US DoD, DRDO has several ongoing R&D projects and likewise with other countries.
also. DRDO also sponsors research and training programs for the scientists in foreign academic institutions.

6.4

Annual bilateral meetings are held on regular basis to review and evaluate ongoing cooperation; new proposals are presented, resolution to technical and administrative constraints discussed, policy directions, cross-linkages with research laboratories, academia and industry are explored. DRDO also participates in Inter-Ministerial consultations for keeping the organizational interest active and updating DRDO’s strategic tie-ups with MoD and MEA and seeks wherever needed, the intervention at the highest level in the government.

7. INTERNATIONAL DEFENCE R&D COOPERATION TO ACHIEVE INDIGENIZATION OF DEFENCE R&D

7.1

A country to become a great power must enhance its capacity to defend its nation with own resources. While it was understood by countries that there was no alternative to being self-reliant and self-assured to meet the military needs, however, as defence budget reduced and defence industrial base withered, re-thinking paved the way to re-alignment among nations. The realization that foreign collaboration was critical for leaping forward and without international support, the self-sufficiency, self-reliance, indigenization and the strategic edge over adversaries would be difficult and delayed if not improbable, countries explored bilateral and multilateral alliances. The foreign alliance thus began to be measured by the technological strength a foreign partnership brought to both partners (Annan, 2005)1. To better appreciate the uniqueness of Defence R&D, it was important that basic ethos of strategy of ‘Working with Others’22 which seeks to develop a network of partnerships for delivery and capability sustenance was followed complemented with International best practices involving (a) equitable sharing of the cost of R&D and deliverable; (b) sharing of R&D facilities and training; (c) access to a larger and more diverse pool of scientists and engineers; and, (d) exploitation of foreign industry for mutual benefit.

7.2

It is also true that no country can be built and secured through imports. In the past decade, India accounted for about 10% of global arms sales. The imported platform or weapon made India hostage to the supplier nation for spares and service for years. India must ensure the success of “Make in India” and advance its capabilities in frontier areas — from space to missiles — where it already boasts impressive indigenous technologies. However, the prevailing security environment necessitates that India besides developing indigenous capability in defence technology and hardware through domestic resources should also establish a dynamic and product centric (involving research, development and production) International cooperation. Domestically countries establish eco-system encompassing government defence R&D agencies, private and public enterprises and supporting academia but due to inherent limitations of resources the international collaboration plays an important role in achieving return on investment by developing R&D collaboration and producing affordable defence equipment leading to export potential. International alliances also provide an access to advanced S&T which countries either don’t have or need strengthening through complimentary approaches.
7.3
In the Indian context, the defence R&D capabilities of the country are seeing an unprecedented growth and have achieved a commendable level of self-sufficiency. It has time and again proved a pivot to India’s ascent as emerging geo-political power. DRDO’s R&D efforts have catalysed the growth of domestic defence and civilian industries as well as and the impact made by those technological innovations prove the value of having a DRDO maintained by the Government in service to the Indian Armed Forces. Yet, India on its own cannot research, develop and produce everything in the country.23 A prolific International cooperation must thus be the vision that a country should visualise for the sustenance of strategic R&D edge and inclusive growth of country’s researches and industry. DRDO also must endeavor to transform into an agency that visualizes the country’s needs before those needs come into existence; an organization that could research and develop the weapon systems of the future.

8. CONCLUSION

8.1
With the slow shifting of convention paradigm into “Make in India” with the vision to build a military industrial base in the country, the high potential of co-development and co-production under G-to-G arrangement in technologies which are unique, critical, niche and transformative must be encouraged. Collaboration under G-to-G is an opportunity to pool resources, share risk and access world market for export of equipment/weapon systems produced jointly and above all enhance government to government commitment.24 It is also hoped that relaxed multilateral regimes would be helpful in DRDO’s quest for self-reliance and indigenisation. As India aspires to be a technology hub, the aim should be to achieve at least 50% from present 30% indigenization. It will also force the Indian companies to develop their expertise and capabilities that probably would also propel the indigenous content enhanced investment in R&D. In the absence of the will to research and innovate, the goals of self-reliance cannot be met by DRDO alone. The DPSUs and private sector will have to take engineering development for production and participation in the design and development from early stages of project conceptualization. The Indian industries must set up their own R&D capability, instead of a foreign tie up. In the US about 70% of defence R&D comes from the private sector, 30% from the government. In India, 80% comes from the government, and 20% from the industry. That scenario must change. Setting-up defence eco-system, encouraging military industrialization; self-reliance in defence/military weapons systems to meet with country’s strategic intent using International collaborative R&D leading to self-reliance and enhancing domestic capabilities of R&D and production should be prioritized.

ACKNOWLEDGEMENT
This paper is based on the experience which the author has acquired while working abroad at the Indian mission and as Director of International Cooperation at DRDO HQ.

REFERENCES


Systems Approach Imperatives for Designing the Unified Secure & Resilient Digital Communication Infrastructure to Empower the Joint Operations

N Kishor Narang  
Mentor & Principal Design Architect,  
Narnix Technolabs PVT LTD.

Abstract—To achieve the vision of ‘integrated approach’ of jointness, in which there is unity of command and effort wherein the three Services operate under a single commander; the joint operations integrated by communication networks shall be the key to overcoming the wide and fluid assortment of threats our defense forces have to deal with.

However, disparate & heterogeneous communication networks integrated on incremental & need basis shall never meet the changing and ever increasing requirements from the Communication Infrastructure for efficient & robust unified operation. It’s imperative to first develop a comprehensive & granular Architecture using the Systems Approach, which advocates & enumerates a holistic, iterative, discovery process that helps first defining the right problem in complex situations and then in finding elegant, well-designed and working solutions. It incorporates not only engineering, but also logical human and social aspects.

The multiplicity of technologies and their convergence in many new and emerging domains, however particularly those involving large scale infrastructure now demand a top down approach to design, starting at the system or system architecture rather than at the product level.

This paper shall delve into the merits and description of the Systems Approach followed by the characteristics of the Unified Secure &Resilient Digital Information & Communication Infrastructure & approach to develop the Comprehensive & Granular Architecture for the Scalable Critical Digital Infrastructure required for efficient & robust Jointness of the three defense forces.

It shall provide insights into strategies to identify the Pivotal Points of Interoperability, as well as, Zones of Concerns in the Infrastructure Architecture and achieve the comprehensive Interoperability amongst all stakeholders of the nation-wide unified Information & Communication Infrastructure, be it at Semantic, Syntactic or Data Sharing levels.

1. INTRODUCTION

1.1
Large Scale Infrastructures now find themselves making three classes of transformations:

(a) Improvement of infrastructure – to make it resilient & sustainable.

(b) Addition of the digital layer- which is the essence of the operational efficiency; and

(c) Business process transformation- necessary to capitalize on the investments in new technologies.

1.2
Jointness is an overarching concept, which demands Tri-Services embodiment across all functions; operations, planning, intelligence, training, logistics, force structuring, procurement, technology management and
Human Resources Development (HRD). Since currently, even any single Defense Service itself, is a complex “system of systems”, involving many different domains and infrastructures, organisations and activities. All of these need to be integrated and work together effectively for that infrastructure to become efficient, and there are many levels at which integration needs to take place. This is not just integration at a technical level, but also about integration of business processes, management and strategic and regulatory integration. It is imperative that all of these need to be integrated and work together effectively for that Operations to become efficient & seamless in the real sense.

2. SYSTEM ARCHITECTURE

2.1 Networks and distributed client-server systems can deliver integrated information to management, key staff, customers and business partners. In many cases the final system is a composite of elements some purchased, some developed in house, and some that reside in third party organizations. The opportunities are great but so are the risks. If the basic structure, the architecture, of the system is not correct these critical systems may never deliver the expected benefits. The architecture is more than the technical design and includes:

(a) The organization of the work and allocation of responsibilities
(b) The process for ensuring all the components are effectively integrated into a unified system, and
(c) Processes for operating and evolving the system

3. SYSTEMS OF SYSTEMS PERSPECTIVE

3.1 Characteristics that distinguish large monolithic systems from system of systems (per Mark Maier [2]) are:

(a) Operational Independence of the elements
(b) Managerial Independence of the elements
(c) Evolutionary Development
(d) Emergent Behavior
(e) Geographic Distribution

Based on the above characteristics and the management control, different classes of system of systems can be defined as - Directed, Collaborative and Virtual

One relevant example of the Systems of Systems and their classification is described in examples in tables below:
Table 1: Integrated Air Defence and System-of-System Properties

<table>
<thead>
<tr>
<th>Discriminating Factor</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managerial independence of the elements</td>
<td>Component systems are acquired by separate program offices and run by separate operation units, sometimes in different military services. They are connected by their common membership in a military command structure.</td>
</tr>
<tr>
<td>Operational independence of the elements</td>
<td>Connected by a military command and control network, which is integrating in both the technical and social sense. Each component is granted limited operational independence to respond to unforeseen and uncontrolled events.</td>
</tr>
<tr>
<td>Stable intermediate forms</td>
<td>Use of Design Principles. A variety of stable forms, both in time and space, are explicit in the design. Stable intermediates in operation are essential to combat robustness.</td>
</tr>
<tr>
<td>Policy triage</td>
<td>Single service systems are centrally directed, but must deal with legacy equipment and politics. Multiservice systems concentrate on interfacing existing systems acquired in traditional service models. Some attempts to form more centrally directed multiservice systems.</td>
</tr>
<tr>
<td>Leverage at the interfaces</td>
<td>Multiservice systems concentrate on information transfer. Single service systems also trade performance among components.</td>
</tr>
<tr>
<td>Ensuring collaboration</td>
<td>Largely achieved through sociotechnical methods of command and control.</td>
</tr>
<tr>
<td>Directed</td>
<td>The system is developed and operated to a common purpose, and that common purpose is expressed through formal organizations, technical standards, and the socialization of its operators (“Boot Camp”) to the common purpose.</td>
</tr>
</tbody>
</table>
### Table 2: The Internet and System-of-System Properties

<table>
<thead>
<tr>
<th>Discriminating Factor</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managerial independence of the elements</td>
<td>Component systems as acquired and operated by independent users. Component systems are developed (largely) by commercial firms following market dictates</td>
</tr>
<tr>
<td>Operational independence of the elements</td>
<td>Operational coordination is through voluntary adherence to technical standards. The standard setting process is also voluntary. The systems defense against noncooperators is only to exclude them. In the Internet’s earlier stages of development it was more deliberately run by the U.S Government. Government sponsored projects continue to be important to the Internet’s development</td>
</tr>
<tr>
<td>Stable intermediate forms</td>
<td>The structure of the Internet is dynamic, with nodes being added and removed continuously and on their own volition. The main protocols are designed to allow evolution through replacement. The core protocol, IP, is now at version 4 with migration to version 6 beginning</td>
</tr>
<tr>
<td>Policy triage</td>
<td>The oversight bodies exercise very limited control, and carefully restrict their control to the network. Applications and underlying physical interconnects are controlled separately, if at all</td>
</tr>
<tr>
<td>Leverage at the interfaces</td>
<td>The architecture of the Internet is its interfaces. Nothing else is constant</td>
</tr>
<tr>
<td>Ensuring collaboration</td>
<td>The system fosters collaboration through low entry costs and benefits to cooperation. However, it is much weaker at excluding deliberate noncooperators, to the detriment of the system. This is a byproduct of its original development environment</td>
</tr>
<tr>
<td>Collaborative</td>
<td>The system began with a directed purpose, but now follows purposes imposed upon it by its users. Operation and development is through the collaboration (largely voluntary) of its participants</td>
</tr>
</tbody>
</table>

### Table 3: Intelligent Transport System and System-of-System Properties

<table>
<thead>
<tr>
<th>Discriminating Factor</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managerial independence of the elements</td>
<td>Component systems are acquired and operated by independent users. Component systems are developed (largely) by commercial firms following market dictates</td>
</tr>
<tr>
<td>Operational independence of the elements</td>
<td>Operation will be through a complex mixture of individual and government action. Some components (traffic controls) will be run by public agencies at various levels. Other components will be run by private firms. All will require individual voluntary action by travelers</td>
</tr>
<tr>
<td>Stable intermediate forms</td>
<td>Since the system has not yet been built, adherence to design principles cannot yet be evaluated. A pervious paper has discussed the application of these design principles to Intelligent Transport Systems [Maier, 1997]</td>
</tr>
<tr>
<td>Policy triage</td>
<td></td>
</tr>
<tr>
<td>Leverage at the interfaces</td>
<td></td>
</tr>
<tr>
<td>Ensuring collaboration</td>
<td></td>
</tr>
<tr>
<td>Collaborative/virtual</td>
<td>No current body, voluntary or otherwise, control ITS related standards in the USA. Participants (governments, firms, users) will often have conflicting purposes which they will simultaneously attempt to fulfill</td>
</tr>
</tbody>
</table>
4. JOINT COMMUNICATION INFRASTRUCTURE AND SYSTEM-OF-SYSTEM PROPERTIES

4.1 Using the above 3 examples, we may define the Joint Communication infrastructure and its System-of-Systems Properties and its classification as the following tabulated.

**Table 4: Joint Communication Infrastructure and System of Systems Properties**

<table>
<thead>
<tr>
<th>Discriminating Factor</th>
<th>Applicability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managerial Independence of the Elements</td>
<td>Component systems are acquired by separate program offices and run by separate operation units. These organizations are not even connected by common membership or any structure.</td>
</tr>
<tr>
<td>Operational Independence of the elements</td>
<td>Operation will be managed independently by each independent organization managing the system, however goals and constraints will be set for each period by a central command center. Efficiencies will be achieved by autonomous organizational systems through negotiation of policies for achieving goals according to constraints.</td>
</tr>
<tr>
<td>Stable Intermediate Form</td>
<td>The structure of joint communication infrastructure is dynamic, with nodes and systems being added and removed continuously and on their own volition. Main protocols are designed to allow evolution through replacement.</td>
</tr>
<tr>
<td>Policy Triage</td>
<td>Oversight body (Central command) exercises control on the vision of the joint communication infrastructure and what services are offered to forces’ members &amp; departments through various ecosystem partners. There is an effort to form centrally directed multi service system.</td>
</tr>
<tr>
<td>Leverage at the interfaces</td>
<td><strong>Architecture is at its interfaces and the information transfer</strong></td>
</tr>
<tr>
<td>Ensuring Collaboration</td>
<td>Largely will be achieved through socio-technical model of command and control</td>
</tr>
</tbody>
</table>

| Use of Design Principles                   |                                                                                                                                                      |
| Classification                             |                                                                                                                                                      |
| Directed + Collaborative                   | Integrated Command and Control Centre is a nodal agency is set up to develop, deploy and manage Digital Infrastructure solutions. The common purpose is expressed through the joint doctrine vision and similar goals documents. However other components of the joint communication system may evolve and be managed on its own. |

5. SYSTEMS APPROACH

5.1 The multiplicity of technologies and their convergence in many new and emerging domains, however particularly those involving large scale infrastructure now demand a top down approach to design, starting at the system or system architecture rather than at the product level.

5.2 System Approach Concept

5.2.1 Concept that considers that functional and structural engineering, system-wide interfaces and compositional system properties become more and more important due to the increasing complexity, convergence and interrelationship of technologies.

5.3 What is a System?

5.3.1 A group of interacting, interrelated, or interdependent elements forming a purposeful whole of a complexity that requires specific structures and work methods in order to support applications and services relevant to the stakeholders.

5.3.2 A System is more than a collective entity. The System is the product of the interactions of its parts, rather than the sum of its parts. Systems have properties that none of its parts have (emergent properties). The performance of a system depends on how the parts fit not how they act taken separately.

(a) The Systems Approach helps finding elegant, effective solutions to complex problems.
(b) It operates as a holistic, iterative discovery process of the real problems that need to be resolved
(c) It incorporates not only engineering, but also the logical human and social aspects.
(d) Systems Approach is increasingly needed but increasingly challenged in the quest to make future systems scalable, stable, adaptable, and humane.

5.4 Systems Approach in Today’s Challenges

(a) Systems Approach is central when aiming at improved system capabilities and quality of life
   (i) The awareness of the criticality of the human element in complex systems
(b) Ambitious projects!
   (i) Large Infrastructures – Grids, Cities, Communication Networks...
(c) Systems of Systems (SoSs)

5.4.1 Systems Approach helps to address risks deriving from relying on:
   (a) Immature Technologies
   (b) Combinations of technologies with incompatible objectives/ assumptions.

5.4.2 Hence, a reference Framework for a complex system of systems such as a Joint Information & Communication Infrastructure for our Defense Forces shall provide a framework that captures the key domains and their interdependences. It does this in such a way as to provide a foundation for the construction of a whole range of useful views and architectures and models that each describe how the complex infrastructure works from the point of view of a particular domain, or level of integration or specific use case.

5.4.3 Critical Communication Infrastructure of even a single Defense Force is an uber-complex, socio-technical system of cyber-physical systems with the following characteristics:
   (a) Huge volume of digital data and information
   (b) Software-intensive
   (c) Distributed and decentralized
   (d) Great influence on Forces’ operations
   (e) Ability to interact with the physical world
   (f) Seemingly mutually contradictory requirements

5.5 Four Levels of Architecting

5.5.1 If the future solutions are rather complex, then it is recommended to use the following four levels of architecting:
   (a) Reference Model is an abstract framework for understanding concepts and relationships between them in a particular problem space (actually, this is terminology).
   (b) Reference Architecture is a template for potential solution architectures, which realizes a predefined set of requirements. Note: Reference architecture uses its reference model (as the next higher level of abstraction) and provides a common (architectural) vision, a modularization and the logic behind the architectural decisions taken.
   (c) Solution Architecture is architecture of the future system Note: A Solution Architecture (also known as a blueprint) can be a tailored version of a particular reference architecture (which is the next higher level of abstraction). Implementation is a realization of the future system.
The dependencies between these 4 levels are shown in illustration below:

5.5.2
The presence of some “loops” of this illustration confirms the complexity of architecting. For example, there is no guarantee that the original high-level requirements have a high-quality content, e.g. based on a prefect terminology; thus, collecting of important concepts in the reference model may necessitate some modifications in the high-level requirements to align their terminology.

The purpose of the reference architecture is the following:

(a) Explain to any stakeholder how future implementations (which are based on the reference architecture) can address his/her requirements and change his/her personal, professional and social life for the better; for example, via an explicitly link between stakeholders’ high-level requirements and the principles of reference architecture.

(b) Provide a common methodology for architecting the system-of-interest in the particular problem space, thus different people in similar situations find similar artifacts or propose innovations.

In case of the “very complex systems” to be implemented in several projects and the necessity to collaborate and coordinate between those projects, it is recommended to develop a reference solution architecture and, if required, a reference implementation. It helps to identify smaller systems elements (e.g. services, data, etc.) and relationships between them (e.g. interfaces) thus they can be shared between projects.

6. CURRENT CHALLENGES

6.1
The current state of Information & Communication Infrastructure has several gaps that need to be addressed:
(a) **Closed Solutions**: Available solutions are extremely closed with an ecosystem that is highly locked-in by vendors i.e., a single vendor owns the vertical application, platform, communication, services, and data. While convergence of technology, unified standard, interoperability, etc., are necessary to ensure customer-centric systems, open markets are essential for competitive, affordable and sustainable solutions. The existing ecosystem allows minimal or no flexibility.

(b) **Force-Fitting Solutions developed for Different Markets**: There is a natural tendency to force-fit existing solutions developed for other countries & regions such as Russian, European & American, etc., to the different defense forces in India. This may not be the right approach given the requirements, constraints and challenges in India. India specific needs should be factored-in upfront in the architecture of these solutions.

(c) **Inappropriate Last Mile Solutions**: Existing last mile technology for sensor networks are undergoing rapid change to meet radical lower levels of capital and operation cost and much higher level of reliability for mass usage in critical infrastructure. We may need to contract wisely to encourage experimentation and migration to successful new approaches rather than get locked into a high cost solution such as the Dabhol Power Station.

(d) **Deployment Diversity**: Different services are expected to contract separately but we need a method to benefit from some commonality and Service-to-Service arrangements.

(e) **Non-Standard Disharmony**: There is no common framework and architecture defined for the various physical infrastructures to be deployed in the defense forces to work in an integrated, harmonized and optimized manner.

(f) **Dichotomy**: There is a dichotomy between, on the one hand, the need for investment in R&D for new products, systems and solutions based on an integrated and secure System Architecture when there is little awareness about the problem among stakeholders, and on the other hand, the creation of a unified System Architecture and Framework where there is no demand due to ignorance about the problem at hand.

6.2

**Application Domains Landscape**: To meet the diverse requirements of all the stakeholders within the defense forces, the Defense services have to create infrastructure and provide fora collection of as many vertical domains as one can imagine. However, in view the core value of improving the quality of life for the officers & other cadres, as well as address the core & strategic requirements the respective forces, some of the services that need to be catered for are:

(a) Water  
(b) Energy  
(c) Waste Management  
(d) Transportation  
(e) Surveillance  
(f) Connectivity  
(g) Command & Control Centre

However, all these Current Applications live in silos...

6.3

**Creating a Common Visibility of Interrelated Issues**: More often than not creating a
uniform visibility of various issues among the consuming, service providing, and governing stakeholders reduces creation of multiple lines of communication and resultant cacophony and noise. At present such platform, which can create inclusive visibility of issues, resolution plans and efforts are also multipoint and vertical specific. Additionally, due to vertical implementation there is lack of transparency and resultant mistrust, suspicion, dissonance and scope of manipulation and corruption. This lack of transparency in what is transpiring within a silo extends both to consumer and to governance layer and strengthens the manipulative element within the vertical domain.

6.4 Interoperability Among the Cross Domains: Once even when a common visibility can be obtained, there can be several issues which are sufficiently structured, that automation and cross domain integration can be achieved and thus delays inherent to manually intervened actions can be avoided, and greater operational efficiencies achieved.

7. THE WAY FORWARD: UNIFIED ARCHITECTURE

7.1
From a siloes approach to a converged common ICT infrastructure pool - Coordination, collaboration and harmonization can be better implemented by the effective use of open, common and shareable, information and communication technologies that allows the creation of a truly interconnected system with seamless communication between services. Even though the services and applications can be diverse, they could leverage the use of common infrastructure to achieve this objective.

7.2 Integrated Management for Common Visibility of Interrelated Issues - At its very foundation, it will integrate with and ingest data from all possible sources, then apply various data models, processes and tools and ensure quality with an aim to provide insight and intelligence on various city resources and services while at the same time establishing a sharing and serving mechanism for all information resources and services in any earmarked geographical territory or across multiple distributed locations.

7.3 Different sources of information can blend together, in some ways compensating their own deficiencies, enriching the larger information pool and therefore providing the ability to offer services more efficiently.

8. THE INTERPLAY – UNIFIED SMART INFRASTRUCTURE – UNIFIED SMART FORCES

8.1 The relationship between Unified Smart Infrastructure and Unified Smart Forces needs to be understood in this context: “In smart forces, beyond the strategic & core services, energy, water, transportation, public health and safety, and other key services need to be managed in concert to support smooth operation of critical infrastructure while providing for a clean, economic and safe environment in which to live, work and play”.

8.2 Hence, the perspective in Infrastructure Design has undergone a paradigm shift with advent of convergence and networking technologies, solutions for information, communication, entertainment, security and surveillance; which are beginning to have a profound impact
on the way we look at the Buildings’ Design (be it residential or commercial) and Town Planning, be it for civic infrastructure or the strategic infrastructure.

8.3
Defense forces are intricate composite environments and the manner in which forces are operated, financed, regulated and planned are extremely complex to say the least. Forces operations are multidimensional and comprise of multiple stakeholders whose dependencies and interdependencies affect and ultimately determine the built & operational environment.

8.4
The various departments mostly overlook these dependencies and interdependencies though known, in their efforts and focus of providing their services and of being answerable only for the services they provide. Part of the answer to making forces ‘smarter’ is a more all-embracing coordinated management of resources and infrastructure, a collaborative approach to improve the operational efficiency of its strategic deliverables to the nation.

8.5
The hugely complex nature of a large infrastructure project creates a very real risk that oversights in the planning phase can cause the sub-optimization of sub-systems, which can severely impair the overall success of the project. Organizations can mitigate this risk by taking a far-reaching, structured, and detailed approach to project planning. By encapsulating the requirements of all stakeholders (both within and outside an organization), modeling the impacts of change, and tracing requirements throughout the project, it is possible to quantify the impact of different decisions in the planning stages, rather than realize mistakes once the project has been completed.

8.6
The relationships of diverse information resources are complicated and could be complementary, reinforced or redundant relationships. The data gathered can further be processed and modelled, correlated with historic data and other activities performed on it before it can be made insightful and can be presented to offer MIS, analysis, decision support or forecasts.

8.7
There is also a recursive cycle to the data in any large organization or infrastructure. Information that is generated is information that is consumed which in turn adds to the information generated which becomes information used again.
An example of recursive nature of Data

8.8 Seven Layers of Information Flow – from Data to Knowledge

Mapping the Smart Infrastructure Philosophy to High-level Functionality - To analyze the relevance of Big Data & Information management in the large infrastructure, we need to contextualize this “Seven Layer Information Flow & Processing” with the entire gamut of use cases to convert the diverse and heterogeneous data collected in Defense Forces to knowledge that would in turn be further processed to provide the Actionable Insights to the Strategists, Planners and other stakeholders. This is achieved by mapping the “Seven layers” to the various Pillars of Defense services framework – Physical Infrastructure, Social Infrastructure, Institutional Infrastructure and last but not the least the core Warfare Infrastructure. The detailed analysis shows that different services applications need changes as part of the user requirements to derive value from different infrastructure pillars but the ICT backbone remains the same.

9. JOINT DEFENSE SERVICES NEED ENTERPRISE ARCHITECTURE

9.1 Any complex system e.g. a building needs to be carefully designed, using a systematic approach, to describe in detail its structure, all the processes needed to fulfill the purposes of the building and all the subsystems within it (water, waste, electricity, telecoms, etc.) and how its design meets the different functional requirements of its users. For instance, for an airport there needs to be detailed descriptions of how luggage is moved around, how passengers get to their plane, how fuel is provided, how planes are serviced, how security is managed, etc., as part of the overall architecture of the building complex.
9.2
This is needed at the construction phase to ensure that the building is properly designed to enable it to fulfill all the requirements of its purpose. However, it is also needed to support the on-going management of that building and to support the design of any alterations and upgrades needed to meet any change in requirements or to benefit from new technologies to fulfill existing requirements.

9.3
The aims and strategy, business structures and business processes of an enterprise and the software applications and communications infrastructures that support them, also need to be carefully described and reviewed. Only in this way is it possible to ensure that its business structures and processes can effectively support the delivery of its strategies and outcomes and to allow these to change and adjust to changing requirements and opportunities.

9.4
Enterprise Architecture is the definition and description of an enterprise from the combined viewpoints of its strategy, business structure, business processes, information systems and technology, both in terms of how it is at present, and of how it needs to be in the future.

**Enterprise Architecture**: The analysis and documentation of an enterprise in its current and future states from a Strategy, Business, and Technology perspective.

\[ EA = S + B + T \]
Development an Enterprise Architectural Framework and a Key Definitions Framework for Joint Defense Forces would need to draw on existing best practices describing the way Forces work in order to ensure that the processes deal with all of the key issues. Clearly adaptations would be needed - for instance we might add an Environment and Infrastructure layer Translating the Digital Infrastructure Architecture Schema to Technology Layers

EA defines how business and Information systems alignment should be achieved. It is where business capability (financial and market goals) and technology capability (products, vendors, and functionality) are tied together with organizational capability (people or process) to drive an ongoing strategy or desired outcome. SOA is recognized as a methodology optimized in applications architecture or Service architecture, with a view to deliver one of the domains within EA namely the applications architecture.
9.6 The Paradigm Shift: From Siloed to Unified - From Vertical to Horizontal

9.6.1
All sectors in the infrastructure framework are influenced by the unified ICT backbone paradigm. However, a common infrastructure pool enables the creation of a interconnected and truly homogenous system with seamless communication between Services. Coordination, collaboration and harmonization can be better implemented by the effective use of standards based open, common and shareable, information and communication technologies. The disconnect amongst technological trends being pursued by the stakeholders of the now homogenous smart infrastructure needs to be bridged without any further delay to maintain the Lifecycle Cost / TCO (total cost of ownership) of these individual components within viable economic thresholds.

9.6.2
Forces that are serious about getting smart know that they cannot rely on traditional ways of doing things. Vertical rollouts, where each communication use case is propped up by a dedicated network, use case-specific data exchange mechanisms, and single-use devices, do not scale.

As defense services strategists strive for greater cross-departmental synergies, it is essential that networks and devices, as well as data, can be used for more than one purpose. Even better if various functions, such as device management, security and communication management, can be shared by multiple applications.
10. SMART CITIES ANALOGY TO SMART DEFENCE FORCES

10.1

The Defence Forces have a lot in common with the cities, beyond their core & strategic operations in defending the sovereignty of the nation. Their base stations and cantonment areas are cities in themselves, and much more. It would be interesting to review how cities are transforming into smart, sustainable, secure & resilient urban habitats. The cities are now embracing the Unified Digital Infrastructure Architecture to meet their imperatives of sustainability, security, resilience along with much needed operational efficiency.

Typical Data Layer Architecture for a Smart City

...Classic Saucer Champagne Glass Architecture:
10.2
The evolved Comprehensively Unified ICT Architecture can be modelled as a “Classic Saucer Champagne Glass” with a wide Flat Bottom Base depicting the multitude of Field Devices & sensors etc. The Saucer Shaped Bowl on the Top depicting being filled with an ever-increasing spectrum of City Applications and Citizens’ Services. The Long Stem depicts all the Common Layers viz.: The Unified Last Mile Communication, Common Standardized Gateways (application or Vertical Agnostic), Common Service layer representing the Common Service Functions in the Gateways, as well as, in the Cloud and the Smart City Middleware & City Data Reservoir in the Cloud.

10.3
It is the “Long Stem” of the “Champagne Glass Architecture Model” instead of the Short & Narrow Neck in the “Hourglass Model” that brings the comprehensive harmonization, standardization & interoperability in the Architecture leading to optimization in operational efficiency & Life Cycle Cost of the ICT Infrastructure in any Smart City.

10.4
This architecture model helps reduce the carbon footprint of the ICT infrastructure, and last but not the least, enables comprehensive security, as the infrastructure is well architected hence all the vulnerability surface areas are well identified, hence well protected.

11. CONCLUSION

11.1
Communication Infrastructure projects are often connected to other aspects of infrastructure and should be thought of as large systems of systems, the success of which relies on the optimization of all the sub-systems that support it. Some of the earliest deployments of digital infrastructure have proven to be not so smart. Most deployments have failed to identify dependencies or interactions with adjacent systems, impacting overall performance and restricting functionality.

11.2
The convergence of multiple networks and technologies, particularly in new and emerging markets involving large-scale infrastructures require a top-down approach to standardization, starting at System Architecture rather than at product level.

11.3
The systems level approach recommended above in design is likely to not only enable newer and better services, but also allow far greater synergies and cost-effective deployments, reducing the lifecycle (total) cost of ownership of any Infrastructure, be it the civic infrastructure of the Defense forces or the Warfare Infrastructure, with attendant environmental benefits, including carbon reductions and building system resilience.

11.4
An integrated approach to Digital Infrastructure assets can help define and strengthen the System standards throughout the technical community to ensure that highly complex market sectors can be properly supported for the increasing conformity, harmonization and convergence of both Information Technologies (IT) and Operational Technologies (OT) systems. There is a need to focus on the creation of a secure, standardized and open infrastructure model for the delivery of services.

11.5
The proposed jointness of Communication Infrastructure amongst the Three Services
shall need a systemic approach to develop a comprehensive & granular architecture to meet the current, near future and long-term requirements of the Indian Defense Forces leveraging the latest disruptive technologies like Big Data, Machine Learning, Artificial Intelligent, Digital Twin, 5G and Quantum Computing etc. in a very structured manner.

REFERENCES
1. IES-City Framework https://pages.nist.gov/smartcitiesarchitecture/
Abstract—Military operations are complicated by increasingly complex demands on the EM spectrum, which is a physical medium through which joint forces conduct operations. The EM spectrum is a highly regulated and saturated natural resource. The Defence services use the EM Spectrum for operation of its command and control systems, modern weapon systems, electronic sensors like RADARS and weapon platform operations. Due to the unique characteristics of frequency spectrum and joint operations of the future war, central management of the electromagnetic spectrum among Tri-services is essential.

1. INTRODUCTION

1.1
In the years to come, in any modern Army/Armed Forces, the warfighting requirements of the organisation are identified in the Armed forces functional concepts of perspective planning and force development. In order to support the futuristic war fighting capabilities, all modern armies will need to procure equipment, which in turn will require an exponential increase in the use of the electromagnetic (EM) spectrum. Recent years have witnessed an explosion of spectrum-based technologies and uses of wireless voice and data communications systems by the Army, as it transforms to a battlespace that is more dynamic and has ever increasing demands for information. This requires an effective and efficient system for Management of EM spectrum in the tactical battle field.

2. TACTICAL BATTLEFIELD EM SPECTRUM MANAGEMENT SYSTEM

2.1
Existing Methodology. All modern armed forces depend on EM spectrum and the importance of the EM spectrum and its relationship to the operational capabilities needs to be properly understood, addressed and optimally utilised. The EM spectrum includes the full range of all possible frequencies of electromagnetic radiation and there is a requirement for coordinating EM spectrum access, throughout the operational environment, among various stakeholders, including Doordarshan, Airports Authority of India, Min of Communication, Dept of Space and within the Armed Forces. This is as it is a challenging task during peace time and assumes even greater importance in a tactical battle field environment.

2.2
Rationale for Automation. There is a need to have an EM Spectrum Management System in the Tactical Battle Area (TBA), to assist in the systematic planning, managing, engineering, and coordinating use of EM spectrum by units engaged in combat and training for combat. At each level, the signal officer is responsible to the commander for spectrum management. At Division, Corps, and Command levels, (and possibly later at theatre levels also, should the concept of Theatre Commands be implemented), specially trained members of...
the signal staff section perform the day-to-day functions for management of EM spectrum. The spectrum manager is responsible for coordination with higher, subordinate, and adjacent units and with other staff sections. The end state aims to exploit, attack, protect, and manage resources within the EM spectrum and resolve electromagnetic interference (EMI) in order to achieve the commander’s objectives. There is a felt need to automate this complex activity.

2.3

Management of EM Battle Space. There is need to procure and deploy a web based system to manage the EM battle space. This will help to automate the spectrum management and assignment issues to achieve EMC in the battlefield. This would be a comprehensive solution for management of the EM battle space, for the three Defence Services i.e, Army, Navy, Air Force and HQ IDS. Such a system would be launched hosted on the existing secured Defence Communication Network (DCN) to provide connectivity to the users in the HQ and field. It would be a web based system with minimal footprints on the user machine. Once deployed, the proposed system would manage and optimize frequency assignments for all electromagnetic emitters and receivers present in the complete geographical area, on a near real time basis. It will also aid the spectrum manager in calculating the spectral density at any location and carry out the interference analysis for all the emitters and receivers in India.

2.4

Procurement Imperatives for System Envisaged. These are listed as under:

(a) There is a need to automate the present system of frequency assignment with a view to achieve higher spectral and procedural efficiency and avoid interference during joint operations.

(b) The present system is highly dependent on the personal expertise of the individual concerned. There is however no interference prediction and hence it provides limited guarantee against the assigned frequency interfering with other equipment in the intended area of operations. The system presently in use is suited for the era where density of communication-electronic equipment was sparse and is not likely to function optimally in the current technology heavy battlefield scenario, especially during hostilities.

(c) The present system cannot guarantee unimpeded operation of these critical systems, when used simultaneously in an actual battlefield environment.

(d) The present system does not optimize reuse and sharing of spectral resources in time and space. The spectrum is assuming more and more significance as a very costly and scarce natural resource. Thus wastage of such a precious resource cannot be allowed in the present and near future.

(e) Thus, the need of the hour is to procure a high end specialised software solution, customised to the user requirement in a reasonable time frame, which could address these procurement imperatives.

2.5

Capability Expectations. The capability being sought to be inducted should help in:

(a) Automation of the Spectrum Management process and frequency assignment process for frequency ranges from 10 KHz to 450 GHz.

(b) Quick assignment of frequencies to the users of the three Services & HQ
Strategic Forces Command (SFC), in a manner that minimises the interference between various emitters.

(c) Maintain a secure database of all assignments and emitters in the area of responsibility. The database could be made accessible to authenticated users on a need to know basis, on a secured media.

(d) Capability of performing Radio Network Planning, including Electro Magnetic Interference / Electro Magnetic Compatibility (EMI/EMC) analysis at any specified geographical area of India through interactive Geographical Information System (GIS).

(e) The system should be able to map the spectral density of the entire country and generate propagation models for all the emitters. It would take into account the terrain and atmospheric conditions to ensure effective management of spectrum in the battlefield and also during the peace time. With this readily available database, joint mission planning can be undertaken more effectively and without any interference.

2.6 Payoffs Envisaged.

(a) Optimum Utilisation of Scarce Resource. The Defence Services use the EM spectrum for operation of their command and control systems, modern weapon systems, electronic sensors and weapon platform operations. In view of the growing commercial demand for the spectrum, the Services share of this natural resource is limited and is likely to shrink even further. Due to the unique characteristics of frequency spectrum and joint operations of the future war, there is a pressing need for its central management among Tri-Services. The system presently in use is suited for the era where density of communication-electronic equipment was sparse. This is not likely to function optimally in the current technology-heavy battlefield scenario. Once such a system is procured, it could be deployed on a secured media network (i.e, DCN).

(b) Automation. Once procured, the system would automate the Spectrum Management process for frequency ranges from 10 KHz to 450 GHz and automate the frequency assignment process through simulation and modelling to achieve spectral efficiency. The system would be performing Radio Network Planning including EMI/EMC analysis at any specified geographical area of Indian Sub Continent through an interactive Geographical Information System (GIS).

(c) Accessible to Multiple Users. The system would be a web based system capable of being hosted and seamlessly functioning on the existing network of the defence Forces. This web based system would be capable of servicing multiple users. Authorised users will be able to access the database and carry out the analysis of technical feasibility of installing various base stations and links used by Indian armed forces, remotely over the web.

(d) Visual Display of EM Spectral Occupancy. The system would calculate electromagnetic influences associated with individual emitters and receivers and display the same on a suitable map display for ease of decision by assignment authorities. The user would be able to easily discover technical
characteristics associated with emitters displayed on the screen. It would also predict and display the electromagnetic spectral occupancy at a selected geographical point based on defined propagation criteria. Once deployed, the proposed system would manage and optimise frequency assignments for all electromagnetic emitters and receivers present in the complete geographical area on a near real time basis.

(e) **Web Based Spectrum Management System.** The proposed system would consist of spectrum management application software, along with centralised server equipment and associated hardware/software components. This secure web based system would be hosted on the existing secured network maintained by Defence Services for user connectivity and would seamlessly integrate into the existing network architecture. The application and the associated databases would reside on servers placed at two locations, to cater for redundancy. The users would access the application through a secure web browser with comprehensive access rights management mechanism for ensuring data security.

2.7 **Tasks Automated.** The proposed system shall automate the spectrum management and frequency assignment to achieve spectral efficiency and ensure Electro Magnetic Compatibility in the battlefield. The proposed system would manage and optimise frequency assignments for all electromagnetic emitters and receivers on a near real time basis. It will help the spectrum manager in achieving the following tasks:-

(a) Accepting and processing requests for frequency allotment from various users and maintaining record of requests.
(b) Analysing the EMI / EMC for the requested frequency.
(c) Aiding the spectrum manager in taking the decision on the existing users and estimation of spectrum occupancy.
(d) Data keeping and maintenance of all station information in a central database system with online-query capabilities.
(e) Searching for free frequencies out of a given frequency pool or suggestion of frequencies to be applied.
(f) Maintaining a database of all the requests, authorised frequencies, allocations, parameters of various emitters and spectral density at various geographical locations.
(g) Tracing of the request process and assigning frequencies to the three Defence services for each and every specific system.
(h) Management of the radio frequency spectrum.
(i) Coordinating the frequencies with the Wireless Planning and Coordination Wing (WPC) and within the three Services and any other organisation.
(j) Estimation of spectrum occupancy.
(k) Technical analysis and preplanning of stations and networks as well as extensions of networks.
(l) Generation of reports in the user specified formats.

3. **CONCLUSION**

3.1 **The system proposed is necessary to facilitate**
the management of EM Battle Space and optimise the planning and utilisation of
scarce spectral resources across space and time in an intense, dynamic and mobile battle environment. The system will help maximise the spectrum efficiency and minimise interference. By capturing the EM characteristics of all equipment it will help populate a database for the same. The same would result in automation of demand and assignment of frequencies from field user level till respective Service Headquarters, on a real-time basis. The effects of allotment of particular frequency spot to the same equipment or other equipment in the battle space would be simulated, based on operating frequency, equipment characteristics, propagation models, terrain and environmental models. This would in turn help in developing a geo-spectral database, depending on existing and required frequency assignments, which is the need of the hour. The information about authorized emitters would be stored in the central database and compared with the information available from the spectrum monitoring system. This should facilitate the identification of authorised users and find if there are any unauthorised emitters causing interference. This is thus the way ahead for the Armed Forces for ensuring both spectral efficiency and effectiveness.

REFERENCES


BIBLIOGRAPHY

Reorganisation of Indian Spectrum Administrator

Maj Gen LB Chand, VSM (Retd)
E-mail: lavchand@rediffmail.com

1. PROLOGUE

“Electromagnetic Spectrum (EM) is an inexhaustible, reusable yet quantitively finite resource”

“Spectrum can neither be created nor destroyed. But it use can certainly be destructively intrusive or wasted if not properly administered”

“Spectrum has been categorised as a National Natural Resource and controlled through Administrative License”

“Most countries adopt an administered system of allocation, which may be in the form of first come first served (FCFS) methodology, beauty contests or lottery.”

“Chawla Committee on Allocation of Natural Resource (CANR) - 2011¹ recommendations are still pending acceptance by GoI. However, the favoured method of allocation by the Government of India is Auction”

“CANR opines - The experience of countries in Europe, who auctioned 3G spectrum in the first decade of this century at high bid prices led to large destruction in firm values and delay in roll out.”

“CANR - The choice of the appropriate method of allocation of spectrum, therefore, depends critically on the context, market conditions and the objectives of extant telecom policy. However, given the current state of development of the Indian telecom market, the Committee has recommended that in future, spectrum for telecom access services should be made available through suitable market related processes.”

“CANR- The other significant recommendations of the Committee are that all future telecom

¹Chawla Committee Report – Committee on Allocation of Natural Resource 2011.
licenses should be unified licenses and also de-linked from spectrum; and, effective measures should be taken to ensure continued efficient usage of spectrum inter alia through re-defining the appropriate geographical units for allocation. At the same time, vacation and re-farming of spectrum for commercial services should be expedited to ensure availability and certainty of adequate spectrum to facilitate optimal usage and revenue realization. Finally, a comprehensive and integrated legislative frame work for spectrum management – both in respect of commercial and non-commercial frequency bands - should be put in place to ensure optimal and efficient use of country’s spectrum resources.”

“Spectrum worldwide has been allocated through Administrative License – India is no Exception”

“National Frequency Allocation Plan was established 1981. Till 1989, the allocation was user based and Defence Services, along with Other Security Forces having lower priority were Categorised as Major User. With the formalisation of New Telecom Policy - 1999 (NTP) the Spectrum Allocations became Service Based from User Based”

“Services Based National Frequency Allocation Plan (NFAP) - 2000 was promulgated in 2000. NTP 2012 was promulgated”

“In accordance to the MoU of May 2009, between MOC&IT and MoD on Release of Spectrum by Defence, Defence Band was formulated by a Committee Co-chaired by Secretary MOC&IT and SO-in-C ion 2010 and was promulgated with certain foot notes in 2014”

“Milestones and timelines for release of Spectrum by MoD have not been adhered to. There are inordinate delays. This has a cascading delaying effect of Vacation of Spectrum by MoD and refinement of Allocation of Spectrum procedures from within Defence Band and most importantly optimum utilisation of spectrum for International Mobile Telephony (IMT) Services”

“Unilateral Decision by Wireless Planning Coordination Wing (WPC) on Spectrum allocation from within Defence Band and delay in implementation of Network for Spectrum (NFS) is complicating the Spectrum usage and is nullifying the extensive efforts of the past in cleaning up and coordinating Spectrum utilisation. If not checked it will adversely impact the National Security.”

“The very nature of EM Spectrum being an invisible commodity, can very easily lead to its theft and encroaching into spectrum band not in use”. WPC has adequate resources and
organisations to resolve spectrum interference, encroachment and misuse internationally (ITU through Monitoring Stations) and nationally (Wireless Monitoring Organisation-WMO). In comparison, Defence and other Security Forces are totally blind wrt their Defence Band monitoring. They are reactive, based upon physical interference experienced and totally dependent on WMO, WCP.

Joint Communication Electronic Staff, HQ Integrated Defence Staff (JCES, HQ IDS) is and has been the lead agency for spectrum harmonisation, coordination, allocation and assignment for Defence use. For Defence Forces monitoring of EM Spectrum was done by WPC. This procedure was adequate till Defence was the major spectrum user. With rapid growth of IMT, the demarcation of EM Spectrum bands for national security and commercial use has blurred. Promulgation of Defence Band has necessitated establishment of Spectrum Monitoring Organisation by Defence.

Long Term Evolution (LTE) and 5G has resulted in harmonisation of additional bands and re-farming for LTE and 5G. Internet of Things (IoT), Machine to Machine (M2M) etc have placed additional demand on EM Spectrum. The only method to meet this ever-increasing spectrum demand is spectral efficient technology – more bits per hertz and harmonisation of Higher Spectral band (> 30 GHz).

To complicate the issue developing nations consider EM Spectrum as a readily available source of revenue for the government. Unfortunately, this is a myopic approach and with negative fallout in longer terms.

Abstract—Post Promulgation of Defence Band there is a necessity to have Armed Forces playing a greater role in Administration of EM Spectrum and particularly the EM Spectrum reserved for Defence. The growing pressure on definite supply of EM Spectrum on one hand and the monopoly of Wireless Advisor over EM Spectrum, as laid down by archaic Indian Telegraph Act 1939 has not only denied adequate EM Spectrum to Armed Forces but also resulted in harmonising spectrum for spectrally inefficient technology. The objective of the paper is:

(m) Based upon the Internationally successful Spectrum Allocation (Federal or Defence Band: USA, UK and other countries) recommend reorganisation of Defence Spectrum Management.
(n) Suggest a Defence Wireless Monitoring Organisation.
(o) Changes necessitated in the existing Act and Rules of Business.
(p) Recommend method to ensure EM Spectrum is not wasted during Peace Time due to it remaining unutilised. And more importantly to ensure that the release of spectrum for Defence use is not delayed when required for National Security.

2. INTRODUCTION

2.1

Radio Spectrum is a limited Natural Resource with extraordinary Strategic, Social and Economic importance. Radio Spectrum does not respect Military or Commercial or for that matter any other man-made boundaries. Radio spectrum is a key input and an integral component of almost all military operations.
and military applications that need radio spectrum for command, control, navigation, communications and information systems, IT (wireless LAN), intelligence gathering, surveillance, reconnaissance and targeting etc. Within the Indian Armed Forces, the Radio spectrum supports a very wide range of vital military requirements including peacetime training and operations, use for internal security and preparations for major operations. In the context of Radio Spectrum having tremendous commercial value but with no physical form/ boundaries/ physical holding the Management of the Radio Spectrum gains Prime Importance. The issue is complicated many times over due to the conflicting interests between Economic, Societal and the National Security Needs. National Security being the paramount factor, Governments world over have significant Radio Spectrum Reserved for its Defence Forces. In UK MoD has the Management Rights to 35% of the Radio Spectrum; in USA National Telecom Information Administration Office of Spectrum Management (NTIA) manages 32% of the spectrum as Federal Band.

2.2

In order to meet these large-scale requirements of Defence Services, most of the countries have earmarked separate bands out of the complete spectrum for its Defence needs. In USA, the Radio Spectrum is Classified as Government Exclusive (Federal use), Non-Government Exclusive and Government/ Non-Government Shared bands; and in UK it is classified as Military use, Civil use and shared Military/ Civil Use. In Indian Context, for the first time an exclusive Defence Band has been jointly worked out between MoD and MoC &IT. While the Defence Band is awaiting the right of Defence Spectrum Managers to Administer the Defence band, the agencies competing over the share of spectrum have intensified their efforts to stake their claim on Spectrum. The advent of LTE and now 5G has put additional demand on EM Spectrum. With only commercial and revenue generating objective in view TRAI, an independent regulatory body, is making its recommendations on Spectrum without consulting MoD, the Major Stake Holder of Spectrum (Defence is the major stake holder in all Nations without exception). Though the concept of Defence Band has been promulgated, but the required modification in the mechanism of its administration has not been put in place. No representative of JCES (which is the agency that has expertise in Spectrum Administration with in MoD) was never consulted when NTP 2012 or even the NFAP 2012. In true sense, concept of Defence Band has not been put into effect in India as yet and in India it being a new concept there may be a lack of clear understanding in the minds of many decision-making bodies.

A committee, headed by Shri Ashok Chawla, was constituted to look into the National Natural Resources Management, which includes Radio Spectrum. This Committee was tasked to look into the Natural Resources allocated/ allotted by GoI; suggest measures to optimise such utilisation; suggest changes in legal system and suggest measurers for promoting transparency. It should be appreciated that the allocation of spectrum is as important as its assignment. The National Security interests and requirements must be addressed at the initial stage of allocation itself. The pull and pressure of organised Cellular bodies and operators cannot colour the vision of the GoI.

2.3

At the outset it must be mentioned that the fault lines are not existing in WPC, TRAI, MOC &IT alone. They are constantly blamed by Armed Forces and MoD for the not honouring
their commitment spelt out in MOU between MOC&IT and MOD on Network For Spectrum (NFS) or Project KRANTI. Armed Forces too have forged ahead and are resisting coordination of Cellular Band Spectrum amongst them. Delay in implementation of NFS, which incidentally was to be completed by 2013, has sowed the seeds of mistrust within Armed Forces. The unilateral decisions on spectrum, without co-opting Defence the major user of EM Spectrum while formulating NTP or NFAP is only complicating the issue. **Immediate corrective measures are required to streamline the Administration of Spectrum by major all Stake Holders.**

2.4

USA is the leader in the concept of Auctioning of the spectrum and in working out the spectrum dividends. They first auctioned their spectrum in 1994, based upon an auction model designed by McAfee, an authority on Industrial Organisation. USA also has a well-defined organisation and process/ laws in place to manage and utilise the Radio Spectrum. In this paper, Spectrum Management procedures of USA and UK have been studied and analysed as one of the governing factors.

3. CONCEPT OF SPECTRUM MANAGEMENT IN DEFENCE

3.1

Military transition into **Future Force** is based upon the premise that the information dominance will provide an advantage to the Armed Forces to amass a superior force at the points of decision. In order to achieve this Armed Forces are moving towards transformation into a **Network Enabled Force** capable of engaging into **Network Centric Operations (NCOs)**. The networked force has the ability to interconnect so as to provide seamless sensor to shooter capabilities; situational awareness and effective command and control on the move. Availability of adequate quantity of spectrum becomes the prime governing factor in NCOs. Defence Spectrum Managers must have the resources and the ability to manage and monitor the spectrum for both communications systems and non-communications systems. This includes radars, sensors, weapon systems, weaponised drones and guided missiles to name a few. This must also encompass all dimensions of the battle space including airborne platforms such as satellites, unmanned aerial systems and subterranean systems. **In the Civil as well as military domain 5G, Autonomous Vehicles, Machine to Machine, IoT etc have increased the EM Spectrum demand many folds. To meet these high-speed demands Harmonisation of Spectrum in Extremely High Frequency bands.**

3.2

This has the effect of further reducing the spectrum available for use. As a result, efficient use and control of the available spectrum is critical to national security for both Information Operations (IO) and Combat Operations. **Effective spectrum management is fundamentally essential for all types of operations and should ensure that operations are conducted with minimal unintentional friendly interference (fratricide) and without negative Electromagnetic Environmental Effects (E3).** Lack of concise, pre-planned frequency coordination may have a disastrous effect upon operations. As part of spectrum management in India currently, Defence is incorporated primarily in spectrum management activities that are focused upon Spectrum Authorisation and relatively less emphasis is paid on the other areas like Spectrum Allocation, Formulation of Policies on Spectrum, Identification and earmarking of spectrum for commercial use. **The fact that Defence was not incorporated in formulation of the National Frequency Allocation Plan 2008 and 2G spectrum was released for**
commercial use without coordination with Defence bears testimony to this. The creation of Defence Band and its management by MoD is a major step in addressing the National Security needs. However, considering that this is the first time that Defence has got exclusive Defence Band adequate care and research must be undertaken before the National Policy on Spectrum Management is finalised. Study of the International methods will assist in formulating the best suited procedures/processes for management of Spectrum in Indian context.

4. SPECTRUM MANAGEMENT IN USA

4.1 National Spectrum Management. The Communications Act of 1934, as amended, governs radio spectrum use in the United States of America and its possessions (US&P). The act established duality in spectrum management in the US between the President for federal government stations and the Federal Communications Commission (FCC) under the direction of Congress. The FCC regulates the spectrum use of non-federal operated radio stations, common carriers, and private organizations or individuals. By Executive Order 12016 of 1978, the President delegated his functions under the act to a new organization, created as the National Telecommunications and Information Administration (NTIA), and placed them under the Secretary of Commerce. NTIA administers the spectrum requirements of Federal Users. See Figure 1 for a diagram of the organization’s architecture.

![Fig. 1: USA National Spectrum Management](image-url)

National Telecommunications and Information Administration (NTIA). Through the NTIA, the President controls all frequency resources in the US&P and authorises foreign governments to construct and operate fixed service radio stations at their embassies. Frequencies are assigned to these stations only if it is in the national interest and if foreign governments grant reciprocal privileges to the US. Figure 2 illustrates the organisation of the NTIA.

The salient components of NTIA are as follows:

(a) Office of Spectrum Management (OSM). The OSM formulates and establishes current and long-range spectrum plans and policies that ensure the effective, efficient, and equitable use of the spectrum both nationally and internationally.

(b) Inter-department Radio Advisory Committee (IRAC). IRAC, under the OSM, assists the Assistant Secretary in assigning frequencies to US government radio stations and in developing and executing policies, programs, procedures, and technical criteria pertaining to the allocation, management, and use of the spectrum.

(c) Office of Policy Analysis and Development (OPAD). The OPAD is the domestic policy division of the NTIA. OPAD supports NTIA's role as principal adviser to the Executive Branch and the Secretary of Commerce on telecommunications and information policies. They conduct research and analysis, and prepare policy recommendations. The domestic policy office generates policies that promote innovation, competition, and economic growth for the benefit of American businesses and consumers.

---

All other components listed above perform the functions of technology studies, administration of technology opportunities programmes and enhance US companies capability to compete globally.

4.2 Defence Spectrum Management

Department of Defence (DoD) is one of the major users in the Federal Spectrum. Specific Service (Army, Navy, Air Force and Marines) frequency assignments within the Continental United State (CONUS) are done by NTIA, the requests for which are routed by formations through their respective frequency management offices. For, joint services assignments within the CONUS, applications are routed through Defence Spectrum Office (DSO) to NTIA. Military Communication Electronic Board (MCEB) is the single window for Chairman Joint Chiefs of Staff (CJCS) to resolve inter-services coordination and interference resolution issues. Outside the CONUS, the Combatant Cdrs are the authority for allotment/assignment of spectrum in their respective Area of Responsibility (AORs).

4.3 Military Assignment Group (MAG)

The MAG is established under the cognizance of the NTIA, IRAC Frequency Assignment Subcommittee (FAS) to provide guidance and procedures for the management of the MAG bands, which are of primary concern to the military departments. The MAG consists of one primary and one alternate member from the Army, Navy, Air Force and the Federal Aviation Administration (FAA). The functions of MAG include:-

(a) The MAG is responsible for determining whether or not applications for frequency assignments in the MAG bands should be approved by the NTIA. The MAG shall provide spectrum-related guidance for the services in these bands including the development, review, and recommendations to appropriate allotment plans. The MAG shall recommend and provide guidance and procedures to ensure the effective and efficient operation and management of spectrum-dependent devices that access the MAG bands.

(b) Be cognizant of the operational requirements of all stakeholders in the bands, especially the unique military tactical and training requirements.

(c) Manage assignments as they relate to the allotment plan for the MAG bands.

(d) Coordinate spectrum policy guidance involving the MAG bands with the members of the applicable NTIA subcommittees and ad hoc groups.

(e) Provide minutes of all MAG meetings to the FAS Chair, Secretary and representatives. In order to facilitate coordination and access to the MAG bands, and to minimize interference among electronic systems, the FAS and the MAG shall observe established coordination procedures.

4.4 A detailed study of the USA spectrum allocation chart (available at http://www.ntia.doc.gov/osmhome/alochrt.PDF) reveals following:-

(a) USA has concept of shared band, other than Federal and non-Federal bands. The shared band is available for use to both commercial and Government agencies.

(b) In addition to the Federal band and shared band, the USA Defence forces when undertake operations in NATO nations, they have NATO band also available at their disposal.

(c) USA has moved its Defence applications in the higher bands.
4.5

There are various acts in place in USA for safeguarding, relocations and groups to manage Spectrum. Some of the important acts are enumerated below:-

(a) Relocation of Federal Government Radio Systems in accordance with Commercial Spectrum Enhancements Act 2004. This act gives detailed procedure for auction of spectrum held by federal agencies as also relocations cost / estimates and timelines.

(b) The Communication Act of 1934, as amended from time to time gives details of the organisational structure as well as various groups / committees which will manage spectrum as a National resource.

5. DEFENCE BAND IN UK

5.1

The regulator Ofcom (The Office of Communications, is the independent telecommunications regulator and competent authority for communication industries in UK) manages civil radio spectrum in the UK and grants spectrum licences, giving users the right to operate over a set locality at a selected range of frequencies. UK has also divided its spectrum requirements in three categories viz, Military band, non-Military band and shared band. The 2003 Communications Act formed Ofcom from 5 existing regulatory bodies. Its responsibilities were to negotiate and adhere to international agreements, ensure the spectrum is used in the interests of citizens and consumers, and employ market mechanisms, where appropriate, to secure optimal use of spectrum resources.

5.2

The UK Frequency Allocation Table covers the radio spectrum from 9 kHz to 275 GHz. It is published by Ofcom on behalf of the National Frequency Planning Group, a sub-committee of the Cabinet Official Committee on UK Spectrum Strategy. The table identifies responsibilities for the management of frequency bands or services showing whether they are managed by Ofcom, the Ministry of Defence, or another Government department or Agency. It also includes The International Telecommunication Union Table of Frequency Allocations contained in the current Radio Regulations. Public sector bodies (such as the Ministry of Defence and the Civil Aviation Authority) manage spectrum for defence, aviation, shipping, science and public safety. Spectrum assignment often follows strict international standards.

5.3

The Defence Band in UK is managed by Ministry of Defence (MoD). MoD being crown agency in UK is exempted from licensing. However, coordination is required with other users. This coordination for Defence operations within the UK territory is done with the help of OFCOM.

5.4

A detailed study of the UK spectrum allocation table (available on internet at http://www.ofcom.org.uk/radiocomms/isu/ukfat reveals following:-

(a) UK has concept of shared band, other than Military and non-Military bands. The shared band is available to both commercial and Government agencies.

(b) In addition to the Military band and shared band, the UK Defence forces, when undertake operations in NATO nations, they have NATO band also available at their disposal.
(c) UK has also moved its Defence applications in the higher bands.

6. SPECTRUM MANAGEMENT IN INDIA

6.1
WPC under MoC & IT is the nodal agency in India for frequency assignment and spectrum management. Indian Telegraph Act empowers WPC to issue all wireless licenses in India. WPC is also responsible for formulating all the policy on efficient spectrum management. All wireless users in India including Defence Services and Govt departments apply for frequency assignments to WPC. National Frequency Allocation Plan (NFAP) is published by WPC from time to time taking in views of all stakeholders. However, it has been felt that Defence Services views as major stake holder of spectrum are not being incorporated in the NFAP documents. Unlike USA, the Spectrum administration for Defence and Non-Defence users is done by one agency WPC – which more often than not has day to day commercial usage pressures colouring their decisions. In this Organisational structure “Conflict of Interest” is unavoidable.

6.2
No Exclusive Defence Band exists in India. In NFAP-81, some of the sub bands were earmarked were in Defence was the major user; however after NTP-99, the subsequent NFAP has been made service specific and no exclusive band such as Defence Band exists. In Dec 1998, a Report of Spectrum Management Committee recommended re-farming of spectrum and creation of Defence Band and Defence Interest Zone (DIZ). Subsequently in May 2009, a MoU was signed between MoD and MoC & IT wherein promulgation of Defence Band and DIZ was agreed to. A Defence Band and DIZ has been mutually identified between MoD and MoC & IT by end 2010, however formal notification and promulgation was done only in 2015 with conditional Foot Notes. Now that Defence Band and DIZ have been promulgated, there would be requirement of firstly, reorganising National Spectrum Administration and secondly, evolving a comprehensive “Standard Operating Procedure on Defence Band Management”.

6.3
Analysis of spectrum Management in India. In India, the importance of spectrum management and its efficient utilization as a scarce natural resource was identified as early as in late 90s. Accordingly, some procedure and methodology in terms of NTP and NFAP have been devised. These Organisations and Procedures continue to be as if DB is non-existent. In various meetings the stand of WPC has been that there would be a need to firstly, make amendments to the Indian Wireless Act 1939 which stipulates that Wireless Advisor has been delegated the powers to Administer National Spectrum, Further delegation would require changes by an act of Parliament; and secondly, The rules of Business do not assign the task of Spectrum Administration to MoD.

7. ORGANISATIONAL STRUCTURE WCP

7.1
The author has been heading JCES during the busy times of carving out Defence Band, Defence Interest Zone and the Inter-Ministerial Group-2 (IMG) meetings to finalise the revised scope of NFS. IMG-2 was necessitated due to the grossly inaccurate projection of NFS cost by BSNL in IMG of 2009. There seemed to be a total lack of clarity in Spectrum Administration back then. Spectrum was being administered by the old SOPs. These SOPs were time consuming and ineffective to meet the very high rate of
applications for spectrum assignment and Standing Advisory Committee of Frequency Allocation (SACFA) clearance. The procedure was unduly delaying the roll out of Mobile Cellular Infrastructure. Delays in return of investments in Spectrum Price by cellular operators was detrimental to Mobile turn over. Changes were made in SACFA Clearances through automation. The No Objection Certificate (NOC) from Local Military Authority (LMAs) could never be obtained in the stipulated window of raising observation/responding. In most cases, NOC was deemed to have been granted by LMAs. Instances of preventing erection of cellular towers by LMAs, even after SACFA clearance was given increased. The mismatch between National Spectrum Custodian and Defence Spectrum Coordinator needs to be suitably addressed on an urgent basis. The eco-system required by LTE or 5G will worsen the situation.

7.2 WPC. The function organisation of WPC is:

(a) WPC is divided into major sections such as Licensing and Regulation (LR), New Technology Group (NTG) and Standing Advisory Committee for Frequency Allocation (SACFA) which makes recommendations on major frequency allocation issues and formulation of the frequency allocation plan, among other functions. The department is responsible for issuing amateur radio licenses, allotting the frequency spectrum and monitoring the frequency spectrum. The WPC is headquartered in New Delhi and has regional branches in Mumbai, Chennai, Kolkata and Guwahati.

(b) Wireless Monitoring Organisation (WMO)\(^\text{10}\), set up in 1952, is responsible for monitoring all wireless transmissions and is essentially the eyes and ears of WPC. Its primary task is to monitor the entire radio frequency spectrum with a view to provide the requisite technical data logistic support to the WPC Wing in the enforcement of the National and International Radio Regulatory and statutory provisions for efficient management of Radio Frequency Spectrum and Geo-Stationary Orbit. This is in the interest of vital national service which, though not revenue bearing, yields considerable indirect benefits through promoting the efficient utilisation of the radio frequency spectrum and the geostationary orbit.

Its headquarters is located at Pushpa Bhawan, New Delhi. Under it, there are 28 Wireless Monitoring Stations (WMSs) (including five International Monitoring Stations, IMSs) and 1 International Satellite Monitoring Earth Station (ISMES), Jalna, Maharashtra strategically located all over the country. These monitoring stations carry out monitoring in MF, HF, VHF, UHF, SHF.

7.3 Joint Communication Electronic Staff (JCES). JCES is an organisation that was set up, in 1949 primarily to manage Radio Frequency Spectrum for Defence use. The current role of JCES covers Electronic Warfare (Joint Electronic Warfare Board – JEWB), Joint Electronics and Communications and EMI/EMC (JEMCAB). Defence continues to be the major as well as nationally important user of spectrum. Therefore, JCES continues to be the lead agency in Spectrum Coordination, Director JCES normally chairs these meetings. The SACFA clearance for Defence is also routed through JCES. JCES is also an important member in various Working Groups of World Radio Conferences – ITU. To perform all the Spectrum related roles JCES has one Joint Director each for Spectrum and

\(^\text{10}\)Wikipedia
SACFA. JCES has no resources or capabilities for Wireless Monitoring against encroachment or misuse / interfering source locating. *With the promulgation of Defence Band MoD urgently needs to acquire the capability of Wireless Monitoring Organisation - WMO for Defence Band.*

8. COMMITTEE ALLOCATION OF NATURAL RESOURCE REPORT – AN OVERVIEW

8.1
Though the CANR Report has not been notified by GoI, de facto its recommendations are being followed. Hence, it is important to elucidate the highlights of CANR’s recommendations.

8.2
A *Spectrum Act* is being formulated for efficient use of spectrum. The Committee expressed its concern in the delay in implementing NFS as per the timelines agreed to by all parties in the MoU of 22 May 2009. The delay is leading to delays in vacation of frequencies in commercial bands that are occupied by Defence. The recommendations are:

(a) The Committee recommends that all future telecom licences should be unified licences and spectrum should be de-linked from the licences.

(b) The Committee suggests that vacation and re-farming of spectrum for commercial services should be expedited to ensure availability and certainty of adequate spectrum to facilitate optimal usage and revenue realization.

(c) In future, spectrum for telecom access services should be made available through suitable market related processes.

(d) In the context of space services, there is a need for the DoT and DoS to review the present rates for spectrum charges and transponder charges.

(e) The Committee thinks effective measures should be taken to ensure continued efficient usage of spectrum by providing appropriate incentives/disincentives for efficient/inefficient usage including stipulation of rollout obligation, disincentives for lower usage levels, consideration of appropriate geographical unit for allocation and measuring usage and a rigorous oversight mechanism including audit, etc.

(f) The Committee sees the need for more liberal mergers and acquisitions (M&A) guidelines keeping a minimum number of service providers to ensure competition. Spectrum sharing should be permitted and suitable conditions should be laid down in this regard in consultation with TRAI. The issue of spectrum trading should also be looked into at an appropriate stage.

(g) In the opinion of the Committee, the promulgation of Defence Band and Defence Interest Zone (DIZ) needs to be expedited.

(h) The Committee sees the need for a comprehensive and integrated legislative framework for spectrum management to be put in place to ensure optimal and efficient use of country’s spectrum resources.

8.3
Deductions from CANR. The salient recommendations that relevant to the scope of this paper are:

(a) A comprehensive and integrated Legislative framework is to be put in place for optimal and efficient use
of spectrum. While formulating the legislation rep of MoD, ideally JCES must be incorporated (Defence is the single largest Spectrum User, any dilution will impact National Security).

(b) MoD needs to set up its own WMO to administer its Defence Band.

(c) Since a fresh Spectrum Legislation is being in acted – MoD must become the Licensee and Administrator of Spectrum within Defence Band and Rules of Business notified accordingly (this would be in lines with the Spectrum Administration in USA and most of other countries). To avoid a conflict between commercial and non-commercial requirement of spectrum WPC cannot be Spectrum administrator of Defence Band.

(d) MoD must be represented in the process of Formulation of NTP and NFAP. In addition TRAI, should not be the regulating agency for Defence Band.

(e) Spectrum is a premium resource and is scarce. MoD must also formulate procedures to ensure that there is no idle Spectrum in commercial band only during peace time. While doing so, it must be assured that the transition from Peace Time to War is not delayed due to vacation by commercial users. The concept of shared band, within Defence Band, needs to be considered.

9. SUGGESTED ORGANISATION OF DEFENCE BAND ADMINISTRATOR

9.1 The current system in India has the major drawbacks in terms of independence in Spectrum Management; Economic Development and Commercial needs often are give more priority by WPC, MoC &IT than the security needs, insufficient legislations / laws and Standard Operating Procedures for Spectrum Management, its allocation, assignment and audit. To meet the strategic, economic and social needs of our country a best practice model for Indian scenario needs to be evolved.

9.2 Spectrum usage has become a daily life necessity because daily use electronics/ appliances like mobile, wireless hot spots, microwave links etc need EM Spectrum. All these appliances have direct impact on the society. Optimum cost has to be arrived at, that balances the revenue generated for the government to meet its societal responsibilities, cost burden on common citizens, operating and capital cost on the Telecom sector etc. If one prices it to low, not only is the revenue generated for the government adversely effected but even the operating cost is impacted in the long run. Spectrum charges are no longer to compensate only the organisational cost of Spectrum Administrator Department. Unfortunately, DOT till 2008 was satisfied with recovering the Spectrum Administration organisational cost or for that matter to meet the urgent requirement of the government to minimise deficit financing. In many countries like USA, UK and other the base auction price is arrived at based upon a study carried out by an independent risk analysis expert agency. For example, in 1994 USA arrived at the base price for auction of spectrum based upon the recommendations of study carried out by MacAfee. India too needs to arrive at the base auction price through an independent risk analyst expert group. To safeguard the interest of Defence, to advise the government on the National Security perspective linked to spectrum usage by defence; formulation of NTP and NFAP and to
9.3
The necessity of Defence Band administration is indisputable. By whom is more important. For better transparency and effective administration of EM Spectrum, more teeth needs to be given to the National Spectrum Administrators. Wireless Advisor reporting to Member Telecom in MOC&IT very clearly elucidates the importance that is given to this administrative body. The administration body needs to be independent and be directly placed under Cabinet Secretariat (akin to the case in USA, UK and other countries). The model that was adequate to handle user-based spectrum administration (allocation) till early 90s is not adequate to administer Services based Frequency Allocation. If these changes are not made then, the probability of reoccurrence of the instances of misadministration of spectrum experienced in 2008 is very high. MOC&IT, which has the responsibility of only ICT will not have the correct prospective of spectrum utilisation by other agencies like Defence, Atomic Energy and other Strategic agencies.

9.4
Defence Band can only be managed in an unbiased manner, without conflict of interest, when the Apex Body is not directly involved in commercial or security related utilisation of spectrum. Defence Band must therefore be administered by an agency answerable to MoD. All aspects of Harmonisation to allocation, assignment, vacation and re-farming with in Defence Band must be done by a restructured JCES. The erstwhile Radio Monitoring Organisation, MoD needs to be restructured to perform the role of Defence Band WMO. A new section needs to be created that looks at
representation of India on National Security at ITU-R and WRC. There is also a great need to incorporate Armed Forces representatives in formulation of ITU Standards. In case of 5G, which has tremendous potential for Indian Army for Tactical Communication System (TCS), Indian Armed Forces went unrepresented in various Study Groups on 5G as well as IMT 2020. 5G Standards formulated are devoid of the security of location of the 5G entities. This itself will be a limiting factor in exploitation of 5G as FWS-TCS (Field Wireless system). If 5G is used, major changes will be required in the 5G stacks.

9.5

The suggested model of Figure 3 above can only be enabled by an Act of Parliament. Under the provisions of ITU-R, National Security is given topmost importance in Harmonisation of Spectrum. Even the ITU-R standards are governed primarily by National Security. There is therefore a need to first build capability within Armed Forces in formulation of ITU-R and ITU-D standards. After developing this capability, the next step is for focused representation of these personnel in various Working Groups both Regional (ITU) as well as Global (WRC).

10. RECOMMENDATIONS

10.1

Considering the need to efficiently administer the Non-Defence and Defence Bands judiciously there is a need to fine-tune the WPC. The recommendations are: -

(a) The Indian Defence Band that has been worked out jointly between MoD and MoC & IT, is in line with the international practice and the same needs to Administered as per the best practices worldwide.

(b) Defence Band and the Non-Defence Band should be separately managed but jointly coordinated by an independent agency under the Cabinet Secretariat. The Defence Band should be managed by an agency under MoD.

(c) There should be a coordination mechanism put in place to coordinate the spectrum usage for Defence and commercial use. The coordination should be done by an independent agency under PMO, with appropriate representation from major stakeholders.

(d) Defence WMO under MoD needs to be established to monitor use of Defence Band. This WMO will ensure efficient utilisation of Spectrum by Armed Forces and Central Security Agencies as well as will protect Defence Band against encroachment.

(e) Armed Forces need to play a more active role in WRC as well as in formulation of ITU-R Standards through Study Groups.

(f) A suitable administrative mechanism, viz, a Spectrum Planning Subcommittee, under an appropriate Secretariat may be formulated to look into the management & allocation of spectrum in non-Defence Band and apportionment of spectrum space between or among the government and non-government activities in India.

(g) A Committee needs to be formed by PMO, with a task to reorganise Spectrum Administration in India. Based upon the committee report, process of amendments to various Acts should be initiated.

(h) There is a need to adopt the concept of Shared Band, akin to USA, at least in the TMT Bands.
11. CONCLUSION

11.1

Spectrum requirements of different Defence services differ and cannot be generalized, as the requirements are peculiar for each nation. However, Defence Forces should ensure that the spectrum is used efficiently, as it is a scarce natural resource and is also required by other agencies. ITU-R constitution provisions for a Nation’s freedom in use of spectrum for their Military Installations vide Article 36 and 48. Accordingly, the countries have constituted their Spectrum Management Organisations and processes. Both USA and UK (the models studied) have an independent spectrum regulatory body at the apex level of President and Crown respectively. The spectrum for Defence and Federal use is managed and controlled by Defence / Federal organisations.

REFERENCES

1.  www.fcc.gov
2.  www.ntia.doc.gov/osmhome/allochrt.PDF
3.  www.ntia.doc.gov
5.  www.ofcom.org.uk/radiocomms/isu/ukfat/ukfat08.pdf
6.  Committee on Allocation of Natural Resources (Chapter 7).
Cyber and Electronic Warfare: Technology Enablers and Challenges

Maj Akhilesh Singh

Abstract—The EW-cyber environment is now so fundamental to military operations and so critical to our national interests that we must start treating it as a war fighting domain. The convergence of these two capabilities provides for Cyberspace Electromagnetic Activities, which are activities leveraged to seize, retain, and exploit an advantage over adversaries in both Cyberspace and the electromagnetic operational environment, while simultaneously protecting the mission command system and denying and degrading our enemies' use of the same. Convergence creates opportunities for Cyber and EW to overlap; however, convergence also creates potential for training, resourcing, and employment changes to dilute skills currently inherent in the EW and Cyber workforce as well as resources.

1. INTRODUCTION

1.1
Modern warfare calls for simultaneous and seamless application of all elements of warfare and synergising the capabilities and resources of the three Services. All five domains – land, air, sea, space and cyber space – are to be employed with maximum effect. New and emerging technologies and techniques like artificial intelligence, machine learning, network centric warfare tools and other elements must be exploited to use force cohesively and in an orchestrated manner: Joint planning and application, joint training, joint doctrines and compatibility in equipment and communications are a prerequisite.

1.2
In the future era of “CDS and Jointness”, integrated Commands will be the imperative need for a single headquarters coordinating diverse elements in the same geographic space. The present arrangement – with 17 geographically separated single Service Command Headquarters and two integrated ones-is clearly a recipe for operational ineffectiveness. Theatrisation of commands will involve the creation of joint HQ with common intelligence, communication, surveillance and air defence systems. To be successful in a technology driven battlefield, non–contact warfare, using means that would often be non-kinetic, synergetic integration of the armed forces is required, which is lacking.

1.3
The proliferation of modern electronically controlled, directed, and commanded weapons has caused a rapid expansion in the field of science that is generally called ‘Electronic Warfare’ (EW). The basic concept of EW is to exploit the enemy's electromagnetic emissions in all parts of the electromagnetic spectrum (EMS) in order to provide intelligence on the enemy's order of battle, intentions, and capabilities. A generally accepted military principle is that victory in any future war will go to the side that can best control and manage the EMS. The use of EW and cyber as a force multiplier is a well-established and Commanders at all levels understand the overall capabilities of this potent force multiplier and employ it as an integral part of their overall
plans. However, due to the changing façade of the digital battlefields of today, there is a need to look beyond the brute force capabilities exerted by the existing systems. Increasingly, there is an understanding emerging of the commonality in Cyberspace, EW, Spectrum Management and the close coordination required between the three. The blending of telecommunications and computer networks, referred to as ‘Convergence’ has resulted in the previously distinct domains of EW and Cyber, merging to become one and the same. This convergence becomes much more relevant in the Tactical Battle Area (TBA) where the entry point for both is the EMS. Looking at the world over, the Chinese have integrated the two through their Integrated Electronic Warfare (INEW) campaign. The US has coordinated and integrated Cyber, EW and EMS Operations through Cyber Electromagnetic Activities (CEMA). As Cyberspace and EW Operations develop similar and complementary capabilities, it is imperative to plan, integrate, and synchronize these with military operations especially in joint operations.

2. SCOPE

2.1
The scope of this service paper is to suggest a model for exploiting the cyber and EW (CEW) in enabling jointness, whereby the military can exploit ibid core elements of Info Warfare with this integrated capability.

3. CYBER AND ELECTRONIC WARFARE (CEW)

3.1
CEW is any military action involving the use of spectrum to control the domain characterized by the use of electronics and the EMS to store, modify, and/or exchange data via networked systems and associated physical infrastructures. A classic example can be, sending a digital signal stream through a network to instruct a controller to shut off the power flow, while sending a high voltage surge through the electrical power cable to short out the power supply is considered EW. However, a digital stream of computer code or a pulse of electromagnetic power or a combination of both can be used to create false images in adversary computers, which is essentially Cyber EW. Cyber EW consists of the following three activities: Cyber Electronic Attack (Cyber EA), Cyber Electronic Protection (Cyber EP), and Cyber Electronic Support (Cyber ES). These three activities are defined as follows:-

4. CYBER ELECTRONIC ATTACK (CYBER EA)

4.1
Use of electromagnetic energy to attack an adversary’s electronics and/or access to the electromagnetic spectrum with the intent of degrading, neutralizing, or destroying an enemy’s ability to store, modify, and/or exchange data via networked systems and associated physical infrastructures.

5. CYBER ELECTRONIC PROTECTION (CYBER EP)

5.1
The passive and/or active means taken to protect electronics and/or access to the EMS from any effects of friendly or enemy employment of Cyber EW that degrades, neutralizes, or destroys ability to store, modify, and/or exchange data via networked systems and associated physical infrastructures.
6. CYBER ELECTRONIC SUPPORT (CYBER ES)

6.1
Any action to search for, intercept, identify, locate, or localize sources of intentional and unintentional radiated electromagnetic energy radiating from electronics used to store, modify, and/or exchange data via networked systems for the purpose of immediate threat recognition, planning, and/or conduct of future operations.

7. CHALLENGES

7.1
As the services provide most of India’s EW assets, a basic understanding of each service’s perspective would greatly facilitate the planning and coordination of EW at the joint level. Doctrinal support for joint operations need to be examined to highlight the training aspects as also the institutional support to be in place for an effective impact at all levels of operations to include strategic, operational and tactical keeping in mind the scope of joint operations in the Indian context. The future battlefield therefore is the software applications, hardware electronic components and the wireless networks. This is the target of CEW, which can be defined as the conduct of CW on an adversary using the techniques of EW for ingress or incapacitation. Some of the challenges in the jointness are as listed below.

(a) Planning, coordinating and integrating CEW for joint operations.
(b) Doctrinal guidance for joint CEW.
(c) Issues of interoperability.
(d) Maintenance of data bases.
(e) CEW in joint exercises.
(f) Development/procurement of equipment.
(g) Management challenges.
(h) Language specialists/translators and interpreters.
(i) CEW support to national strategic assets.

8. CYBER EW IN AN OPERATIONAL ENVIRONMENT

8.1
An operational environment is a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bearing on the decisions of the commander. An analysis of an operational environment must consider the five domains and the EMS. The four traditional domains (air, land, maritime, and space) and the EMS exist naturally. The fifth domain, cyberspace, is man-made. Cyberspace and the EMS provide commanders the ability to share information, communicate, integrate, and synchronize operations across all war fighting functions and echelons. Conversely, cyberspace and the EMS provide adversaries and enemies an effective, inexpensive, and anonymous means for recruitment, information activities, training, and command and control. Cyber EW provides commanders with the ability to gain and maintain an advantage in cyberspace and the EMS.

9. FEW EXAMPLES OF LATEST TECHNOLOGY

9.1
Few examples of latest technology being followed and developed to conduct future operations are:-

10. COUNTER ELECTRONICS HIGH POWERED MICROWAVE ADVANCED MISSILE PROJECT

10.1
In 2012, Boeing released footage of its weapon, the Counter Electronics High Powered Microwave Advanced Missile Project (CHAMP),
cruise missile with an electromagnetic war head disabling a bank of desktop computers. It merges EW and cyber warfare by conducting ‘protocol-based attacks,’ where you actually get into the system and displace ones and zeroes to break that communication chain between the trigger and the (radio-controlled) IED receiving those ones and zeroes.

11. **DIGITAL RADIO FREQUENCY MEMORY (DRFM)**

11.1 Digital Radio Frequency Memory (DRFM) is the latest technology; one can create false targets or hide real targets using the enemy’s own wave forms against him. DRFM jammers employ a computer-based ‘library’ of known threats that are used to identify and neutralize incoming signals. DRFM equipment may also include an Electronic-Intelligence (ELINT) capability which monitors and collects information on enemy signals and jammers.

12. **POWER DOWN**

12.1 Electromagnetic weapons could also be used to disable enemy vehicles or in the case of the US Active Denial System (ADS) be used to repel humans.

13. **AIRBORNE PLATFORMS**

13.1 EW equipment is gradually shifting from the ground-based platforms to airborne platforms due to miniaturisation and better electromagnetic interference management, especially
those dealing with Electronic Support functions such as interception and monitoring. Increasingly, EW equipment is now based on aircraft and drones because of its inherent advantages. Airborne systems, though limited by size and power output, have the advantage of range and reach. Jammer pods used in dedicated EW aircraft were generally more capable than those mounted on other kinds of aircraft. Fifth generation aircraft such as the US F-35 are capable of stand-off as well as stand-in jamming using power outputs almost ten times that of legacy fighters including dedicated EW aircraft. Reports indicate that such truly multi-role aircraft operating in high threat AD environment will be more effective than single mission electronic attack legacy aircraft. The pairing of existing UAV platforms with Jammer Pods (like the MQ-9 Reaper with a Northrop Grumman Jammer Pod) brings in an entirely new dimension in which the spectrum battle can be fought in an integrated manner using both ground and aviation assets. The future may see a gradual shift when some of the functions of EW aircraft are taken on by capable, multirole UAV platforms. The EA 18G Growler is the US Navy electromagnetic warfare plane, capable of eavesdropping on and disrupting electrical systems, such as those in guided missiles.

14. STRIKING AT A DISTANCE

14.1

16. Defence firms are also looking to build long range weapons, such as missiles with electromagnetic warheads.
15. JAMMERS

15.1
To the layman, a jammer is synonymous with EW. It is undoubtedly the most visible component of EW. Modern jammers are significantly different from their decade-old cousins. Equipment such as the Krasukha-4 or the Turkish KORAL ground-based jammer can generate very high power output over a broadband of frequencies which can be effective at distances up to 300km; a big jump from the previous generation of jammers which had limited ranges and effectiveness while in broadband jamming mode. Some reports also suggest that equipment such as the Russian communications suppression station Murmansk-BN is capable of jamming about 20 spot frequencies at ranges up to 5,000km. In order to achieve these high ranges, jammers are no longer restricted to the line-of-sight mode and even use reflected signals from the ionosphere. Shoot and scoot capability is available to these high power jammers based on high mobility trucks with built-in generators. Such mobility was feasible earlier in low power stand-alone jammers. Future jammers are likely to be expendable (including air dropped) and mounted on unmanned ground vehicles.

16. DRONE/SWARM COUNTERS

16.1
Drone swarm’s offensive could be blunted through the use of countermeasures like EW techniques, cyber-attacks, laser and microwave weapon systems, small arms fire, camouflage and concealment or pitching a counter drone swarm. In January 2018, Russia confirmed a swarm drone attack on its military base in Syria. Six of these small-size UAVs were reportedly intercepted and taken under control by the Russian EW units. USA is now deploying new radars like Q-53 system that can detect and identify such small objects and then initiate the kill chain using laser weapons.

17. ARTIFICIAL INTELLIGENCE (AI)

17.1
Reacting quickly involves being able to patch systems quickly. Army can’t spend days or weeks on those tasks, but AI can help human analysts do better work and spend time more efficiently rather than having to sit through data. For instance, the application of AI could help reduce the time needed for EW/Cyber systems to reconfigure and change techniques (or tools) to enable and protect friendly forces’ access to spectrum and information systems while denying adversaries access to the same. AI could do this by integrating into EW/Cyber systems and quickening the OODA loop well beyond human capabilities. AI could also enable and enhance dynamic planning and execution, dynamically identify threats, close the gap between technology and operator capabilities, and minimize focus on data analysis to enable a shift to execution.

18. FUTURE EW SYSTEM

18.1
Some of the essentials features required in the future EW sys are as listed below.

(a) Fielding of Integrated Non-Communications EW systems for the Indian Army.
(b) Dedicated EW systems for LICO in both Northern and North-Eastern sectors.
(c) Elevated EW platforms for enhanced range and area coverage.
(d) Track based EW platforms to support fast moving and highly mobile mechanized forces.
(e) Development of Directed Energy (DE) weapons system to damage or destroy adversary equipment, facilities and personnel by a beam of concentrated EM energy or atomic or subatomic particles. Possible applications include lasers, radio frequency weapons and particle beam weapons.

(f) Satellite Communications and Cellular Communications monitoring systems at the field level.

(g) Acquisitions of systems to take on enhanced frequency coverage, use of ‘frequency hopping’ ‘communication equipment’s, induction of ‘Software Defined Radio’ sets and growing sophistication of anti-jam propagation techniques.

(h) Qualitative technological improvement of Direction Finding (DF) sub-systems to achieve greater accuracy and flexibility in its deployment.

19. BREACHING THE ELECTRONIC – CYBER – OPTICAL GAP

19.1

The term ‘spectrum warfare’ is being used to denote the blending of electronic and optical warfare, while Cyber-EW systems are simultaneously emerging in mainstream military space. Spectrum warfare seeks to combine EW technologies such as electronic jammers, interception, radars, electronic spoofing and deception along with electro-optical technologies such as infrared sensors, multi-spectral and hyper spectral sensors, visible-light sensors and laser technologies. The convergence of Cyber and Electronic Warfare is a natural progression. While EW is the coarser and close-in tool, Cyber Warfare is more targeted and specifically focused on chosen computer systems, networks and applications.

The US Army has updated its field manual and released FM 3-12 on “Cyber and Electronic Warfare Operations” in April 2017. The EW systems of the future will have Cyber Offence and Defence capability and will operate at the cutting edge of the TBA, a distinct shift from the strategic level at which cyber operations are focused presently. Such equipment will have the capability to carry out cyber malware injection off the air into the networks of the adversary including air gapped and off-line systems.

20. CEW SUPPORT TO SPACE BASED OPERATIONS

20.1

Space is inexorably becoming the new high ground and Star Wars are no longer in the realm of science fiction. Physical destruction, laser blinding and cyber and EW are all likely to be employed to deny the enemy the use of satellites and to safeguard the use of one’s own satellites for their force multiplier value. India is on the threshold of entering a new era in space exploitation. There is a need to deliberate on how best the space assets could be integrated into our military operations. The Defence Space Vision --2020 which outlines the road map for the Armed forces in the realm of space includes intelligence, reconnaissance, surveillance and navigation as the thrust areas in its first phase (2007-2012). The ability to restrict or deny freedom of access to and operations in space is no longer limited to global military powers. Knowledge of space systems and the means to counter them is increasingly available on the international market. Nations if they wish can possess or acquire the means to disrupt or destroy an adversary’s space systems by attacking the satellites in space, their communication nodes on the ground and in space, or ground nodes that command the satellites. The reality is that there are many extant capabilities, such as
Anti-Satellite Weapons, Denial and Deception measures, Jamming, use of micro satellites, hacking and nuclear detonation that can deny, disrupt or physically destroy space systems and the ground facilities that use and control them. More and sophisticated technologies for jamming satellite signals are becoming available. For example, it is learnt that Russia is marketing a handheld GPS jamming system. A one watt version of such a system, the size of a cigarette pack is able to deny access to GPS out to 80km; a slightly larger version can deny access up to 192 km. Both are compact and powerful enough to jam an aircraft’s GPS receiver signal, which could disrupt military missions or create havoc at an airport. Such indicators of the potency of EW need to be taken cognizance of and appropriate defensive steps initiated.

21. DIRECTED ENERGY WEAPONS (DEWS)

21.1 Development of DEW has been in progress since the 1940s with the development of the German experimental weapons. Successes achieved in the laboratory and the test ranges have not seen commensurate translation into the battlefield. Use of DEW in the RF spectrum which can disrupt communication links, navigation links and telemetry links and against small, mobile platforms like UAVs, is indicative of the things to come. The development of Radio Frequency (RF) disrupters as protection against drones has tremendous potential. It also signifies the use of the spectrum to achieve kinetic effects, a significant shift from traditional EW philosophy.

22. SOFTWARE DEFINED RADIO (SDR) BASED EW

22.1 SDRs have transformed the way radios are used in the battlefield. These sets are agile and the same platform provides the ability to use different frequency bands, modulation schemes, FH Rates, FH Bands, power output, gain and other parameters. Due to their versatility, these sets can switch over to the EW role while free from communication role. Now that SDR is a reality and increasingly the traditional radio inventory of armies across the world is being changed to SDR, many short range and discrete EW functions are likely to be taken over by such sets in the TBA. The SDR sets are also likely to be deployed closer to the enemy forces than traditional EW equipment, thus enhancing the effectiveness to interfere with the enemy links.

23. CONVERGENCE OF COMINT AND ELINT

23.1 Information value from intercepted communication is reducing due to communication systems switching to better FH schemes, use of non-standard protocols, encryption and other ECCM techniques. Staging areas near the international boundaries are now extensively connected using optical fibre and other non-radiating media. Hence the previously practiced methods of picking up enemy Order of Battle from radio transmissions made during mobilisation and preparations at the staging areas will not yield any dividends. ELINT, on the other hand, depended on picking up signatures of enemy radars and other transmitters and compare the same to existing libraries in order to evolve a larger intelligence
picture. Gradually, we can see a perceptible shift in the way modern EW systems are looking at COMINT in the same way as ELINT. Advanced receivers can carry out ‘fine grain’ analysis of enemy communication transmitters and radar transmitters and carry out radio finger printing. This can involve receivers based on UAVs, special aircraft, ground-based or satellite-based. This also involves advanced data management capability and automation.

24. BIG DATA IN THE MILITARY DECISION MAKING PROCESS

24.1 Effective command and control in war demands that the commanders have access to timely, relevant and accurate information continuously. The primary staff products are information and analysis and can be visualized as data sets characterized by their ‘variety’ of type (structured & unstructured data), ‘volume’ (terabytes to petabytes) & ‘velocity’ of change (speed of analysis & presentation). In order to reach correct situational awareness results, we must analyze correct data coming from correct source and produce information from raw data. This will enable commanders to take swift and better decisions thereby reducing the OODA loop. A few sectors where Big Data can find its place in the Indian Army are listed below:-

(a) Operational Planning.
(b) Counter Insurgency Operations.
(c) Big Data War gaming.
(d) Cyber Warfare.
(e) Disaster Management.
(f) Manpower Management.
(g) Logistics Management.
(h) Cognitive Analytics.

25. CONCLUSION

25.1 The future tactical battlefield will be replete with wireless networks providing the media for battlefield management systems in the informationalised combat environment. The logic of a more integrated approach to cyber and electronic warfare is not just functional or operational – it is also financial, and would lead to rationalisation and budgetary optimisation in defence procurements. The EM-cyber environment is now so fundamental to military operations and so critical to our national interests that we must start treating it as a war fighting domain on par with-or perhaps even more important than-land, sea, air, and space. The increasing convergence of electronic, cyber and optical domains will require a perceptible shift in war fighting techniques. In this paper, the author has combined the existing methodologies of CW and EW, and propagated the converged concept of Cyber Electronic Warfare (CEW). It is imperative that the same specialists be now trained on both these techniques so that this domain of future wars can be fully exploited and commanders are presented with a battle winning option, both for offensive and defensive operations.

REFERENCES

Tri Services Training in Joint Environment

Col Deven Makhija
E-mail: dmakhija.485p@gov.in

Abstract— Human resource development in armed forces is a continuous process for the development of skills of personnel and entire organization. Training in joint environment has its own challenges due to varied ethos and silos of services. Joint services institutes and framework for joint training needs to be promulgated based on national security strategy and operational directives. Joint training requirements, planning, execution, validation and assessment needs to be modeled. This paper has proposed a model and framework for joint training along with few envisaged fields for participation by academia and industry to enhance the skills of tri services for joint operations.

The nature of warfare has changed over years and is ever evolving. Jointness in operations in present era has evolved and is an important prerequisite for success. Jointness has to be based on operational philosophy and mandated strategic and operational directives based on national security. Jointness of Army, Air Force and Navy is about effective, efficient and optimal utilisation of resources that dictate various requirements in terms of optimisation of force structures, acquisition processes, training methodologies, and research and development on strategic capabilities. Four major aspects for jointness thus incorporates operational, organisational (or structural), training, and doctrinal shift.

Training is an important facet as command and control, planning, coordination and operational execution at all levels is assured by well rehearsed and trained personnel. Training is achieved by imparting instructions and applied exercises for acquiring and retaining knowledge, skills, abilities, and attitudes necessary to complete specific tasks. Joint training is training, including drills of individuals, units, and staffs using joint doctrine and tactics, techniques, and procedures to prepare joint forces or joint staffs to respond to strategic, operational, or tactical requirements.

1. INTRODUCTION

1.1

Joint environment strategy emphasizes that all future wars need to be conducted in such a manner that the Land, Air and Naval Commanders jointly formulate, orchestrate and implement war plans. It mandates unified command and control structure and push for a tri-service approach for modernisation of the armed forces. Human resource development to ensure requisite skill set, abilities, attitude, knowledge and experience is imparted to personnel of tri services for conduct of operations is an essential component for jointness. To achieve jointness, it is essential that personnel from the three services serve and train together in organisations across the military, strategic, operational and tactical levels. Joint training will thus be the bedrock for all future endeavors and an essential prerequisite for jointness. In order to fight together the tri services must develop structure and framework to support joint training and operations.

2. STAGES OF JOINT TRAINING

2.1

The Services have evolved in silos and have different ethos and infrastructure for training. Thus training in joint environment needs deliberate planning, development of infrastructure and models. The important stages of training envisaged in joint environment are as depicted at Figure 1 below.
2.2 Individual Training. This incorporates structures like academic, education, pre commissioning and regimental centre training. Education focuses on the instruction of personnel to enhance their capacity to perform specific functions and tasks; education imparts general aspects of knowledge and develops mind for application to a wide spectrum of endeavors. Education is largely defined through the cognitive domain and fosters diverse perspectives, abstract reasoning, critical analysis of ambiguity and uncertainty and innovative thinking, particularly with respect to complex, nonlinear problems. Elements of education and training are most often blended in application to achieve desired learning objectives, ultimate results and outcomes. Virtually all training institutes and courses include elements of both education and training in their academic curriculum. Education and training thus, are partners in the generation and sustainment of an individual’s abilities to perform. Individual training in joint environment will ensure development of ethos, camaraderie, spirit de corps and cohesive bond for rest of career in Services. Thus, in joint environment it is imperative to ensure availability of joint institutes and infrastructure at all stages of training.
2.3 Self-development. Empowering individuals with responsibility to actively participate in their own professional growth is a necessary and positive step. Self-study in pursuit of knowledge accelerates individual development, and allows flexibility and accommodation to individual needs and desires.

2.4 Service Specific Professional Training. It empowers the personnel on service specific, technical, staff and leadership roles. In joint environment cross training in these fields is encouraged to understand the intricacies of each field and enhance the cognitive horizon on limitations and capabilities of each.

2.5 Joint Training. Joint war fighting is not academic; it is the application of the acquired knowledge, ability, aptitude and skills in an operational environment where increased levels of experience correspond directly with increased levels of proficiency and performance of theatre, operational or domain specific tasks. To maximize joint readiness, joint professional training is essential for all personnel preparing for assignment on a joint staff, including officers in professional specialties and diplomacy. Joint training institutes assume competent service educated, trained, and experienced individuals as the training audience. Joint performance reflects the successful application of what individuals learn via joint assignments, joint education and training, joint exercises and self-development and is essentially based on theatre and operational directives.

3. JOINT LEARNING PROTRACTION MODEL

3.1 The Joint Learning Protraction (Figure 2) is a proposed model for coordinated progression of integrated, structured and unstructured learning processes and events to prepare tri service personnel to specified joint performance standards. This protraction of professional learning instills habits of mind, skills, abilities, attitudes and values through education, training, self-development, and experience. The learning model ensures human resource development by continued training cycles. It focuses on creating and sustaining joint qualified personnel and joint leaders capable of effectively integrating and synchronizing national capabilities to successfully implement national security and military strategies.
3.2
The integration of individual preparation and collective preparation through learning cycle ensures effective integration of education, training, self-development, and experience to achieve preparedness for joint tasks and operations.

3.3
The systematic approach to professional development throughout the career as embodied in the model is important to ensure availability of trained human resources for joint tasks. Trainers, commanders and mentors can use varied state of art techniques, resources, technologies and training aids to facilitate achieving specific learning objectives. Improvements in joint preparation and readiness are achieved through the integrated application of those elements, systems, and processes. Commanders at each successive level must exploit the training aids and determine how best to efficiently reach pinnacles of experience and performance. Model ensures monitoring, managing, and integrating individual, and collective joint preparation by commanders, and training institutions to improve joint operational capability and achieving joint readiness.

![Joint Training Framework](image)

**Fig. 3: Joint Training Framework**
3.4 Joint Training Framework. The joint training framework (Figure 3) supports implementation of the Joint Learning Protraction by providing a methodology to plan and implement a comprehensive training program. It supports all aspects of human resource development for personnel to include elements of training, education, self-development and experience. Training requirements are based on felt need, operational requirements and strategy. The training directive is formulated at apex level based on joint capability development road map consistent with command priorities, required capabilities, and available resources and formulates joint training calendar. Training plan facilitates the adoption of an integrated, operational capability requirements-based method for aligning individual and collective joint training programs with assigned operational roles. Framework provides methodology for assessment and validation of training and operations at all levels and the incorporation of lessons learned, emerging technologies, shift in concepts and doctrine across the organisations.

4. ROLE OF ACADEMIA AND INDUSTRY

4.1 Joint Training Structures. Joint training institutes need to be earmarked or raised ab initio to attain greater training and operational synergy amongst the three services. Few specialized training institutes could straightaway be centralized amongst the three services to avoid duplicity of effort and resources, such as training of law, intelligence, musician, catering, provost, space, cyber, and logistics. Expertise with academia and industry in fields of intelligence, space, cyber, nuclear, chemical and biological training needs to be exploited to upgrade the Joint Training Structures.

4.2 Tri Service Communication Infrastructure. The existing training structures need to have communication interface for integration in addition to joint training structures. Joint communications are pre requisite for joint operations and is the start point for Joint Training Structures. Few suggested measures wherein industry can facilitate networks and communications for joint training are establishment of Common Web, Tri Service One Network, Common Standards and Protocols, Joint Encryption systems, Common GIS, Common Data Sharing Platforms, Standard Policies and Procedures for communications, development of plug and play model for communication at the theatre level and tri services Command, Control, Communications, Computers, Intelligence and Reconnaissance (C4ISR) by data sharing. Holography, video conferencing studio, seamless networks and integration of communication facilities of training institutes can be facilitated by industry.

4.3 Electronic Training. Self development of personnel is an important facet in joint training protracted model and framework. Academia and industry has varied expertise and platforms to support self development through certificate courses, e Learning and Online Courses. Study Webs of Active Learning for Young Aspiring Minds (SWAYAM) platform for hosting Massive Open Online Courses (MOOCs) has been fielded by Government of India duly developed by Information Technology industry. Similar exclusive platforms with security overlay for e Learning and online courses for joint training of armed forces personnel may be proposed by academia and industry.
4.4

Academics, Research and Development. Specialisation courses in niche domains like aviations, cyber, space, project management, leadership, national security and national strategy can be subscribed by tri services directly based on memorandum of understanding with reputed academic institutes and online learning firms. Annual Management Study Board for brain storming seminars on niche technology and Armed Forces Technology Board can be explored for problem statements and its solution. Development of new projects and research and development on varied fields can kick start based on Technology Board recommendations.

4.5

E Library. The integration of training and structures for joint training mandates requirement of integrated database of research, publications, articles, experiences, lessons learnt, books and precis. Digitisation of existing library infrastructure and fielding an integrated environment for library, e books, journals and training material with security overlay is feasible with latest tools and platforms.

4.6

Simulation and Wargames. Training aids like simulators and computerised wargames are effective and ensure optimum utilization of resources. It saves on wear and tear of operational equipments and is economical. Joint live, virtual, augmented reality and constructive training capabilities, war games, table-top exercises, assessment, and training ranges are recommended to be developed to conduct or support joint training. Joint training hubs incorporating simulators and wargames may be deployed for faster, efficient and economical joint training.

Fig. 4: Role of Academia and Industry
4.7

**Automation.** Information Technology software giants have plethora of opportunities and can play pivotal role in automation and development of tools related to joint training. Some applications envisaged are Virtual Labs, Web based Knowledge Sharing, Training Validation, Evaluation of Training Effectiveness, Course Report Generation, Cadre Management etc. Used cases for same can be built based on expertise available with Tri Services and solutions on problem statements can be proposed by industry.

5. **CONCLUSION**

5.1

Government of India has announced implementation of long standing recommendations of various committees on post of Chief of Defence Staff (CDS). Jointness amongst the three services has to be top driven and once the intent is clear the organization would systematically embrace the spirit of jointness. The integrated headquarters with CDS is likely to take firm decisions on jointness. Aspects like Integrated Theatres and joint capability development are on forefront. Joint training command or theatre in place of services training commands may be brainstormed in addition to expeditious institutionalisation of Indian National Defence University (INDU). The forces have to adapt to changing scenarios, doctrine and strategy; thus joint training protracted model with associated training framework needs to be implemented in coordination with active participation of academia and industry. Joint training needs to be given due impetus so that trained and capable human resources are made available battle ready for joint operations.

**REFERENCES**

2. The Defence Training Model, Australian defence force publication 7.0.2, 14 July 2006.
3. Open source information https://www.bharatshakti.in; assessed on 17 Sep 2019.
Computational and Correlational Data Analytics for Increased Military Effectiveness

Brig A Shridhar

Abstract—The future battlefield would be increasingly complex with emerging and enabling technologies, sophisticated systems, flexible communications and enhanced computing power being pushed to the forward edge of the battle field. Military commanders have always lived and died by information, both for quantity and quality. Hence, while these systems would enhance the Intelligence, Surveillance and Reconnaissance (ISR) capability resulting in increased battlefield awareness and battlefield transparency paving way to network centric and nonlinear operations, they would also exponentially increase the amount of information and data generated. Increasingly high momentum and speed of operations due to complex emerging and enabling technologies being pushed into the battlefield would result in shorter and shorter decision cycles or the ‘OODA Loop’. The military concept of decision making places information flow at the heart of all activities from operations to logistics. With information so central to all activities, the military is naturally hungry for technology or tools that improve processing of information or data.

1. INTRODUCTION

1.1 Emerging technologies bring with it organizational and security challenges that present both opportunities and obstacles. The importance of data in modern warfare poses three distinct challenges for a commander, firstly handling the sheer volume of data produced, secondly integrating numerous types of data into one coherent battlespace picture and finally handling the time pressure in military decision making due to shortening of the decision cycles and increasing volumes of data.

1.2 Technologies for storing, quickly retrieving and getting out meaningful analytics and desirable outcomes from large volumes of diverse and disparate data need to be identified and mastered. Data analytics would go a long way in adding value, by identifying hidden patterns, correlations and also attempt reasonable predictions of future activities with veracity from this voluminous, variety of high velocity data being generated.

1.3 As technological options multiply, the difficulty in choosing the right, the best and the most efficient technology also multiplies. Almost all militaries worldwide are faced with the much publicized ‘Guns Versus Butter’ macroeconomic debate. This aspect particularly gains greater importance in a developing country like India. It would not be worthwhile to experiment with technologies only to dump them later. Each technology will have to be carefully studied, weighed and compared to extract the best bang for the buck. Computational data analytics supported with increased computing power would significantly add value and substance to the seat of pants approach in military decision making.
2. DATA ANALYTICS

2.1
Future battlefield will rely on a virtual net of sensors and communication systems for battlefield awareness and transparency. Hence, demands for accurate, timely and actionable information is the need at every level, right from an infantry patrol to the highest level of planners at the planning desk to make well-informed decisions. Proliferation of sensors churning out voluminous data is overwhelming at present for any meaningful analysis due to lack of tools to efficiently process, store, analyze, and retrieve vast amounts of data. Existing automation tools do not aid users in finding complex and adaptable threats within mission critical timelines. Robust networks to accurately detect, identify, geo-register, classify, store, retrieve, search, mine and exploit explicit information from unstructured data is the need of the hour.

2.2
Current defense systems for processing information struggle to effectively scale to the volume and characteristics of changing data environments and the range of applications for any kind of data analysis. Overcoming these challenges requires fundamentally new approach is required to be adopted for data science, including distributed computation and interactive visualization.

2.3
Emerging technologies in data analytics need to provide us with the ability to leverage immensely large, disparate data and analyse the data with the help of enhanced visualization, correlation, cognitive computing and other advanced analytics into creating a refined intelligence output to support a decision or a course of action. The key challenge here is to garner the confidence of commanders on the analysis of data before a decision is made.

2.4
Military data analytics can be broadly classified into three layers as under:-

(a) The Data Management Layer. These technologies are driven by the Information Technology (IT) industry and is fairly mature with multiple options to choose from.

(b) The Data Analytics Layer. These technologies are immature and niche. It is primarily driven by the military, involves huge costs, with suspect outcomes. It is this area where one needs to concentrate on.

(c) The User Interface Layer. These technologies are again driven by the Information Technology (IT) industry and is fairly mature with multiple options to choose from.

2.5
Data Analytics is not only important in the field of military operations, it would yield much more visible results in operational logistics, administration and logistics and can be of other welfare and administrative domains such as suicide prevention, maintenance of weapon platforms, planning of convoys, patrols searches, terrorist strikes etc the list is endless.

2.6
Indigenous Industry Participation. Data analytics does not require imported equipment or technology, our very own Indian firms dealing with data analytics are claiming to provide this kind of intelligence. Infosys cofounder Mr Kris Gopalakrishnan has also invested in an Artificial Intelligence (AI) and Predictive Big Data Analytics Chennai based startup M/s
Crayon Data. Hyderabad based Modak Analytics provided BJP the much needed social analytics during their election campaign in 2014. There are over 200 plus data analytics firms in India, most focusing on increasing sales and profits. Some of the other major players include Mu Sigma, Latent View, Absolut Data, Manthan, Brillio, Gramener, Bridgei2i, Tata iQ, Fractal Analytics, Cartesian Consulting, among others.

2.7 Commercially Available Software. Exploiting commercially available software permitting ‘Try before you buy’ such as IBM i2 Enterprise Insight Analysis, Microsoft Power BI, Google Earth visualization, Predictive Analysis by SAP is a good start point. Later open source architecture with industry participation gradually graduating into niche and proprietary protocols for the nation should be attempted. This architecture should enable rapid integration of existing and future exploitation tools to achieve a new paradigm in the management and analysis of military data.

2.8 It should also be understood that one particular algorithm / architecture would seldom bring in results for the diverse environments the Indian Military is operating. Opting for a single enterprise analytics platform may seem like a logical decision, a way to ensure consistency and cost-effectiveness across all the analytics initiatives. However, an all-encompassing, one-size-fits-all platform is unlikely to succeed due to the sheer diversity of military analytic needs. Moreover, as the military commanders and military analysts get comfortable and proficient in analytics, they would demand advanced features and capabilities.

2.9 In most cases, the analytics platforms developed would evolve from a descriptive ‘what happened’ to a predictive ‘what is likely to happen’ and later to a prescriptive ‘how to increase the chances of desired outcomes’ analytics. Building incrementally as these needs arise is a more logical approach. An incremental approach also leaves open the opportunity to tap into ongoing concurrent innovations worldwide. Technology platforms represent a fast-moving, ever-changing landscape, hence committing to a single track may cost us the opportunity to leverage something newer and better.

2.10 At the same time, the opposite approach of building each component individually and then integrating the components, can be equally frustrating and ineffective, with much of the cost and effort spent on integration of the components. Here, the US DARPA initiative of the XDATA Program is worth emulating which is experimenting with approximately 35 different data infrastructure, data analytics and data visualization tools each.

2.11 It is by now reasonably well understood that effective analytics provide insight into what happened, why it happened, what is likely to happen and also include the factors that could help shape different outcomes. But when it comes to the ‘how’ of analytics – including which technology platform or platforms will be used to support them – there is less clarity as there are fundamental challenges in building analytics capability, including the pros and cons of investing in all-encompassing technology platforms.
3. MILITARY COMPUTATIONAL ANALYTICS

3.1
Exploitation of computational analytics as a solution for military has been bone of contention for high mathematical content involved in modeling and solving for answers. With increased computing power available, computational analytics requiring powerful computing algorithms can now be done at the forward edge of battle field to save on mission critical time and effort. Most military decision situations involve allotting scarce resources to competing alternatives. Selection of strategic targets by enhanced computing algorithms to identify the maximum capacity of an adversary’s road /rail / air/ communication networks, juxtaposed with the minimum effort required to disrupt the maximum flow through these networks would yield rich dividends for which mathematical algorithms exist.

3.2
Analysis of military situations with multiple strategies with multiple probabilities including posterior probabilities of selecting a particular strategy or a course of action can be computed, simulated and mathematically gamed to determine the best course of action including sequential moves over time. Decision support systems with multiple criteria which may be complimentary / contradictory, qualitative / quantitative or tangible/intangible can be computed with advanced computing algorithms. Complex logistical and supply chain when mathematically modelled and solved by exploiting enhanced computing power will result in quantum improvement in efficiency.

3.3
Shortest and the best routes for reconnaissance, visits, campaigns, tours etc. can be easily computed utilizing advanced software. Complex optimization problems such as utilizing minimal scarce resources to achieve maximum effect both in operations and in logistics can be computed. Game Theory and Queueing Models to emulate tactical situations, weapon system analysis, logistics and economics can be formulated and solved. However, more important to the military planner is the fact that the implications of the theory can be brought to bear on more complicated military situations.

3.4
With these algorithms and mathematical models and enhanced computing power in place, the next challenge is ensuring the quality and veracity of the data that enters the analytics engine. The phrase ‘Garbage in, Garbage out’ applies here. If data is of poor quality, the output too will be of poorer quality resulting in military commanders losing faith on analytics.

3.5
Some of the areas where computational analytics has been successfully exploited and implemented to cut costs and improve effectiveness are ARMOR\(^2\) in Los Angeles International Airport, PROTECT\(^3\) for the US coast guard, IRIS\(^4\) for Field Air Marshals and GUARDS\(^5\) in the US Transportation Security. Realizing the vast potential of data analytics in the military an ‘Intelligence Analysis Summit’\(^6\) is being organized at Washington D.C, USA, from 30 Apr to 02 May 2018 by the International Quality and Productivity Center, New York, USA encouraging military participants from round the world to participate.

4. CONCLUSION

4.1
Although data analytics and computational data analytics, have been dealt with differently in
the paper, they are meant to achieve the same, improve military effectiveness by optimizing scarce military resources. We now need to focus our energies towards exploitation of the emerging technologies in the forward edge of the battlefield by effective data analytics both computational and correlational. Enhanced computing power available at the forward edge of battlefields would make this a reality in the near future. A specialized team is recommended to be set up for interacting with available industry and academia so that available Data Analytics strategies can be adopted by the Indian Army for effective exploitation.

REFERENCES

The Role of SDR as an Enabler in Joint Operations

Col Rohit Nandan Prasad

Abstract—Any modern fighting force consists of the fighting elements that deliver combat potential and support and logistical components that sustain the fighting components during operations and in peace. Unless synergized by an agile and responsive nervous system, both these components are ineffective and will not perform their intended role. The backbone of an effective fighting force is an effective Command and Control structure and the spinal cord joining command and control system with the forces is an agile, responsive and robust communication system or network.

In today’s fast paced, multidimensional operations, which necessitate diverse forces to operate in synergy, the role of seamless and failsafe communications assumes greater importance. The biggest impediment to smooth, unimpeded inter force communications so far was the usage of different hardware, secrecy and protocols by each organization. The deployment of Software Defined Radio (SDR) will change this paradigm.

1. INTRODUCTION

1.1

The modern battlefield encompasses multiple domains and dimensions. In earlier wars, conflict was restricted in time and space to the period of hostilities in the battlefield. The scope of conflict too was restricted to the armed operations carried out by soldiers in isolated theaters of operations. In contrast, today’s wars are fought in a space time continuum without break, simultaneously in multiple domains and dimensions. The ingredients for success in the modern battlefield are simultaneity, speed and surprise.

1.2

For a contemporary fighting force to be effective, dominance across the entire spectrum of conflict is of paramount importance. The spectrum of conflict encompasses widely disparate domains such as economic, perception and political over and above the military dimension. For the purpose of this paper, we restrict the analysis to the geographical theater of operations where armed forces are engaged in actual conflict. Even so, there are a number of different forces deployed in any conflict zone today. These can range from the traditionally deployed Army, Navy and Air Force to the Coast Guard, Border Security Forces, Civil Police, CAPFs, Fire Brigade, Medical Staff, Rapid Action Forces, Special Operations Groups, Intelligence Agencies, Home Guards, etc. Operations today demand jointness, not only within the Armed Forces but also with these other forces and organizations.

1.3

The spirit of jointness implies that forces work in synergy towards the common national, political or strategic objective. Synergy in operations assumes more critical proportions today, since even a small action by a soldier or tactical unit has the capability of triggering a chain of events that will potentially change the course of the conflict inexorable by influencing factors in the domains of perception, economic etc.
1.4
Thus, Joint Warfare is a military doctrine which seeks integration of the various service branches of a state's armed forces into one unified ambi-dexterous force. Joint warfare is in essence a form of combined arms warfare on a larger, national scale, in which complementary forces from a state's Army, Navy, Air and Special Forces are meant to work together in joint operations, rather than planning and executing military operations in isolation.

1.5
The biggest deterrent to successful planning and execution of joint operations was the different communication systems hardware, protocols, frequencies, modulation techniques and secrecy algorithms deployed by different forces. Merely replacing these with one common set of equipment and protocols would not have sufficed because each force has a different set of tactics, training, command structures and strategic objectives. What was needed was a communication system that could transform its various technical parameters in response to the situation, tactical grouping and role.

2. THE CONCEPT OF SOFTWARE DEFINED RADIO

2.1
Software Defined Radio (SDR) is a radio communication system where components like mixers, filters, amplifiers, modulators, demodulators and detectors that were traditionally implemented in hardware are instead implemented by means of software on a personal computer or embedded system. While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which were once only theoretically possible.

2.2
A basic SDR system may consist of a personal computer equipped with a sound card, or other analog-to-digital converter, preceded by some form of RF front end. Significant amounts of signal processing are handed over to the general purpose processor, rather than being done in special-purpose hardware (electronic circuits). Such a design produces a radio which can receive and transmit widely different radio protocols (sometimes referred to as waveforms) based solely on the software used.

2.3
As already brought out earlier, successful planning and execution of joint operations was impeded by the different communication systems hardware, protocols, frequencies, modulation techniques and secrecy algorithms deployed by different forces. Induction of SDR will help bridge the divide between forces and transform a platform centric force into a network centric force. The nature of SDR enables it to swiftly deploy different waveforms on the fly in order to communicate with different military entities. Quick changing of waveforms and security algorithms allow the SDR to be used by forces which are swiftly and frequently regrouped and redeployed in different tasks under different commands.

2.4
SDR based systems have significant utility for the military and commercial communication service providers, both of which must serve a wide variety of changing radio protocols in real time.

2.5
In the long term, SDRs are expected by proponents like the SDR Forum to become the dominant technology in radio communications. SDRs, along with software defined antennas are the enablers of the futuristic cognitive radio.
2.6

A software-defined radio can be flexible enough to avoid the “limited spectrum” assumptions of designers of previous kinds of radios, in one or more ways. Spread spectrum and ultra wideband techniques allow several transmitters to transmit in the same place on the same frequency with very little interference, typically combined with one or more error detection and correction techniques to fix all the errors caused by that interference.

Some additional features offered by SDR are as below:-

(a) In SDR, software defined antennas can be designed and deployed to adaptively lock onto a directional signal, so that receivers can better reject interference from other directions, allowing it to detect fainter transmissions.

(b) Cognitive radio technique can also be deployed, wherein each radio measures the spectrum in use and communicates that information to other cooperating radios, so that transmitters can avoid mutual interference by selecting unused frequencies. Alternatively, each radio connects to a geographical location database to obtain information about the spectrum occupancy in its location and, flexibly, adjusts its operating frequency and / or transmit power not to cause interference to other wireless services.

(c) SDR technology permits smart algorithms to be deployed in order to effect dynamic transmitter power adjustment, based on information communicated from the receivers, lowering transmit power to the minimum necessary, reducing the near-far problem and reducing interference to others, and extending battery life in portable equipment.

(d) Wireless mesh network can be engineered using SDR, where every added radio increases total capacity and reduces the power required at any one node. Each node transmits using only enough power needed for the message to hop to the nearest node in that direction, reducing the near-far problem and reducing interference to others. This enables frequency reuse and optimizes spectrum usage.

3. JOINT OPERATIONS AND SDR

3.1

In the realm of Joint Operations, the term Battlespace is more relevant than battlefield. Battlespace is a term used to signify a unified military strategy to integrate and combine armed forces for the military theater of operations including air, sea, land, cyber, space and information domains to achieve military goals. It includes the environment, factors, and conditions that must be understood to successfully apply combat power, protect the force, or complete the mission.

3.2

This understanding of joint operations in the battlespace includes both enemy and friendly armed forces, infrastructure, weather, terrain, and the electromagnetic spectrum within the operational areas and other areas of interest. Thus, over the last few decades, the understanding of the military operational environment has transformed from primarily a time and space driven linear understanding (a “battlefield”) to a multi-dimensional system of systems understanding (a battlespace).

3.3

This system of systems understanding implies that managing battlespace has become more
complex, primarily because of the increased importance of the cognitive domain, a direct result of the information age. Today, militaries are expected to understand the effects of their actions on the operational environment as a whole, and not just in the military domain of their operational environment.

3.4
Battlespace agility refers to the speed at which the war fighting organization develops and transforms knowledge into actions for desired effects in the battlespace. This essentially implies that must be better than the adversary at doing the right actions at the right time and place. Inbuilt into this understanding is that battlespace agility is not just about speed, but it is also about executing the most effective action (ways) in the most efficient manner (means) relative to achieving the desired impact on the system (ends).

3.5
At all times, battlespace agility is dependent on the quality of situational awareness and a holistic understanding of the battlespace to determine the best actions. This logic that has become the driving force behind a renaissance of interest in the quality of military communications. Effective military communications are heavily linked to the ability of intelligence analysts and operational planners to understand their battlespace, and their targets, as networks in order to facilitate a faster, and more accurate shared situational understanding. This in turn increases targeting efficacy and helps retain the overall initiative. Battlespace agility as a concept has its roots in the more generic Command & Control (C2) agility concept, but works specifically with an agility concept within the context of warfighting only. Hence it is framed by effects based thinking, system of systems analysis, and competing Observation Orient Decide Act (OODA) loops.

3.6
As brought out earlier, battlespace agility is enabled and catalyzed by SDR which enables tactical units to be swiftly regrouped and integrated into the command and control communications structure by loading the appropriate waveform and secrecy algorithm. SDR also facilitate the freer flow of information in all dimensions as brought out earlier.

4. BATTLESPACE AWARENESS

4.1
Battlespace awareness is a practice of military philosophy that is used as a valuable asset by joint component and force commanders, to predict courses of action before employing troops into a prescribed area of operation. It utilizes the intelligence preparation asset to assist the commander in being ‘aware’ of recent, current, and near term events in his battlespace.

4.2
Battlespace awareness is based around knowledge and understanding obtained by the Intelligence, Surveillance, and Reconnaissance (ISR) system. It is another methodical concept used to gain information about the operational area—the environment, factors, and conditions, including the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain—that enables timely, relevant, comprehensive and accurate assessments. It has become an effective concept for conventional and unconventional operations in successfully projecting, or protecting, a military force, and/or completing its mission.
4.3
The SDR is an enabler of Battlespace Awareness. Each soldier carrying the SDR becomes an information gathering node and a surveillance outpost. It is not necessary for the soldier to be aware of this aspect of his mission. The use of applications embedded within the SDR will enable automatic gathering, processing and collation of data at every level. The inherent computing capability of the SDR enables computation to be done in situ; thus enabling fail safe and distributed node computing.

5. BATTLESPACE DIGITIZATION

5.1
Battlespace digitization is designed to improve military operational effectiveness by integrating weapons platforms, sensor networks, Ubiquitous Command and Control (UC2), intelligence, and network-centric warfare. This military doctrine reflects that in the future, military operations will be merged into joint operations rather than take place in separate battlespaces under the domain of individual armed services.

5.2
Intelligence Preparation of the Battlespace (IPB) is an analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive database for each potential area in which a unit may be required to operate.

5.3
The database is then analyzed in detail to determine the impact of the enemy, environment and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process.

5.4
Network-centric warfare, also called network-centric operations or net-centric warfare, is a military doctrine or theory of war pioneered by the United States Department of Defense in the 1990s.

5.5
It seeks to translate an information advantage, enabled in part by information technology, into a competitive advantage through the robust computer networking of well informed geographically dispersed forces.

5.6
The ideas of networking sensors, commanders, and shooters to flatten the hierarchy, reduce the operational pause, enhance precision, and increase speed of command were captured in this document.

5.7
Modern information technology permits the rapid and effective sharing of information to such a degree that “edge entities” or those that are essentially conducting military missions themselves, should be able to “pull” information from ubiquitous repositories, rather than having centralised agencies attempt to anticipate their information needs and “push” it to them.

5.8
The doctrine of network-centric warfare for the United States armed forces draws its highest level of guidance from the concept of “team warfare”, meaning the integration and synchronization of all appropriate capabilities across the various services, ranging from Army to Air Force to Coast Guard. This is part of the principle of joint warfare.
5.9

The tenets of network-centric warfare are as under:-

(a) Tenet 1: A robustly networked force improves information sharing.

(b) Tenet 2: Information sharing and collaboration enhance the quality of information and shared situational awareness.

(c) Tenet 3: Shared situational awareness enables self-synchronization.

(d) Tenet 4: These, in turn, dramatically increase mission effectiveness.

6. CONCLUSION

6.1

Thus SDR can be seen as the major technology that enables a force to transition from being platform ready to network ready. Other than facilitating the tactical soldier or unit to communicate and deploy applications with value added services, SDR also permits the rapid and effective sharing of information to such a degree that "edge entities" or those that are essentially conducting military missions themselves, are able to collect information, process it and push it to central repositories where it is available for other entities across the spectrum to pull and utilize. This is the single largest factor that singles out SDR as the game changer for modern forces in contemporary warfare.
Threatscape Segmentation: Network Invigilation for Realizing Vulnerable Assets using Neural Analytics (NIRVANA) to Mitigate Zero Day Attacks

Lt Col Vivek Bardia, Lt Col Gaurav Upadhyay, Lt Col Raja Vijit, Lt Col Akshay Sati and Lt Col Yogesh Sati

Abstract—This research paper highlights how technologies like Big Data, AI&ML can be used to enhance the Cyber Security Posture by detecting and mitigating Zero Day Attacks orchestrated by motivated state actors, such as foreign governments and issue-based organizations using asymmetric warfare thereby improving our national cyber security posture. The increasingly digital nature of our everyday work and personal lives have driven a demand for ubiquitous and frictionless access to data and networks thereby, making cyber-attacks an increasingly attractive option because our valuable data & the number of devices connected online is increasing by the day, providing countless new windows into our networks & lives. The concept caches upon User Collaboration, Data Visualization and Analytics for faster detection, segmentation and mitigation of threats and vulnerabilities in networks and systems aided by humans to perform faster outlier detection reducing the Window of Vulnerability which is the key for mitigating zero day attacks as even the latest AV, IDS, IPS & UTM do not guarantee mitigation of Zero Day Attacks as they rely largely on signature & behaviour based methods to identify malicious code before the malicious code can cause harm to computer systems. However, signature & behaviour based mechanisms are in effective against zero-day exploits since the signature of zero-day malware is, by definition, unknown as the malware has not previously been identified as such.

1Artificial Intelligence (AI) is decision making. Machine Learning (ML) allows system to learn new things from data. It leads to develop a system to mimic human to response behaviour in a different circumstance.
2A zero-day vulnerability is an undisclosed computer-software vulnerability that is unknown to the vendor which hackers can exploit to adversely affect computer programs, data, additional computers or a network. It is known as a “zero-day” because it is not publicly reported or announced before becoming active. This security hole is then exploited by attackers before the vendor becomes aware and hurried to fix it—this exploit is called a zero-day attack.
3Asymmetric Warfare is war between belligerents whose relative military power differs significantly, or whose strategy or tactics differ significantly. This is typically a war between a standing, professional army and an insurgency or resistance movement militias who often have status of unlawful combatants.
4The time from when a software exploit first becomes active to the time when the number of vulnerable systems shrinks to insignificance, is known as the Window of Vulnerability (WoV).
1. INTRODUCTION

1.1
With technology at our fingertips waiting to be exploited, the past decade saw the revolutionizing Human Computer Interactions (HCI). The ease with which a user could interact was the Unique Selling Proposition (USP) of every sales team. HCI have many underlying parameters like Data Visualization and Presentation as some to deal with. With the race, on for better and faster presentations, evolved many frameworks to be widely used by all software developers. As the need grew for user friendly applications, more and more software professionals were lured into the front-end sophistication domain. Application frameworks have evolved to such an extent that with just a few clicks and feeding values as per requirements we are able to produce a commercially usable application in a few minutes. These frameworks generate quantum lines of codes in minutes which leaves a contrail of bugs to be discovered in the future. We have also succumbed to the benchmarking in Software Quality Metrics and have made ourselves comfortable with buggy software’s to be rectified in future.

1.2
A study of the various Threat Detection, Protection and Mitigation Systems revealed a common similarity wherein either users have been totally ignored or the systems rely heavily on the user inputs for its correct functioning.

1.3
Compiling the above study, NIRVANA was conceptualized wherein a Security Behaviour Observatory (SBO) was established to store processed user data & computer behaviour over years in addition to the latest threat feeds from Threat Intelligence Platforms to identify and mitigate the risks. The study also focused on the presentation of the same in the easiest and the fastest manner to the NSoC & the end users with minimal time delay. We gave an opportunity to the end user to understand the complete flow of data packets in and out of his system & other process activities being carried out by attaching meaningful information to packets, sessions & processes. This study led us to attest that collection of a wide array of data on user & computer behaviour over time & involvement of users in real time exponentially enhances machine learning and segments the threat canvas faster for a more reliable output.

1.4
A layered approach implementation encompassing the End Users & using Analytics at the Apex Level NSoC tries to solve the Zero Day detection & mitigation problem. This method empowers the fence-sitter users with tools to actively participate in protecting themselves from threats. The alerts by users & their system raise a priority flag at the NSoC and draw the attention of highly trained professionals to address the same.

---

6Human–computer interaction (HCI) researches the design and use of computer technology, focused on the interfaces between people and computers. Researchers in the field of HCI observe the ways in which humans interact with computers and design technologies that let humans interact with computers in novel ways.

7Data Visualization is the graphic representation of data. It involves producing images that communicate relationships among the represented data to viewers of the images. This communication is achieved through the use of a systematic mapping between graphic marks and data values in the creation of the visualization.

8NIRVANA: Network Invigilation for Realizing Vulnerable Assets using Neural Analytics.

9Network & Security Operations Center (NSoC) is a centralized unit that deals with security issues on an organizational and technical level. A NSoC within a building or facility is a central location from where staff supervises the sites beyond the confinement of the four walls.
2. **NIRVANA FOR MILITARY NETWORKS**

2.1

Military networks are by design hierarchical and have always striven for an optimised jointness in operations. This templated hierarchy also has homogeneity in operations. For example, the role of a dispatcher of a Brigade Headquarters would be similar to the role of all dispatchers in all Brigades of the Army. Similarly, the role of an Exchange Operator in a Battalion Headquarter would be similar to Exchange Operators across all Battalions of the Army. This hierarchy at times hampers the synergy due to operational/functional requirements.

2.2

Lateral sharing takes priority over hierarchal sharing for critical operation tasks like sharing information on a new threat/zero-day attack and mitigation measures for the same to contain the threat and minimize the damage in the network. The officials manning systems& sub-systems in all three services generally face similar kind of threats and are at same level of technical competence. The task and capability of a data clearance official in Army will be similar to that of the official in Navy or Air Force. This similarity translates to a similar set of actions by the service personnel (end users in this case) upon encountering any unusual behaviour in the system, unrecognised occurrences/events.

2.3

NIRVANA frame-work derives its power from User Collaboration to segment the threat scape; the greater number of users – more reliable is the output derived. NIRVANA proposes to integrate NSOCs of the various Military Networks; NSoC (Army), NSoC (Navy), NSoC (Air Force), NSoC (SFC) etc. laterally allowing organization to maintain autonomy over their own NSOCs. The NIRVANA framework is highly scalable and can further integrate with non-Military critical infrastructure networks like that of the Power Grid Corporation of India, Railways, Nuclear Plants, etc. can also be plugged-IN and contribute as well as derive benefits of the yet larger threat scape.

2.4

The results thereof, both interim as well as final, are designed to be shared among all the feeder networks’ (NSoC). Thus, any threat/vulnerability detected in any part of the network will be disseminated in real-time through autonomous NSoCs, thereby presenting a Threat Intelligence Platform for joint evaluation of threats to Military Networks in a de-centralised yet synergised manner. This integration will not only enhance the jointness of the Military Networks, but will draw its power from the jointness of the users manning the sub-systems of the network.
3. NIRVANA BUILDING BLOCKS

3.1
The NIRVANA platform is composed by several building blocks. As illustrated in Figure 1, NIRVANA allows to collect data from different data sources. These data sources, also referred as data feeds are divided into external data and internal data.

3.2
The resulting data is enriched, i.e. it is complemented with geo location, WHOIS, DNS and reverse DNS lookups, hashing, autonomous systems name and number, DKIM and SPF records and file and URL analysis data. This data is important to get context around the threat event under analysis.

3.3
All of this data is then analysed and stored on different database systems (e.g. Malware DB, Social Media Database, Email Database, Phishing Database). These databases contain historic data useful to perform both real-time and historical analysis. The analysis process is supported by a big data analysis engine like Hadoop using a map-reduce model. This engine is used to perform search, count, aggregation, correlation and regression analysis operations.

3.4
The communication between users and the platform is made via well-established frameworks from the open source community to make it a fully qualified modular solution. The real-time alerts generated provides insightful visualization and analysis over the data.

3.5
Combining real-time with historic analysis; allows organizations to: gain situational awareness; discover organizations requirement to remediation services; understand the indicators of compromise, methods of infection, pinpoint the internal root cause for the problem and follow the remediation steps.
4. SECURITY BEHAVIOUR OBSERVATORY (SBO) AT NSOC

4.1

Security Behaviour Observatory (SBO) would be the heart of the decision-making process. Neural Network algorithms auto-tune as per the severity and criticality of the user/infrastructure set. The historical data is saved and every work done by users across the organization is logged and sent to this Observatory. This is a client-server infrastructure designed to collect a wide array of data on user and computer behaviour from a panel of hundreds of participants over several years. The SBO infrastructure is designed to fulfill several requirements.

(a) First, the SBO scales with the desired length, breadth, and depth of data collection.

(b) Second, extraordinary care is taken to ensure the security and privacy of the collected data, which will inevitably include intimate details about our participants’ behaviour.

(c) Third, the SBO is adaptable to our interests, which will inevitably change over the course of time, as when the collected data is analysed & interpreted it may suggest further lines of inquiry & other data collection points.

4.2

Our understanding of computer and user behaviour, with respect to security and privacy, has largely been based on studies of short duration and narrow focus. The SBO caters for the following:

(a) File system: Track changes to the file system, including the added, modified, or deleted file’s size, last date modified, permissions and other related information.

(b) Installed software and operating system updates: maintains a list of installed applications, version numbers, and other related data, to determine what privacy or security software (e.g., antivirus, firewall, ad blockers, anonymizers) are installed, and whether they are up to date. The SBO also tracks which (and how soon after their release) operating system updates and patches have been installed. This allows us to measure the duration and severity of client machines’ vulnerability to security threats.

(c) Processes: Monitors which processes (e.g., programs, applications) are running on clients’ machines. It captures when all processes start and terminate, and can provide additional process status information at regular intervals. Primarily, this data will assist with the detection of malware. The SBO also collects general computer usage statistics that may help prioritize future security and privacy work, such as towards frequently-used applications.

(d) Security-related events: SBO also notes general security-related events, such as account-related events (e.g., logins, settings changes, password changes), registry modifications, wireless network authentications, firewall changes, and potential attacks detected by the operating system. This will provide valuable insights on multiple usable security topics, including the security measures users employ on their computers, potentially dangerous program behaviour, and the types and frequency of attacks that occur on machines.
(e) Network traffic: SBO captures all network packet headers sent and received to client's computers. This data would allow us to detect various network traffic types that may be risky (e.g., peer-to-peer file transfers, dangerous websites) or suspicious (e.g., malware, intrusion attacks). We could thereby verify whether risky Internet behaviour is correlated with a higher probability of an attack or infection.

5. NIRVANA: USER AID & COLLABORATION

5.1
One of the central tasks in scientific computing is to accurately approximate unknown target functions. This is typically done with the help of data — samples of the unknown functions. In statistics this falls into the realm of regression and machine learning. In mathematics, it is the central theme of approximation theory. The emergence of Big Data presents both opportunities and challenges. On one hand, big data introduces more information about the unknowns and, in principle, allows us to create more accurate models. On the other hand, data storage and processing become highly challenging. Moreover, data often contain certain corruption errors, in addition to the standard noisy errors. Yet another challenge is to present numerical algorithms that address two issues:

(a) how to automatically eliminate corruption/biased errors in data; and
(b) how to create accurate approximation models in very high dimensional spaces using stream/live data, without the need to store the entire data set.

5.2
We tried to address both the challenges by incorporating users at the correct intersections as human heads have a supercomputer, tuned by evolution over hundreds of millions of years, and superbly adapted to understand the visual world. Users over two decades of exposure in some way or other to technology have become seasoned to understand the basics of threat and are proactive to protect themselves in the manner which they understand as best. This human evolution has raised our basic understanding benchmark for technology and threats which would be used to identify Zero Day Threats and surpass the intelligence of machines that learn.

5.3
Users can play a vital role in identifying threats. It is not necessary for the user to be highly qualified for the role of threat identification and mitigation for his surroundings. Users behaviour is known to him best and he can find out outliers in his pattern faster than a machine which learns and uses a far bigger and complicated canvas to produce acceptable results in the same time frame. End users aid to segment an unknown threat canvas would pave the way for segmenting the threat canvas and deploying the available resources in the most vulnerable place for further investigation; hence shortening the WoV.
5.4

Users in this study were presented with an interactive dashboard with a world map to visualize near real-time sessions on their computers with the power given to mark these sessions as suspicious or as clean. It also had an interactive task manager to visualize the systems functioning encompassing the services, system logs and other SIEM\textsuperscript{10} data. Maximum possible metadata was added to processes running before being fed to a visualization report maker by giving users realizable names and probable reasons for their running in the system by using lexical, syntax analyzers, log parsers, filtering and cleansing techniques. Users aided with this interactive dashboard outperformed the latest AV, IDS, IPS and UTM systems as the users had an eye to identify outliers with their basic understanding.

\textsuperscript{10}SIEM: Security Information and Event Management (SIEM) is an approach to security management that combines SIM (Security Information Management) and SEM (Security Event Management) functions into one Security Management System.
User data was collected over time was incrementally returned back to them from SBO as Systems Opinion with metadata added, enrichment done, deduplication algorithms run, clustering and uniformization performed to get a final output for storage and retrieval of the same. Subsequently, data from other users were also amalgamated and displayed to all other subjects during the period aiding their decision making to give a feel of collaborative learning.

Humans knew exactly what they were doing on their systems and were extra cautious while scrutinizing actions and had even flagged rudimentary cache files, cookies, automatically downloaded updates as suspicious. They had an eye to identify outliers with their basic understanding.

6. COMPILATION OF CONFUSION MATRICES FOR ZERO DAY ATTACKS

6.1 Network Awareness: Users were quick to identify the outliers and mark them as suspicious in almost all cases and further being extra cautious about their own privacy and security they went further marking a whopping 15 % False Positives too, as shown in Table.

6.2 Process Awareness: Users were quick to identify the outliers and mark them as suspicious in almost all cases and further being extra cautious about their own privacy and security they went further marking a whopping 25 % False Positives too, as shown in Table.
6.3
The above methods when used in conjunction with the latest AV, IDS, IPS and UTM systems would facilitate the growth of the sensor canvas by involving users exponentially to provide the cutting-edge solution for mitigating zero-day attacks which is the biggest problems in today’s cyber threat canvas. The help from end users would act as catalysts and contribute to the Security Professionals, Experts and Analysts work and by segmenting the abysmal data and focus their attention to mitigate threats.

7. CONCLUSION

7.1
The value of storing volumes of data depends on our ability to extract useful reports, spot interesting events and trends, support decisions and policy based on statistical analysis and inference, and exploit the data to achieve business, operational, or scientific goals. There will always be a shortage of Security Professionals, Experts and Analysts as we inch forward into this Digital Era.

7.2
Large databases of digital information are ubiquitous. Current hardware and database technology allow efficient and inexpensive reliable data storage and access. The vast diversity, velocity and veracity of data presents unique challenges to implementing efficient and reliable mechanisms to present colossal data which is generated in a manner easy to understand and comprehend reducing the decision-making time.

7.3
Maintaining integrity on a computer is extremely challenging, when it comes to the highly sophisticated zero-day attacks wherein we are left with little help from the environment of latest and most advanced AV for protecting our end user systems. As the study primarily focused on Zero Day Attacks which look the most innocent programs and services in a computer, a little help from the end user can do the trick of segmenting the vast threat canvas.

7.4
To the best of our knowledge we have commercial Antivirus systems which totally neglect continuous interactions with end users in the gambit of ease of use in real time and update their datasets accordingly.

7.5
This work focused more on the presentation of data along-with analysis carried out by ML & AI superimposed in the Security Behaviour Observatory in the easiest and the fastest manner to the end user with minimal time delay. Further to say, we did not interrupt any services of the system to let the user have no degraded performance issues while being a subject in the test.

8. FUTURE SCOPE

8.1
We further propose a Configuration Management framework which integrates seamlessly with other security needs and facilitates regular, recurring scans. We also propose to implement Vulnerability Management which is concerned with understanding the security posture of an organization with respect to known vulnerabilities. It involves collecting information regarding vulnerabilities and patch levels of assets across the enterprise. The information is regularly fed into aggregate reporting, and may also be used to do targeted or large-scale remediation of discovered vulnerabilities.
SATCOM—Last Mile Secure Connectivity to Difficult Terrains of Tactical Battle Area

MR Sujimol, Anita Panday and K Shahana
Delhi Earth Station, SNGG/SAC, ISRO, New Delhi-110021, India
E-mail: sujimol@sac.isro.gov.in

Abstract—Satellite Communication usage has become predominant throughout the country for various applications in terms of coverage and outreach. Tactical Communication technology provides secure communications such as voice, data and video among mobile/static users to facilitate command and control within, and in support of tactical forces keeping in view of the changing tactical situations and varying environmental conditions. The last mile connectivity in the Tactical Battle Area (TBA) provides highly reliable connectivity, as it is meant to empower the soldier who is at the cutting-edge of our forces. ISRO provides last mile connectivity in difficult terrain of TBA by launching communication satellites for mobile services. The high power, high gain satellite of ISRO provides four different types of service viz, reporting service, two-way voice service, two-way multimedia service and broadcast service in the S-band spectrum for strategic purpose. ISRO has also launched a satellite for South Asian Countries to provide portable Ku x Ku VSAT network in that region for better communication, weather forecasting, tele-medicine and response to disaster management. The Portable Satellite Terminal, VSAT is capable to link with Last mile connectivity for secure and seamless communication in difficult terrains of TBA. This paper describes ISRO’s capability of SatCom applications, which can provide last mile secure connectivity in the entire Indian subcontinent, adjoining Oceans for empowering forces.

1. INTRODUCTION

1.1 Space segment is increasingly being used as a platform for various needs today, including communication, navigation, intelligence and surveillance, education, weather prediction and disaster management amongst many others. It can play an important role in the communication desired in Tactical Battle Area (TBA). The tactical domain is extremely fragile with rapid mobility in a hostile and dynamic environment. In such an environment, modern day communication tools play a crucial role as they ensure constant information flow that help ground forces perform their operations efficiently\(^1\). Military tactical communications are generally employed to provide direct or indirect support to forces deployed in TBA. Such communication can be used securely for voice, data and video transmissions both for locations that are static and by users that are mobile. Over the past three decades, ISRO’s technology has matured in terms of power and band width substantially and now finds use in a large number of commercial applications. Defence sector has used this technology minimally till now and thus has a scope to utilizing this extensively specifically for providing redundancy to terrestrial networks and communicating in inhospitable areas where the forces operate.

ISRO’s communication satellite launched in 2015 features a high power, high gain and unfurlable on board antenna of six meters in diameter. This paves way to use of smaller and low power hand-held terminals for strategic use\(^2\).
2. SATCOM FOR STRATEGIC USERS

2.1

The prime requirement of military satellite communication is encryption, reduced probability of interception, ruggedized ground terminals and anti-jamming capabilities. In dynamically varying tactical situations and environmental conditions, ISRO’s communication satellite provides secure communications (voice, data and video) in the form of reporting service, two-way voice communication, multimedia and broadcast services on a mobile terminal.

TBA communication services are broadly categorised as either mobile or static communications. ISRO’s Mobile Satellite Services (MSS) is used for mobile communications, while Portable Satellite Terminal (PST) for static communication. Both these systems independently provide last mile connectivity.

2.2 Mobile Satellite Service

Mobile Satellite Services in India has been of utmost importance for Tactical Battle Communication as terrain at border area are inaccessible, have harsh environment and difficult terrains and even it is difficult to connect with terrestrial links. Also during disaster, the terrestrial link fails completely and satellite link is the best and reliable means of communication during this adverse conditions.

2.2.1 Handheld Reporting Service Terminal

The Handheld Reporting Service Terminal supports tracking and real time position reporting of Vehicle/Vessel. Additionally, it supports emergency messaging through soft keys, data collection and SMS services. The reporting terminal is primarily a S-Band transmitter transmitting its position periodically (1 sec interval min.) at 1200 bps to respective Hub through high gain satellite along with secured short messages for tracking. From the hub the information is delivered to the User through GSM / web portal.

These terminals support short messages edited from key board, UART or USB interface and Bluetooth along with co-ordinates from GPS/NavIC (multi-Constellation). One potential usage is Fleet Management and Monitoring wherein the MSS terminal with NavIC receiver is mounted on the vessels to transmit position information via a satellite to fleet management control Web portal as shown in Fig-1. These terminals are battery based and can operate on AC power supply also.

![Fig.1: RT Integrated with NavIC Receiver for Vessel Tracking and Monitoring](image_url)
All updates/events from RT are received at NMS using MFTDMA mode and emergency messages, like accidents, attack, SOS etc., in ALOHA mode. For emergency messages, the NMS coordinates with emergency services through GSM/GPRS gateway or through Satellite Terminal and sends acknowledgement to RT. The NMS generates periodic reports on the hub efficiency (received and transmitted messages) as shown in Fig-2.

Security of service is ensured by commissioning of the terminal at the hub by its unique ID, information is viable/visible only to the end-user.

RT firmware/application software can be remotely upgrade/patched using 4G n/w without manual intervention. One of the potential application is Two Way Reporting Service for Coastal Surveillance to meet the requirement of coastal security, tracking of sub-20 m boats for coastal surveillance. The cost-effective, rugged, reliable two way RTs can be mounted on Sub-20 m boats to track its position and support to exchange emergency messages from RT-Hub (vice versa) as shown in Fig-3.

![Efficiency of RT Services](image)

**FIG. 2: EFFICIENCY OF RT SERVICES**
2.2.3 Two-Way Voice Communication: Satellite Mobile Phone

In the TBA, Satellite based mobile voice communication is inevitable using small portable hand held battery operated two-way voice communication terminal designed by SAC/ISRO. The terminal can support voice & data communication at 2700 bps with inbuilt GPS. The user friendly terminal is interfaced with Android Smartphone for display as shown in Fig-4a & 4b.

*Fig. 3: Two Way RT for Coastal Surveillance*

*Fig. 4a: Two Way Terminal Voice Communication for strategic purpose*
An app on android phone performs the front end functionality of satellite phone, viz. registration, making calls, messages etc. The terminal can be used for transferring secured text to another terminal or Hub or to a group of soldiers. This is a proof of concept terminal and can be scaled up for user’s requirement without changing any hardware.

3. PORTABLE FIX SATELLITE SERVICE FOR LAST-MILE CONNECTIVITY

3.1

A Satellite based DVB-RCS/customized VSAT network can provide secure connectivity among users for exchanging real time information, command and control in various modes like text, voice, images, video, broadcast services, video-conferencing etc. It will facilitate communications from Corps Headquarters to the troops deployed in the forward areas and to offensive formations operating beyond the borders in the enemy territory. On disaster management front, the VSAT to VSAT connectivity can also be utilized for secure communication, response to disaster struck areas and also provide secure hotlines during disaster and other tactical situations.

3.2

The extended coverage foot print of South Asian Satellite can be utilized for tactical communication using VSATs especially in border areas. The Ku band VSAT star network is standard DVB-RCS format where forward link from centralized Hub to user is DVB/MPEG-2 format and return link from user to Hub is Multi-Frequency– Time Division Multiple Access (MF-TDMA) scheme, for two-way exchange of information. The forward link offers 1 to 45 Mbit/s and return link 64 kbps to 4 Mbps per carrier. To establish communication at remote VSAT location, user requires Satellite modem, LNA, BUC and typically 1.2 m Ku-band reflector. The antenna and ODU are required to keep outside and others units can be inside.
The VSATs employ a scheduled MF-TDMA scheme to access the network and participate in bidirectional communications. The MF-TDMA allows a group of VSATs to communicate through the Hub using a set of carrier frequencies, each of which is divided into time-slots. The Hub allocates to each active VSAT a series of bursts each defined by a frequency, bandwidth, start time and duration. Video conferencing can be established between two VSATs in remote strategic location and with the control centre where Hub is located as well. Such VSAT networks ensures connectivity to the last mile as shown in Fig-5, internet facility in hostile locations, access to other geographical information using India’s Geo-platform Bhuvan and meteorological data access using MOSDAC portal of SAC makes it a vibrant platform.

4. CONCLUSION

4.1
SATCOM renders excellent, secured mobile & fixed services, precise location information to meet the needs of secure communication in changing tactical situations and environmental conditions. The reporting, monitoring and tracking of tanks, vessels and fleet is feasible with indigenous satellite based infrastructure irrespective of geo-location. Reliable voice, data and video connectivity among mobile/static users facilitates command/Control within, and in support of tactical forces. In case of VSAT, the antenna and ISRO’s high gain, high power satellite serves strategic users in conjunction with readily deployable Portable Satellite Terminal (PST) and VSAT together for providing seamless communication in tactical battle area. Future thrust is to launch high throughput satellites with Ku-band spot beams, Ka-band high potential Gateways to foray and deliver a wide Spectrum of applications. In general, India’s Space Programme has emerged as powerful platform, tool delivering products for Social, Scientific and Strategic purpose.
ACKNOWLEDGMENT

Special thanks to all the members of SAC, ISRO involved in the design and testing of MSS terminals and NaVIC receivers. Also indebted to all people involved during the various field trials.

REFERENCES

1. Tactical Communications Command and Control
   Dilip Kumar Mekala, New Delhi

2. Annual Report, ISRO 2016-2017 (English)

3. Satellite and Space Applications in Defence Sector, Colonel NS Yadav, A Journal of Defence Information and Communication Technology, 2017

4. GSAT-9 Brochure, ISRO.


Mobile Communications using Modified 4G LTE and Futuristic 5G for Joint Operational Environment

Col A Oberoi

Abstract—The pressing requirement in a joint operational environment of connecting the battle space over a high bandwidth, highly resilient, intelligent, secure and pervasive wireless network calls for the Indian Armed Forces to explore options of procuring commercially available 4G LTE solutions for the forward edge/tactical battlefield area. However, committing to this technology for large scale induction might not be the most optimal path. 4G LTE is a developing technology with Release 13,14 and 15 in the adoption pipeline. Mission critical requirements of latency and security should be factored in when a wireless roadmap is chalked out for joint mobile network. Also, future development of Military Internet of Things (IoT) would require omnipresent ultra-reliable connectivity for which we must plan for inducting futuristic 5G technologies. This paper endeavours to touch upon 4G LTE, its recent releases, vulnerabilities, and futuristic 5G standards. It recommends that the framework for providing a joint mobile network should incorporate use of civil cellular 4G LTE network in the hinterland, while relying on a captive tri-services mobile network at the forward edge. Further, it suggests evolving a tweaked 4G LTE standard for joint military requirements of security and protection against jamming.

1. INTRODUCTION

1.1
Today the Indian Armed Forces are poised towards becoming joint wherein shared situational awareness will take predominance. All entities will always require to be ubiquitously connected to facilitate applications to share relevant data amongst themselves. Each Service (Indian Army / Indian Navy and the Indian Air Force) have put in place unique network architectures for provision of mobile communication in respective operational environments. Varied applications such as the IACCS (Integrated Air Command and Control System), MDS (Maritime Domain Awareness), upcoming Tac C3I (Tactical Communications Control Computers and information) the CIDSS (Command Information Decision Support System) which incorporates the BMS (Battlefield Management System) and many others require a scalable, reliable, resilient and spectrum efficient network at the forward edge of the battlefield. These applications would need to talk to each other seamlessly while simultaneously exchanging operational info-centric data with the entities operating at the forward edge.

1.2
AREN (Army Radio Engineered Network) in the Indian Army for Strike and Pivot Corps communications have outlived their life. It is voice centric with negligible support for data applications. Various heterogeneous solutions using COTS (Commercially Available Off the Shelf) equipment have been incorporated in formations to meet communication requirements. The MCCS (Mobile Cellular Communication Systems) inducted in the Indian Army for static operational corps has been deployed in two Corps with plans to induct the same in three more corps. The AFCEL (Air Force Cellular Network) is a WCDMA (Wideband Code Division Multiple Access) system.
Access) based 3G network that provides secure end-point connectivity for Air Warriors at all stations. The navy is looking forward to a similar mobile network in its mission critical ports and fighting platforms.

1.3
With considerable deployment costs, it is worth taking a stock of available options today and analyze the present and futuristic requirements with the aim of proposing a road map for exploiting 4G LTE (4G Long Term Evolution) while adapting it to specific military requirements. At the same time, we need to spell out upgrades for incorporating 5G technologies in future.

1.4
The relationship between technology and requirement is very interesting especially in the military. The best available technology in the commercial world may not be the most optimal for the military. With the commercial sector driving technological development as also with limited R&D available for defense within the country, the Indian Armed Forces cannot be expected to roll out a fresh tailor made wireless communication standard. Therefore, we must home on the best suited technology, coordinate with the industry for tweaking it for military specific applications while at the same time be ready to exploit futuristic technological developments.

2. PROPOSED MOBILE NETWORK ARCHITECTURE UNDER JOINT OPERATIONAL ENVIRONMENT

2.1 Existing Mobile Networks

2.1.1
An analysis of the status of existing networks in the three services reveals the following issues as depicted conceptually in figure 1:

(a) Existing 2G and 3G mobile networks of the Indian Army are disjointed with limited capability of transporting data.

(b) AFCEL (3G) existing in pockets across various Air Force stations has limited data carrying capability and is not connected with any army network.

(c) Backbone support for tri services network is not available since the networks in hinterland are not seamlessly connected.

(d) End to end secrecy over mobile networks is not available to facilitate operational communications.
2.2 Conceptual Framework for Joint Mobile Network

For supporting joint operations, the desirable end-state is to have a seamless common cellular network for the three services with end to end secrecy. This however is a utopian solution which may not be realizable in the real world due to resource and manpower constraints. Therefore, the proposed strategy should be to achieve seamless connectivity through available civil cellular networks in the hinterland and utilize captive cellular networks for the forward edge of the operational space. A conceptual depiction of the same is given at Figure 2 below. The captive Tri-Service Cellular networks must be based on 4G LTE modified to meet the requirements of bandwidth for joint battlefield applications. End to End secrecy using robust applications on hardened mobile devices must be utilized to facilitate exploitation of civil cellular networks. The mobile network must be seamlessly integrated with the combat net radio as well as the terrestrial networks. For this standards and interfaces would need to be specified. Select high bandwidth and mission critical applications can be supported by futuristic 5G over short ranges.

2.3 Envisaged Application of 4G LTE Networks

Robust 4G LTE solutions will holistically cater for inter and intra system requirements while executing joint operations. Some of the requirements which the cellular network will facilitate are as follows:

(a) Mobile communications for commanders and staff during operations and integration with Combat Net Radio.
(b) High bandwidth surveillance data transfer from the forward edge.
(c) Mobile operations especially for the Strike and Pivot Corps of the Indian Army.
(d) Data centric applications existing today such as the ACCS (Army Artillery Combat Command and Control System), IACCS (Integrated Air Command and Control System), IMMOLS (Integrated Maintenance Management On Line System) and many others can be fruitfully utilized if seamless IP connectivity is provided using LTE.
(e) Seamless cellular communications on Naval Platforms for Intra and Inter system communication and battlespace awareness.

![Fig. 2: Conceptual Framework for Seamless Cellular Tri-Service Connectivity](image-url)
3. 4TH GENERATION LONG TERM EVOLUTION (4G LTE) AND ITS SUITABILITY FOR JOINT MOBILE NETWORK

3.1 The 4G LTE Standard was finalized by the 3GPP (3rd Generation Partnership Project) in 2008, and its earlier versions were commercially deployed in 2009 in Stockholm and Oslo. It evolved to Release 10 and was named as LTE Advanced in 2011. As of today LTE Release 14 has been frozen in Jun 2019 which involves support for mission critical services, however it has not been completely introduced in the market.

3.2 4G LTE has been widely adopted by major telecom providers in India to provide higher bandwidths and an all IP platform for data driven applications. LTE network Infrastructure providers have been making efforts to gain inroads for absorption of their systems into the Indian Army. The requisite spectrum for both LTE FDD (Frequency Division Duplex) as well as LTE TDD (Time Division Duplex) has been allocated. Although both standards aim towards duplexing, the main differences between the two and its military implications can be summarized as follows.

<table>
<thead>
<tr>
<th>Feature</th>
<th>FDD</th>
<th>TDD</th>
<th>Implications for Military</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Latency</td>
<td>Lower, since uplink and downlink frequencies are used simultaneously</td>
<td>Higher, since time slots are shared between uplink and downlink.</td>
<td>Military Applications require low latency especially for mission critical data, therefore FDD should be preferred.</td>
</tr>
<tr>
<td>• Spectrum Efficiency</td>
<td>Inefficient</td>
<td>Relatively more efficient</td>
<td>Spectrum is a scarce resource in the battlefield and would require to be judiciously utilized.</td>
</tr>
<tr>
<td>• Distance Preferability</td>
<td>Distance does not affect the efficiency of the system</td>
<td>As distance to the base station increases, the guard interval between time slots for uplink and downlink increases due to propagation delay and increased multipath. Therefore efficiency decreases.</td>
<td>FDD will be more robust to varying distances in battlefield conditions.</td>
</tr>
<tr>
<td>• Unbalanced Factor/ Dynamic Adjustment for increased Downlink traffic</td>
<td>Dynamic adjustment not possible</td>
<td>Number of time slots allocated to downlink can be increased dynamically and therefore the system can be tweaked to specific requirements.</td>
<td>Flexibility of TDD is desirable for military applications.</td>
</tr>
<tr>
<td>• MAC Layer and Timing Complexity</td>
<td>Less complex</td>
<td>More complex due to requirement of accurate timing requirements.</td>
<td>Lower complexity is desirable for military applications.</td>
</tr>
<tr>
<td>• Equipment Cost</td>
<td>Requires a duplex or to separate frequencies and therefore more costly.</td>
<td>Cheaper as no duplex or needed</td>
<td>-</td>
</tr>
<tr>
<td>• Device to Device (D2D) communications</td>
<td>Less suited, although D2D is feasible.</td>
<td>More suitable for D2D communications since single frequency is used.</td>
<td>D2D is a desirable feature for military applications where in absence of base station will not render the user equipment useless.</td>
</tr>
</tbody>
</table>
3.3
We realise that both FDD as well as TDD have their own inherent advantages for military applications. Latency for mission critical and real time requirements of a primary concern and therefore FDD is a desired technology. However spectrum efficiency, dynamic bandwidth or capacity configuration between uplink and downlink and requirement of simple MAC (Medium Access Control) layer communications for devices such as Military IoT, TDD is more suitable. A recommended approach would be to have a co-deployment scenario with both TDD and FDD with inter-workability options and traffic load balancing as per requirement. Nokia is offering such solutions in the market today

3.4 Frequency Considerations
Utilisation of 4G LTE by the Indian Armed Forces for static as well as mobile operations for beyond line of sight connectivity needs to be carefully planned. Use of lower frequency window in the LTE band, of about 700 MHz would make it possible for providing longer ranges under obstruction by vegetation or built up areas. However the number of users at these frequencies for a single base station gets restricted and therefore for smaller more dense cells in areas where headquarters are located, higher frequencies with smaller micro/ pico cells would be ideal.

3.5
The evolution of various incremental releases of LTE forecasted till induction of 5G is given in the following diagram. It is foreseen that by 2020, 5G wireless standard would be adopted by most global service providers.

*Fig. 3: 4G LTE Release Versions and Timelines*
4. TECHNOLOGICAL ISSUES IN USE OF COMMERCIAL LTE AND PROPOSED ADAPTATION FOR THE THREE SERVICES

(a) Latency: In wireless networks latency is of two types, the Control Plane latency (Network access by end user equipment- the time it takes to establish the connection) and User (End to End) latency which involves the delay from the gateway to the service provider. For real time mission critical applications in a joint operations, such as fire control systems, air defence and remote piloting of UAVs (Unmanned Aerial Vehicles) and Drones, latency considerations are of prime importance. While the end to end latency is also dependent on the robustness of the terrestrial network, the control plane latency needs to be as minimum as possible. However the 3GPP standards have set the control plane latency to 100ms. This might not suffice for time critical applications and therefore control plane latency standards are required to be spelt out. For 5G, the control plane latency desired is 10ms or less.

(b) Handover Performance: LTE implements ‘Break before Make’ handover. The ITU (International Telecommunication Union) target is 30-60ms and observed to be typically 49.5ms. Also if a handover is unsuccessful this time may increase to as much as 200ms. This may become an issue for critical connected mobility applications with stringent latency requirements. This issue is presently being addressed by 5G in “Make before Break”, “Multi Cell Connectivity” and “Synchronised Handovers”. Certain modifications of LTE presently have been tried with experimental equipment for ultra-low latency handover performance.

(c) Vulnerabilities of 4G LTE: Several independent studies have been conducted to highlight existing vulnerabilities in the 4G standard. Some of these which are of relevance to military applications and which must be further studied by Indian Army are as follows.

(i) Vulnerability to Smart Jamming Attacks: LTE utilises OFDMA (Orthogonal Frequency Division Multiple Access) for the downlink and the SC-FDMA (Single Carrier Frequency Division Multiple Access) for the uplink. The LTE air interface consists of control channels which carry critical handshake and data channels. Smart jammers can learn the network timing and control channel configuration. Two concepts have been often discussed with jamming strategy as ‘cheater’ and a ‘saboteur’. It has been shown that the performance of the LTE network gets severely affected by smart jamming approach. This approach consists of a combined action of four types which include the following.

<table>
<thead>
<tr>
<th>Jamming Types for LTE</th>
<th>Proposed Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Barrage Jamming</td>
<td>FDM Based solution</td>
</tr>
<tr>
<td>Partial Band Jamming</td>
<td>TDM based solution</td>
</tr>
<tr>
<td>Single Tone Jamming</td>
<td>Transmit power control solution</td>
</tr>
<tr>
<td>Multi Tone Jamming</td>
<td>Frequency hopping solution</td>
</tr>
<tr>
<td>Asynchronous off-tone jamming</td>
<td></td>
</tr>
<tr>
<td>Pilot tone jamming and pilot nulling</td>
<td></td>
</tr>
<tr>
<td>Attack Target</td>
<td>Attack Type</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>LTE Security</td>
<td>User Identity and Privacy threat</td>
</tr>
<tr>
<td></td>
<td>- Control Plane data modification</td>
</tr>
<tr>
<td></td>
<td>- eNB attacks, unauthorized access to the network.</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>- Redirection attacks/false base station attacks</td>
</tr>
<tr>
<td></td>
<td>- Evolved Packet System Authentication and Key Agreement (EPS AKA) weakness exploitation</td>
</tr>
<tr>
<td>False Base Station</td>
<td>- Initial attach procedure</td>
</tr>
<tr>
<td></td>
<td>- Inter-EPS (Evolved Packet Core) handoffs</td>
</tr>
<tr>
<td></td>
<td>- Fake base station requesting IMSI of user equipment.</td>
</tr>
<tr>
<td>VoLTE Attacks</td>
<td>- SIP security threats including SIP flooding</td>
</tr>
<tr>
<td></td>
<td>- Signaling bearer attacks</td>
</tr>
</tbody>
</table>

(ii) Attacks on LTE Networks: LTE networks have been found to be susceptible to the following types of attacks. It is therefore prudent to explore options for including the proposed solutions for induction into the Indian Army.

5. 5TH GENERATION AND ITS UTILITY IN THE FUTURE

5G has been thought to be much more than a simple incremental advance on 4G. It is foreseen that the number of devices and the corresponding data rates will grow exponentially and reach hundreds of billions. In order to meet the surge in demand, 5G standardization activities are being undertaken. The motivating factors for 5G is shown in the following figure.
5.1
The aim of 5G would be to provide ubiquitous high-rate, low latency network connectivity while at the same time integrating with WiFi standards and LTE. A comparison between the two when being used in the commercial world can be appreciated in the following figure which depicts the sub-ms latency which 5G networks will promise.

5.2
A number of applications will ride on 5G and a brief analysis of services which can be delivered though 4G LTE or legacy technologies and those which need 5G is given in the following figure. The tactile internet meant for military use lies in the region supported by 5G. The requirements of tactile internet are high bandwidth combined with ultra-low latency. Indian Armed Forces must therefore aim towards exploiting 5G for the forward edge wireless connectivity in the tactical battlefield and work towards absorption of relevant standards.
5G Technologies: A number of challenging technologies have been foreseen to form part of the backbone of 5G. These are as follows.

(a) Millimeter waves: The traditional sub-3GHz spectrum has become congested and its limit of utilization has been reached. MM waves offer huge spectrum which can revolutionise wireless communications. For example in the 60GHz range there is 9 GHz of unlicensed spectrum available for being exploited. Also mm Waves call for very small antennas which can be packed as MIMO arrays on the handsets in a very small area and afford high degree of beamforming. 28 GHz and 38 GHz bands are presently being utilized by 4G standard for fixed wireless applications. However mm waves suffer from severe pathloss, fading due to rain and obstacles and therefore strategies for exploiting these are presently being explored.

(b) Massive MIMO This is an evolving technology which proposes to utilize hundreds of antenna arrays for spatial multiplexing so as to achieve space and time diversity to exploit the channel for higher data rates

(c) Spectrum Sharing: Distributed and centralized spectrum sharing techniques are proposed to be utilized to ensure better efficiency to utilize free time of available spectrum

(d) Small Cells: Smaller cells will enable spatial reuse of frequency and higher density affording higher data rates.

(e) Beamforming: Capability of Massive MIMO will enable beamforming and BDMA (Beam Division Multiple Access) schemes.

(f) Full duplex: Instead of using FDD and TDD as is the case in LTE the proposed 5G systems will be able to use full duplex schemes. The transmit and receive will take place at the same frequency as well as the same time thereby greatly enhancing spectrum efficiency. This will be possible using RF interference cancellation techniques and electrical isolation.

6. FUTURISTIC REQUIREMENT OF LTE ADVANCED PRO AND 5G FOR INDIAN ARMED FORCES

6.1 With greater emphasis on joint operations in the battlefield, the Indian Armed forces will require connectivity options with high degree of reliability, very low latency and flexibility in terms of bandwidth and connectivity with base station. Some of the applications which will require ultra-reliable low latency communications as guaranteed by LTE Advanced Pro (release 14) and 5G are as follows.

(a) Provision of high speed data transfer with swarms of Drones and UAVs.

(b) Ubiquitous connectivity for Narrow Band IoT applications for battlefield surveillance, monitoring, battlefield medical and health applications.

(c) Push to Talk setup for communication with combat net radio.

(d) Casualty evacuation and medical emergencies involving real time video links and high definition image transfers.

(e) Dynamic Spectrum Access utilizing white spaces in the spectrum under heavy interference and enemy jamming.

(f) End to end security protocols for secure
resilient links. 5G will support true encryption at physical layer and all control and signaling information would also be encrypted.

(g) Self-organizing network setup with additional nodes automatically configuring themselves as these get deployed in the battlefield.

(h) M2M (Machine to Machine) communications for sensors, drones and logistics.

(i) D2D (Device to Device) including relay in areas where users go out of range.

(j) V2X (Vehicle to Everywhere) communications for high speed connectivity for mobile commanders in the battlefield.

7. CONCLUSION

7.1
As a part of strategic planning, we must take cognizance the recent developments in 3GPP (3rd Generation Partnership Project) and 4G LTE especially the releases 11, 12, 13 and 14. We must avoid a situation wherein the Indian Armed Forces are left with fate accompli towards procuring commercially available 4G LTE platforms without the requisite reliability and security built into the systems.

7.2
A thorough understanding of available 4G LTE options, its vulnerabilities and of options of military hardenings an inescapable requirement for relevant personnel involved in conceptualizing, planning and operating joint mobile communication networks.

7.3
In order to utilize 4G LTE it is imperative that military specific standards be evolved which will ensure interoperability, security and availability for joint battlefield applications. A Backbone Framework is required to be established for the same. Further, in order to accommodate futuristic tactical applications, Military IoT and Real-time mission critical implementations we must be ready to deploy and optimally utilize 5G solutions.

7.4
It is therefore recommended that induction of 4G LTE for Tactical Battlefield communications should be brainstormed and a modified standard specific for Indian Armed Forces must be evolved. In addition, development of joint battlefield applications must be factored for future requirements and corresponding 5G technologies should be earmarked. For facilitating seamless mobile connectivity for joint operations we must be able to utilize the 4G civil cellular network across the length and breadth of the nation. The Industry must be taken into confidence to incorporate military hardened standards and an ‘Experts Committee’ should be setup as a standardization group. Collaboration with US Army / NATO may be explored to gain knowledge about similar endeavours for US Mil Standards. We must therefore lay down the following as the “way forward”.

(a) Formulate customized standards and ensure that all procurement policies conform to the standards.

(b) Press hard for end to end encryption for mobile devices so as to be able to ride on civil cellular networks.

(c) Closely collaborate with the industry, academia and specialists by spelling out clear requirements and standards.

(d) Optimise our investment strategies for R&D.

(e) Lay down roadmap to facilitate adoption of future technology trends such as 5G (future proof).
REFERENCES

6. From LTE to 5G for Connected Mobility, Mar 2017, IEEE Communications Magazine, Mads Lauridsen, Lucas Chavarria Gimenez, Ignacio Rodriguez
7. Resilience of LTE Networks Against Smart Jamming Attacks: A Game-Theoretic Approach By Farhan Muhammad Aziz, 2017
9. Understanding 5G Perspectives on future technological advancements in mobile – GSMA Intelligence, Dec 2014
Developing Synergy and Jointness in Cognitive and Social Domains

Col K Pradeep Bhat (Retd)
E-mail: kpbhat@nciipc.gov.in

Abstract—The Joint Doctrine for Indian Armed Forces published by HQ Integrated Defence Staff in Apr 2017 describes how, with Jointness, “a high level of cross-domain synergy is attained that vastly enhances success potential”. The doctrine also describes “Integration’ as the integration of ‘processes’ across all operational domains, towards optimisation of costs and enhancing readiness”. Many other studies also point out that trust (a cognitive characteristic), culture, teamwork and collaboration (social characteristics) are essential to success in today’s high-paced operations.

This paper explores why and how synergy and jointness have to be tackled in the cognitive and social domains, and how leaders have to adapt themselves to ensure its success. Technology frameworks that can support these two domains are also discussed.

1. INTRODUCTION

1.1
All large enterprises visualise the implementation of their organisational goals, objectives and strategy through the three dimensions of people, processes and technology. The Defence Forces, traditionally used to Service-based siloed operations, have generally tried to address Jointness through technology to integrate entities, coordinate their actions and develop shared understanding through joint training. This approach has its limitations in the sense that it does not fully tackle the “people” dimension at the cognitive and social levels. This aspect is recognised in the Joint Doctrine for Indian Armed Forces, which mentions that “Commanders need to actively invest in people, time and resources to develop jointness amongst personnel of the Armed Forces”.

1.2
Vice Admiral Arthur K Cebrowski, US Navy, who first coined the term “Network Centric Warfare”, describes NCW as primarily about human behaviour as opposed to information technology. Warfare is about human behaviour in a context of organised violence directed toward political ends. Hence, the focus has to be on human behaviour in the networked environment, rather than on the network itself. In other words, the “network” is not to be treated as a noun, rather treat “to network” as a verb.

1.3
Vice Admiral Cebrowski also contended that conflict in the modern battlespace encompasses the physical, information, cognitive and social domains. The relationship between these domains of conflict are shown in the figure below.
2. UNDERSTANDING THE COGNITIVE DOMAIN

2.1

The cognitive domain is in the minds of the individuals and the leaders, where perceptions, awareness, understanding, beliefs and values reside and where, as a result of sensemaking, decisions are made.\(^6\)

2.2

There is a unique spirit inherent in the Indian Armed Forces personnel that embodies their motivation and commitment to serve the nation, their readiness to lay down their lives for the security of the nation, and their ungrudging acceptance of physical and emotional hardships that they have to face in their line of duty. Human behaviour analysts would agree that this spirit is fostered and enhanced in the individual Services through their respective military ethos, traditions and other key intangibles inherent in their respective organisational histories.

2.3

The culture of jointness can be developed by extending the “military spirit” beyond the individual Services. Organisational culture is a nebulous concept that manifests itself through the behaviour of individuals, teams and leaders of the organisation. Each of the three Services have their own unique organisational cultures and the way to bridge the same is through a common understanding and appreciation of each Service’s culture, capabilities, strengths and limitations. This effort has to further extend to encouraging and developing trust amongst individuals of different organisations, who form part of joint groups.
2.4
It is important that the common understanding and shared appreciation have to percolate from the top leadership of the Services down to the frontline troops. An even bigger challenge is to sustain the same, when some events and incidents take place, which causes a build-up of distrust. Leadership then plays a major role to contain the build-up of negativity and regain the lost trust.

2.5
Measuring the success of jointness at the cognitive level is very difficult. Behavioural analysis techniques and trained analysts would be required to design appropriate measurement mechanisms.

3. UNDERSTANDING THE SOCIAL DOMAIN

3.1
Jointness is less about grand architectures and systems, and more about day-to-day living in a culture of interdependence. The social domain plays a very important role to develop synergies amongst individuals within and across various organisations. Lifetime bonding between individuals of different services is the raison d’etre of our tri-services institutions like the National Defence Academy and the Defence Services Staff College. It is important that similar social bonding is extended to all individuals of the three Services through some forums. It should be further extended to other organisations, with whom the Defence Forces have an inter-dependent relationship.

3.2
It must be recognised that social collaboration is prone to inter-personnel conflicts, many times triggered off by mismatch in understanding of organisational cultures. This, if not controlled, can lead to serious dysfunctional relationships. Formal and informal leadership again plays an important role in the resolution of conflicts.

3.3
Measuring the success of jointness at the social level is easier than that at the cognitive level. Both quantitative and qualitative analysis techniques will have to be used to design appropriate measurement mechanisms.

4. SUPPORTING TECHNOLOGIES

4.1
Enterprise Social Collaboration platforms are best suited for supporting jointness at the cognitive and social domains, specially across multiple federating organisations. Such platforms enable individuals to digitally build and sustain their human networks within and across organisations. The platforms also let individuals share their professional details, knowledge and expertise with others, provide a ‘face to a name’ through business cards, and provide collaborative spaces for engagement, such as team rooms, communities, and discussion forums. Such forums also enable leaders to connect better with their command through a non-rigid hierarchy.

4.2
The enterprise social collaboration platforms are useful for organisations to build trust, empathy and common understanding that revolves around non-classified information. Classified information however needs additional technological mechanisms to ensure that trust is retained between individuals and organisations around the “need to know” and “need to share” critical and sensitive information, typically centred around operations, intelligence and operational logistics.
4.3
Technology by itself is not sufficient to tackle the issue of trust. It also needs research and analysis of human behaviour as to why do individuals and organisations share or decline to share information, even when they are aware that it is for the larger common good. A great deal of work is happening in this area, globally and in India, but it is limited to non-military enterprise domain. Similar research is required for the military domain too.

5. ROLE OF HUMAN RESOURCES MANAGEMENT
5.1
The HRD programs in the Armed Forces are targeted towards imparting of skills and knowledge that is essential for each progressive rank and appointment held by an individual. Joint training programmes are focused on efficiency and effectiveness of teams and groups. There is little focus on enabling cognitive thinking in individuals in aspects like understanding their own behaviour and that of the others, handling inter-personal conflicts, and collaborative leadership. This aspect needs to be addressed too, on our road to jointness.

6. CONCLUSION
6.1
Synergy in the cognitive and social domains is vital for achieving Tri-Service jointness. It has to be driven primarily from the people perspective, duly supported by processes and technology. It has to also extend beyond the Defence forces to other arms of the Government, for synergy to be achieved at the national level.

REFERENCES
A Framework for Implementation of Smart Documents for Armed Forces

Maj Kunal Pal¹ and Dr CRS Kumar²
E-mail: ²suthikshnkumar@diat.ac.in

Abstract—Intelligence is the process of planning, collection, collation, analysis, interpretation, and dissemination of collected information. The security of this information in any military operation is of prime importance for the success of the mission. Providing the right information at the right time and at the right place is very important for the Commanders at all levels to enable them for a better decision making to achieve their objective. This sensitive information is provided by numerous sources spread throughout the battlefield in a hostile environment. In such an environment, an adversary endeavors to manipulate the information to disrupt our planning. So, it is of extreme importance to ensure that the information provided by any source in a highly contested environment is verified for its integrity, authenticity and that the information is reliable, immutable and available as and when required. Thus, in this paper, a method of sharing information using Smart Documents embedded with a Quick Response (QR) code which will contain the Digital is proposed Signature of the originator to provide an efficient mechanism for verification of the document. The use of Block chain technology will provide a secure, immutable and verifiable model for the storage of these Smart Documents without depending upon any third party. Also, the paper proposes a viable framework for the creation of a Smart Documents and verification of the same.

1. INTRODUCTION

1.1
Colonel John Boyd of U.S. Air Force developed a decision making cycle called the OODA Loop [1] (Observe-Orient-Decide-Act) which enable Commanders at all level to rapidly, observe and react to a sequence of unknown events of the adversaries by getting into his decision making cycle and gaining advantage. The first step in the OODA Loop is to Observe. At this point, the main aim of any Commander is to gain an accurate picture of a given situation by using all the information sources available with him. Information will be available via various sources like Human Intelligence, Imagery Intelligence, Technical Intelligence, Signals Intelligence, Open Source Intelligence and lastly Measurement and Signatures Intelligence[2].

1.2
The information from these sources is shared via documents with all the intelligence agencies for better command and control of the situation. Thus, multiple copies of these documents are created and send to them individually where they are handled separately with updates/changes to them also handled separately. Most of the organizations are using independent centralised storage solutions to store this information which suffers from inherent weaknesses of the trust-based model. Thus, the data generated, stored and transferred from a centralised storage system into a military network may have issues related to integrity, availability, and authenticity of data.

1.3
This paper proposes an architecture for the creation of QR code and digital signature based
Smart Documents with the help of blockchain technology. The proposed architecture provides a mechanism for easy storage, access, and retrieval of documents and at the same time provides a transparent and auditable environment for verification of integrity and authenticity of the documents. The proposed methodology to create a Smart Documents is by embedding a QR code [3] on the required document to be verified. The QR code due to its high data storage capacity and fast readability makes the process of verifying a document simple. This QR code will contain the digital signature which will enable authentication of the issuing authority. Also, the documents hash value and its unique ID along with credentials to verify the sender are stored in the blockchain framework that enhances the credibility of the document.

1.4

The rest of the paper is organized in the following manner: Section II covers the literature review. Section III describes the proposed method and the technologies that are used in the creation of Smart Documents. Section IV covers the method of creation of a Smart Documents and verification of the same. Section V discusses the testing and evaluation of the proposed framework. Finally, Section VI gives out the conclusion of the paper.

2. LITERATURE REVIEW

2.1

Blockchain technology is expanding beyond the use of crypto currency sector initially proposed by Satoshi Nakamoto [4] in the Bitcoin white paper. As the concepts of blockchain technology are evolving, there are a few emerging directions relevant to defence applications where research is being carried out is, tracing of defence related shipments and contracts [5], secure messaging [6], cyber warfare [7], and protecting weapons systems in defence networks [8].

2.2

Most of the military equipment is based on a centralised control platform where the security of this equipment is based on the trust of the information provided by various intelligence sources. These intelligence sources may include various documents that may be classified or unclassified like the dispatch document, intelligence reports, operation plans, maps of the hostile area, aerial/satellite images, etc. These documents are usually generated, shared and stored by various departments. Each department handled these documents separately with updates/changes to them also handled separately. The data, when stored in the centralised environment has various issues like a single point of failure, data availability and denial of service (DoS).

2.3

Various techniques like the use of barcode and public key encryption have been proposed to mitigate the issue of authenticity and integrity of documents both in the hard and soft copy of the document [9,10]. In [11] the author has proposed the use of digital signatures to verify the authenticity of a document. In [12] they have given the solution to verify the integrity of a document using cryptographic hashing, 2D barcodes, Optical Character Recognition (OCR) and digital signatures. In [13] instead of encrypting the complete document only the basic details of the document like the title, header, addressee, date of signature, etc are used to create a digital signature.

2.4

Many blockchain based methods have been proposed for the secure storage of documents. The simplest method to store a file using a blockchain is to store the complete file in the block. However, it will result in a large block size due to which there will be high latency
in the network thus making it inefficient. Nick Szabo in [14] has proposed the creation of a blockchain based smart contract which computer generated contract that enables a computer to digitally validate and impose the performance negotiation agreed in the contract. The clauses in the contract are trackable, irreversible and tamper-proof due to the use of blockchain technology. In [15] they have proposed a method in which the data is split and stored in multiple computers of the same network. The method provides reliability as the data is replicated among several nodes of the network and can be retrieved even if one of the nodes goes down. However, to achieve data consistency and synchronization, the method proposed in [15] requires complex algorithms. In [16] an Inter Planetary File System (IPFS) has been used that connects all the computers using a P2P (peer-to-peer) network. The single large file is divided into small size and the hash of these files is distributed using the P2P network among all computers. In [17] they have proposed a method known as Storj in which P2P cloud storage has been used that does not rely on any third party. The client stores his data on to the cloud using an encryption technique and is responsible for the key management. In [18] the author has carried out measurements of efficiency between Hyper ledger and SQL database in terms of throughput, latency and execution time and found that Hyper ledger is more efficient for a data intensive application.

3. PROPOSED METHOD

3.1

In this paper, a method for the creation of a Smart Documents has been proposed which aims at verifying the authenticity and integrity of a document and at the same time provide a mechanism for easy storage, access, and retrieval of documents from a transparent and auditable environment. To provide a simple verification process, it is required to print the digital signature of the owner on the document. A digital signature can be easily verified from an electronic document however they cannot be verified directly from the hard copy of the document. The use of QR code in Smart Documents helps us in overcoming this problem. The QR code embedded in the Smart Documents can be scanned by a QR code scanner and retrieve the details from the distributed, immutable, reliable blockchain network for verification purpose.

3.2

The succeeding paragraphs cover the technologies that are used in the creation of Smart Documents.

(a) Digital Signatures:

(i) Digital signatures are equivalent to a handwritten [19] signature which offers far more security as they cannot be copied or forged. By using encryption and hashing technique it gives the recipient a strong cause to believe that the document was created by the owner which has not been altered during transmission or storage thus, providing authentication of the originator and integrity of the message. Also, since the digital signature has been created using the private key it can be only be verified using the corresponding public key of the originator and thus, the originator cannot deny signing the document. This property is called non-repudiation. A unique digital certificate [22] is required to create a digital signature that is based on asymmetric key cryptography, also known as public-key cryptography. RFC 5280 [20] gives out the current standard for the use of digital certificates X.509.
(ii) The diagram shown in figure 1 illustrates how to sign the document and verify it. The owner of the document passes the document to be signed through a hash function which gives out a unique hash digest. Hash digest is then encrypted using the owner’s private key which gives out a digital signature. The document along with its digital signature is sent to the recipient where he uses the public key of the owner to decrypt the digital signature and get a hash digest. Simultaneously, the document received by the recipient is also passed through a hash function to create a hash digest. If both the hash digests are found to be the same then the digital signature is verified else it can be said that the document has been tampered with.

(b) **QR Code:**

(i) The QR (Quick Response) [21] code proposed to be used is a two dimensional bar code that was first designed by Denso Wave in 1994 for the automotive industry in Japan. It has more data storage capacity and provides an efficient mechanism for encoding the information. The diagram as shown in [21] and given in figure 2 shows the key features of the QR code: -
(aa) Version information: There are currently 40 different QR code versions. Each version has a different module configuration that can store a different size of data in them.

(ab) Format information: It contains the information of the encoded patterns to enables the rest of the region to be decoded [21].

(ac) Data and error correction area: It contains the actual data that is encoded in the QR code. A conventional barcode can store upto 20 digits whereas a version 40 QR code can store up to 7089 numeric data, 4296 alphanumeric data, and 2953 binary data. This area is also used for error corrections which are based on Reed-Solomon Codes [23].

(ad) Positioning detection pattern: QR code can be scanned from any direction. The use of positioning detection helps us find the correct position of the QR code.

(ae) Alignment pattern: A large QR code may have issues with its orientation, the use of alignment pattern in the QR code help with the same.

(af) Timing pattern: It is used to find the width of the code or the dimensions of the data matrix.

(ag) Quiet zone: This spacing is used to separate the QR code from its surroundings.

(ii) QR codes outperform other one-dimensional barcode standards because of its high capacity, strong error tolerance, fast readability, and flexible encoding options, thus qualifying it to be a suitable scheme for URL sharing, contact sharing, business card, Wi-Fi access point, information sharing at tourist and public places, electronic payment, ticketing, and shipping services.
(c) Blockchain:

(i) The concept of blockchain was proposed by Satoshi Nakamoto in 2008 [4]. The emergence of blockchain technology can be linked to the introduction of decentralised crypto-currency for the internet like Bitcoin [4].

(ii) The advantages of using blockchain over the legacy centralised storage system are shown in table 1.

<table>
<thead>
<tr>
<th>Characteristics</th>
<th>Blockchain</th>
<th>Centralised Storage System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Storage</td>
<td>Decentralised</td>
<td>Centralised</td>
</tr>
<tr>
<td>Reliability</td>
<td>Data replicated across various nodes</td>
<td>Potential single point of failure</td>
</tr>
<tr>
<td>Security</td>
<td>Cryptographic keys</td>
<td>Established via central authority</td>
</tr>
<tr>
<td>Trust</td>
<td>Immutable records</td>
<td>Administrator based</td>
</tr>
<tr>
<td>Control Authority</td>
<td>Base on the consensus mechanism</td>
<td>Centrally controlled</td>
</tr>
<tr>
<td>Audit</td>
<td>Not required due to immutable records</td>
<td>Regular checks required</td>
</tr>
<tr>
<td>Architecture</td>
<td>Peer to Peer(P2P)</td>
<td>Client-Server Based</td>
</tr>
</tbody>
</table>

(iii) Blockchain is a distributed ledger technology that contains valid transactions that are recorded into a block by the nodes, and these blocks are linked together in a way that makes tampering of them difficult. The participating nodes can sequentially append additional blocks [4] to the existing chain of blocks.

(iv) The diagram in figure 3 shows what a block in a blockchain contains and how they are linked together. The first block in a blockchain is known as the genesis block [24]. Each block contains a hash digest generated by passing the document through a hash function, the hash of the previous block and the transactional details. Thus, every succeeding block of the blockchain is linked with the hash of the previous block that prevents the new block from being altered or adding in between. So, each block added into the blockchain strengthens the verification of the previous block and hence the entire blockchain. The method makes the blockchain tamperproof and immutable.
(v) To add a block into the blockchain network a predefined rule based on a consensus mechanism [25] is used as given in figure 4. The consensus mechanism is an algorithm that ensures that updates to the blockchain are agreed by the majority of the nodes participating and the same is communicated across the entire network thus, providing a transparent and auditable environment. There are various types of consensus mechanisms being used in the blockchain system e.g. Proof-of-Work, Proof-of-Stake, Practical Byzantine Fault Tolerance, Knowledge Proof, Proof-of-Authority, Proof-of-Capacity, etc [25].

(vi) Blockchains can be public, private or consortium based [26]. A public blockchain also called a permission less blockchain. It can be used by anyone on the internet for reading, writing, and auditing. They are transparent and can be viewed by anyone on the network. A consensus mechanism like Proof-of-Work (POW) and Proof-of-Work(POS)
may be used for example Lit coin [27]. Private blockchain also called a permissioned blockchain is specific to any individual or an organization. The members or participants have to be authorized before they can access the services. All participants may not be part of the consensus mechanism for example Bankchain [28]. Whereas in a consortium or federated blockchain members of the selected consortium are given the access rights to *run the blockchain network. Thus, instead of any one individual being in charge there are a group of peoples or companies who come together for the decision making process, for example, Energy Web Foundation (EWF) [29].

For the proposed method, the use of a private blockchain like Hyper ledger Fabric [30] will be done.

4. SMART DOCUMENTS

4.1

In the following paragraphs, we cover the proposed framework for the creation and verification of Smart Documents as shown in figure 5 and figure 6 respectively.

(a) Creation of Smart Documents:

(i) Let us say user A (A) wants to create a document (D_i)

User A \rightarrow D_i \hfill (1)

(ii) The document (D_i) mention in equation (1) is passed through a hash function (H) (e.g. SHA-1, MD-5, Whirlpool and SHA 256) to create a hash digest (H_D_i) which is then encrypted (E) using the private key (PR_A) of user A (A) to create a digital signature (D_S (A) D_i).

E(PR_A(H_D_i)) \rightarrow D_S (A) D_i \hfill (2)

(iii) A unique identity (X_{D_i}) and the time stamp (T_{(X) D_i}) of the document (D_i) is created. Unique identity (X_{D_i}) along with the digital signature (D_S (A) D_i) mentioned in equation (2) is used to generate the QR code which is embedded in the document (D_i) mentioned in equation (1) to create a Smart Documents.

SD \rightarrow SD_1 \hfill (D_i \| QR_{((X) \to D_i)} \| (X) D_i) \hfill (3)

(iv) The block (B_i) is sent to every node in the blockchain network for validation that consists of hash digest (H_D_i), unique identity (X_{D_i}), time stamp (T_{(X) D_i}) of the document (D_i) along with hash digest (H_D_{i-1}) of the previous block (H_D_{i-1}), and public key (PU) of user A (A).

B_i = (H_D_i \| H_D_{i-1} \| X_{D_i} \| T_{(X) D_i} \| PU_A) \hfill (4)

(v) Once the block (B_i) is validated based on consensus by the majority of the nodes in the blockchain network then the block (B_i) is added to the blockchain (BC_i)

BC_i = (\ldots B_{i-2} \| B_{i-1} \| B_i \| B_{i+1} \| B_{i+2} \ldots) \hfill (5)
(b) Verification of Smart Documents:

(i) Let us say a Smart Documents (SD) as shown under is received for verification:

\[ \text{SD} \rightarrow \text{SD}_k \left( D_k \ || \ \text{QR} \left( \left( (DS)_A \right) D_k \ || \ \left( X \right) D_k \right) \right) \]  

\[ \text{(6)} \]

(ii) QR code (QR) in the Smart Documents is scanned to retrieve unique identity (X) and digital signature (DS) of the Smart Documents (SD):

\[ \text{QR} \left( \left( (DS)_A \right) D_k \ || \ \left( X \right) D_k \right) \rightarrow X \]  

\[ \text{(7)} \]

\[ \text{QR} \left( \left( (DS)_A \right) D_k \ || \ \left( X \right) D_k \right) \rightarrow DS \]  

\[ \text{(8)} \]

(iii) Using the unique identity (X) of the document (D) found in equation (7) the public key (PU_A) of the user A (A) is retrieved from the block (BC) of the blockchain (BC):

\[ \text{BC} \rightarrow \left( \ldots B_{k-2} \ || \ B_{k-1} \ || \ B_k \ || \ B_{k+1} \ || \ B_{k+2} \ldots \right) \]  

\[ \text{(9)} \]

\[ B_k \left( \text{HD}_k \ || \ \text{HD}_{k-1} \ || \ X \ || \ T \ || \ \left( (X) D_k \right) \ || \ \left( PU_A \right) \right) \rightarrow PU_A \]  

\[ \text{(10)} \]

(iv) The public key (PU_A) found in equation (10) is used to decrypt(D) the digital signature (DS) found in equation (8) to get a hash digest (HD):

\[ D \left( PU_A \left( DS \right) \right) \rightarrow HD_k \]  

\[ \text{(11)} \]

(v) Successful decryption (D) of the digital signature (DS) authenticates and gives out the non-repudiation of user A (A). Simultaneously, the document (D) of the Smart Documents (SD) received in equation (6) is passed through the hash function (H) to create a hash digest (HD):

\[ \text{SD} \left( D_k \ || \ \text{QR} \left( \left( (DS)_A \right) D_k \ || \ \left( X \right) D_k \right) \right) \rightarrow D_k \]  

\[ \text{(12)} \]

\[ H(D_k) \rightarrow HD_r \]  

\[ \text{(13)} \]

(vi) If the hash digest (HD) given in equation (11) and hash digest (HD) given equation (13) are found to be the same, then it can be said that the integrity of the document is intact and thus, the document is verified.
(c) **Use of Blockchain in the proposed framework**: The blockchain (BC<sub>n</sub>) mentioned in equation (9) will also help us in verifying the integrity and authenticity using the hash digest (HD<sub>k</sub>) for a given document (D<sub>k</sub>) which is distributed and stored by all the nodes. Since the block (B<sub>j</sub>) was added to the blockchain (BC<sub>n</sub>) based on the consensus mechanism so it eliminates the need for any trustless centralised controlling authority. The record of the transactions is available publicly and can be viewed by all the participants in the blockchain network thus providing transparency of the creation of the given document (D<sub>k</sub>). Once the transaction has been added to the block it cannot be altered or deleted as the copy of these transactions is held with every node present in the blockchain network thus providing immutability.

5. **TESTING AND EVALUATION**

5.1

For testing the proposed framework, a system with the following hardware configuration was used, Intel(R) Core (TM) i7-8550 CPU, 1.80–1.99 GHz, 8 GB RAM, 64-bit Windows 10 Operating system having 1 TB of a hard disk. The tools and software used were Oracle Virtual Box 6.0, Image of Kali Linux 2018.2 vbox-i386, openssl library in Linux, QR-Code Studio 1.0, Adobe Acrobat Reader DC.

5.2

To create a Smart Documents a test case has been prepared in which a file which contains text, images, graph, word art, and smart art has been created so as to check that the proposed framework works for all type of contents in the file. Using openssl library available in Kali Linux, an X.509 digital certificate is created using the 4096 bit RSA Private key. A digital certificate so generated is then used to sign the file. In the next step, the digital certificate and a unique ID of the file are provided to the QR code generator. QR code so generated is then embedded to create a Smart Documents as shown in figure 7.
5.3 To verify the file for its integrity, authenticity, and non-repudiation the PKCS7 signature is extracted out of the digital certificate. The PKCS7 signature is then used to verify the file based on the digital certificate. As shown in figure 8, the verification for the same was successful. Then, few changes were made to the file and a new modified file was made and a similar procedure was followed to verify it. It was, however, found that the verification of the modified file failed and thus, the above procedure helps us in evaluating the correctness of the proposed framework.
5.4

To test the performance of the blockchain network, it is proposed to use Hyperledger Fabric which is an open source blockchain network. Hyperledger caliper [30] is a benchmark tool that is used to compare the performance of the blockchain in terms of transactions per second, throughput and latency. However, at this point, the testing and evaluation of the blockchain have not been carried out and the same is proposed using the Hyperledger caliper.

6. CONCLUSION

6.1

The security of information generated, shared, and stored by any source in a highly contested environment will always have issues concerning its integrity, authenticity, and availability. Since this information is very critical for the success of a mission in any military operation, a framework is required that will provide the same. The paper proposes a QR code and Digital Signature based Smart Documents using Blockchain technology for Armed Forces. These Smart Documents can ensure the integrity and authenticity of information using Digital Signatures and provide a mechanism for easy storage, access, and retrieval of documents in a transparent and auditable environment using the Blockchain technology. The proposed solution will facilitate the verification of documents both in its electronic and paper form. Thus, the complete framework will aid the Commanders at all levels in the faster decision making process to achieve their objective by giving them assurance of integrity, authenticity, and availability of information in an immutable and transparent military network.
REFERENCES


Technology for Standardization of Sensor Data from Legacy Heterogeneous Sensors in Tactical Surveillance Application for Joint Operations

Vandana¹, Sanjay Motia², Pradeep³ and Anoop Kumar Rai⁴
E-mail: ¹vandana@bel.co.in, ²sanjaymotia@bel.co.in, ³pradeep@bel.co.in, ⁴anoopkrrai@bel.co.in

Abstract—In any command and control system used for decision support, data is obtained from heterogeneous sensors, legacy sub systems as well as external systems residing at various echelons with different interfaces, formats to process information in the form of text, audio, video, image and intelligence reports gathered by recce. The processed information is disseminated to peer echelons as well as higher echelons and vice versa to get a complete tactical picture for planning and executing the offensive or defensive operations. This paper analyses the challenges involved and proposes a technology to standardize the information received from various sources after envisaging the various possible scenarios.

1. INTRODUCTION

1.1
Due to low maintenance, ruggedized operations, high efficiency and accurate detection many legacy sensors which have already lived their useful life, are still being used in real-world tactical surveillance applications in many developing countries. These sensor includes legacy radars, electro optic (EO) devices, thermal imagers and many more. Most of these sensor either have traditional RS422/232 interfaces or only a few support wired/Ethernet interface. Generally, these sensor systems communicate on the messages as defined in proprietary Interface Control Document (ICD) from original equipment (sensor) manufacturers (OEMs). Usually, these sensors systems vary in their communication interfaces, commands and types of data they sense, capture and communicate to external systems. The inherent heterogeneity in terms of OEMs[1], communication interfaces, data formats and contents of the different legacy sensors makes their integration difficult and complex, thereby making the development of higher echelon software systems complex and difficult to handle[7].

1.2
In addition, the legacy sensor systems are built on very old and outdated operating systems (with no or very little support available) which has limitations in integration with today’s consumer systems such as decision support or command and control system[8]. Some of the legacy systems even don’t output any data out of them as they are initially developed for standalone operations driven by the operators and their integration along with information sharing to any external system which was not envisaged at that time. To help in mitigating these issues, there is an utmost requirement of developing an integration utility or software technology module that acts as a bridge between the robustness and accuracy of old-age systems and novelty and dynamic operations of state of art technology driven consumer or end user systems.
1.3

Furthermore, the recent decision support command and control systems, generally expect standardized input data in a standard format like NMEA or ASCII. So it becomes very crucial for the integration software module to output standard data format for seamless system integration and data flow for necessary information sharing. The design and development requirements of sensor and system integration module, includes interfacing via interface configuration for both sensors and respective communication interface[9], sensor data collection, preprocessing, format conversion for standardization data output/ packet built from processed inputs from heterogeneous sensors and systems.

1.4

In view of the above, the purpose of this technology is to develop a mechanism of data integration from legacy sensors such as EO, thermal imagers and radars being utilized for many years for tactical surveillance application in tactical domain. The technology covers logical sensor interfacing via operator driven configuration, data collection (as text, messages, images defining information on various important physical and environmental parameters under observation) preprocessing, format conversion to standardized data format. The standard data format includes necessary information captured from the legacy sensors bundled into single data packet having standard data frame format. The standardized data format makes these sensor devices and systems accessible in a unified way making it easily integratable into any third party application such as command and control system or any tactical decision support systems.

Figure 1 depicts the block diagram of the proposed mechanism of sensor integration and data standardization.

![Figure 1: Conceptual Diagram of the Proposed Technology of Legacy Sensor Integration](image)
1.5

A generic data dissemination technology for acquisition of data, image and video has been proposed for joint operations. The technology only caters for data collection from state of art sensor interfaces but doesn’t cater data format conversion into a standardized data format[10]. In addition, it doesn’t cover the data handling from message based legacy sensors whose interface requirements have been defined in Interface Control Document (ICD). The non-standard output from sensor systems causes difficulties in interfacing as well as integration. Integration of such legacy sensors is one of the major challenge for sensor integrators where on one end there are legacy interfaces and data communication mechanism and on the other hand third party consumer software has capability only to accept data in standard encoding schemes.

The work is structured as follows:
Section 2: Challenges in integration of data.
Section 3: Technology solutions.
Section 4: Standardisation of data by format conversion.
Section 5: Features and Technology.

2. CHALLENGES

2.1

The summary of challenges and proposed solution for integration of data from legacy sensors is as follows:

2.1.1 Summary of Challenges

(a) Standalone legacy sensors with single operator use with no data output.
(b) Data flow through serial interfaces (RS422/232) making data integration and processing complex and cumbersome.
(c) Diverse communication interfaces, commands and types of data as sensor systems are from different OEMs/Vendors and have different ICDs/Integration mechanism.
(d) No mechanism to take data out from Sensor system which is standalone in nature from operation point of view[2].
(e) Non-standard output from legacy sensor system causing difficulties in integration with systems that requires standard inputs.
(f) Different encoding schemes of output data from sensor system.

2.1.2 Summary of Scope/Key Concepts in Proposed Solution

(a) Configures the sensor system and data communication interface
(b) Logical data integration from sensor system over configured communication interface.
(c) Provision for data capturing from standalone legacy sensors via text and images.
(d) Seamless data collection and command transfer over serial interfaces (RS 422/232) with error check and control.
(e) Data collection and command initiation over Ethernet interface over standard UDP/TCP communication protocols
(f) Integration of data over diverse communication interfaces, ICDs as defined by different OEMs/Vendors
(g) Data extraction form sensor systems where no mechanism to extract information out of sensor system due to system limitation. For example, sometime no mechanism is defined in some sensors systems to take data out of them due to standalone nature from operational point of view.
Data processing of text, images and message data to extract useful information for end use.

Protocol conversion and data bundling

Data packet formation into standardized data format

3. PROPOSED TECHNOLOGY

3.1

In the proposed work, a technology for data collection, pre-processing and storage is presented which collects the real-time sensor data from legacy sensors [RADAR, EO and thermal imager (TI)] operating on different legacy interfaces with proprietary interface and data communication protocols as defined by the respective OEMs. The employment of the technology not only eases the end system application development but also improves the quality of the decision support and real-time monitoring [4]. The research contributions to the proposed work are as follows:

(a) A soft mechanism (software utility) for data collection, pre-processing and format conversion into standardized data format is presented which supports the common interfaces of decades old sensors, instrument and systems.

(b) The software utility provides the uniform access primitives, which hides many details of the hardware and thus relieves the developer from dealing with them.

(c) The soft mechanism also offers the output data in a standard NMEA format for different consumers cum data analysis software, which can facilitate integration with todays’ systems.

(d) The software utility also handles sensors and systems which do not have direct accessibility or that does not have any means to output data.

(e) The soft mechanism also handles file transfer and handling for image as well as text files.

(f) The design of the integration software utility is based on the sensor interface, their data types (stream, message, files) and, interaction capability with external system.

(g) The communication interfaces between the software utility and the higher level external systems are classified into the serial, and ethernet.

(h) The communication protocols between the software utility and high layer application is based on SERIAL/UDP/TCP/IP.

(i) Once the software utility acquires all the data variables, it converts the data into a standard NMEA data format (through unit and protocol conversion) before transferring to next higher level software system. The data transferred shall contain a timestamp t which represents the sampled time, the data value of a sensor at time t, the identification of the sensor.

3.2

The technology is governed by a software utility which handles following real-world scenarios:

3.3 Scenario-1

3.3.1

The proposed technology has the capability to extract data from sensors and systems which even do not have capability to output any data. The software utility which when loaded at the decades old sensor which do not give direct access. The architecture design of the software utility is depicted in figure 2 The steps involved in data integration[9] of these systems are:
3.3.2 Software Utility at Sensor End

(a) On initialization configure itself as per the details in configuration data.

(b) Checks the health status of software applications at both ends (sensor and data consumer system). Periodic polling is used to check application health status.

(c) Validation of connection status over the configured interface. Periodic polling is used to check health status.

(d) Collects the image (as captured by operator via print screen command) of the screen.

(e) Extracts the useful information from the image file and forms a textual report of useful information.

(f) Sends both the text and image files over serial (RS232/422) interface after fragmentation of both the files into small data packets with assigned checksum, to the similar software utility on the other end (consumer software).

3.3.3 Software Utility at Consumer Software End

(a) On initialization configure itself as per the details in configuration data similar to configuration details of software at corresponding sensor end.

(b) Receives the data stream on serial interface

(c) Checks for no of data packets, packet number, missed, erroneous packets,

(d) Validates the checksum and assemble the valid data packets to form the image and text file.

(e) In case the data packet is to be corrupted, negative acknowledgement is sent back to software utility at sensor end for retransmission of valid data packet in replacement of corrupted or erroneous data packets. This iterative process continues till all the valid data packets are received by the software utility at consumer end.

(f) If the sensor and the consumer system has different geo-references, then the technology also caters for conversion of location data into geographic coordinate system which is used universally.

(g) The formatted data is stored in in local database or local memory. The data from local database and memory is extracted for formation of standard data format for usage in consumer system. Same process if utilized to take the data for sensors which do not give direct accessibility but have ethernet interface.

3.4 Scenario-2

3.4.1

The proposed technology also collects data from sensors and systems which have capability to output any data to external system. In this case no installation or porting of software utility is required at sensor end. The steps involved in data integration of these systems are:

(a) On initialization configure itself as per the details in configuration data.

(b) Receives the data stream on configured interface (serial or ethernet) using communication protocol (SERIAL/UDP/TCP)

(c) Checks for sensor type and data details (stream, messages, files)

(d) If stream or data packets of file (image/text) is received then data startup word, end word and checksum is checked.
(i) If checksum is valid, then extracts data from the data stream
(ii) no of data packets, packet number, missed, erroneous packets,
(iii) Stores the extracted data in local memory or local database
(iv) Process repeated until all the data packets gets received
(v) Assemble the valid data packets to form the data structure from stream and image/text file.
(e) If message is received, then message is processed and data is stored in local database or memory
(f) If the sensor and the consumer system has different geo-references, then the technology also caters for conversion of location data into geographic coordinate system which is used universally.
(g) The formatted data is stored in in local database or local memory. The data from local database and memory is extracted for formation of standard data format for usage in consumer system.

4. FORMAT CONVERSION INTO STANDARDIZED DATA FORMAT

4.1
After acquiring data from the sensors and systems[5], the software reorganizes the sensor data [6] and converts into the standard data format before transferring them. In the data standardization, an NMEA data frame format is designed which basically consists of start and end data attributes termed as preamble and termination bytes. The remaining part of the data frame contains three types of data, (1) Number of sensors, (2) sensor details (sensor type, sensor name, sensor number) (3) sensor data details (type of data (ASCII, Message, File), (4) Sensor Data (stream, Message), (5) Separator, (6) checksum. Table-1 describes each element of standard data format. The data transmission rate is configurable (Default data transmission rate is one second).

**Fig. 2: Class Diagram of the Proposed Technology of Legacy Sensor Data Standardization**
### Table 2: Standardized Data Format for Data from Heterogeneous Legacy Sensors

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Attribute Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>!</td>
<td>Startup byte</td>
</tr>
<tr>
<td>No of Sensors</td>
<td>Indicates no of sensors to be integrated</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Sensor ID-1</td>
<td>Sensor Identification No</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Sensor Name-1</td>
<td>Name of the Sensor</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Logical ID-1</td>
<td>Logical ID of the Sensor</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Sensor Type</td>
<td>Type of Sensor (RADAR, EO, TI)</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Output Accessibility</td>
<td>Yes(1)/No(0)</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>File Availability</td>
<td>Yes(1)/No(0)</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>File Type</td>
<td>Image(1)/Text(0)</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Sensor data type</td>
<td>Data stream(1), Message(2)</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Sensor Data Payload</td>
<td>Refer Note-1</td>
</tr>
<tr>
<td>#</td>
<td>separator</td>
</tr>
<tr>
<td>Attribute</td>
<td>Attribute Details</td>
</tr>
<tr>
<td>---------------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>0x55</td>
<td>Chunk startup byte</td>
</tr>
<tr>
<td>No of data chunks</td>
<td>Total number of small size data packets</td>
</tr>
<tr>
<td>Max chunk size</td>
<td>Max Size of chunk (200 byte) configurable</td>
</tr>
<tr>
<td>Chunk Number-1</td>
<td>Identification No of chunk</td>
</tr>
<tr>
<td>Current Chunk-1 Size</td>
<td>Size of Current Chunk</td>
</tr>
<tr>
<td>Chunk-1 Details</td>
<td>Variable</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Chunk Number-1</td>
<td>Identification No of chunk</td>
</tr>
<tr>
<td>Current Chunk-1 Size</td>
<td>Size of Current Chunk</td>
</tr>
<tr>
<td>Chunk-1 Details</td>
<td>Variable</td>
</tr>
<tr>
<td>Checksum</td>
<td>Checksum (CRC16)</td>
</tr>
<tr>
<td>0xAA</td>
<td>Termination Byte</td>
</tr>
</tbody>
</table>
Sensor Data Message (Table 2)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Attribute Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>No of Messages</td>
<td>Total number of Messages as per ICD of Sensors</td>
</tr>
<tr>
<td>Message ID-1</td>
<td>Identification Number of Message</td>
</tr>
<tr>
<td>Message-1 Type</td>
<td>Status(0), Location (1), Target (2), Characteristics(3)</td>
</tr>
<tr>
<td>Message-1 Name</td>
<td>Status Message(0), Location Message(1), Target Detection Message (2), Sensor Characteristics Message (3), Command Message</td>
</tr>
<tr>
<td>Message-1 Size</td>
<td>Variable as per Message Type</td>
</tr>
<tr>
<td>Message-1 Payload Details</td>
<td>As per Message</td>
</tr>
</tbody>
</table>

| Message ID-N               | Identification Number of Message                                    |
| Message-N Type             | Status(0), Location (1), Target (2), Characteristics(3)             |
| Message-N Name             | Status Message(0), Location Message(1), Target Detection Message (2), Sensor Characteristics Message (3), Command Message |
| Message-N Size             | Variable as per Message Type                                       |
| Message-N Payload Details  | As per Message                                                      |

5. **SALIENT FEATURES OF THE PROPOSED TECHNOLOGY**

(a) The standard packet enables interoperability between systems for joint operations.

(b) It offers a uniform interface for the data acquisition from variety of legacy sensors promoting seamless sensor and system integration. Thus different monitoring and decision support systems can share the data from the same data acquisition sensor and system.

(c) The technology developed for data standardization not only drastically speeds up the development and debugging process of the monitoring and decision support system.

(d) The technology caters variety of sensor and system interfaces (mostly legacy instruments) with multiple communication protocol (SERIAL/UDP/TCP)

(e) Handles file format (Image/Text) efficiently with optimum use of available bandwidth in wireless communication media and also supports sending of text message to central agency and vice versa
(f) Makes the real-time capturing and delivery of status, location and target information from sensors and systems possible.

(g) The technology also enhances the throughput as packet loss is minimized by handling errors via error detection and correction techniques for receiving, processing and sending the information over serial interface in wired as well as wireless communication media [3].

(h) The latency required in these safeguarding systems of land is up-to one minute and thereby met as sensors transmit at one second.

(i) This technical solution is capable of receiving data of entity which is continuously moving. It receives input from central agency to make equipment move from one location to another or to make equipment track a particular entity.

6. CONCLUSION

6.1

The technology developed acts as a bridge between legacy sensors/systems as well as higher end applications such as monitoring and decision support systems and can ease the overall system development in the light of numerous well proven, robust and efficient legacy sensor and systems. Furthermore, it introduces standardized view of collected data from diverse sensors which can facilitate their integration with current state of art monitoring and decision support systems.

REFERENCES


2. Yaw Wen Kuo, Cho Long Li, Jheng Han Jhang, Sam Lin, Design of a wireless Sensor Network Based IoT Platform for Wide Area and Heterogeneous Applications.


Private LTE Networks for Defence Critical Communications and Digital Defence 4.0

Philippe Agard*, Public Safety and Defence Segment Leader
Nokia Networks, 7th Flr., Bldg. 9A, DLF Cyber City, Gurugram-122 002, Haryana, India
E-mail: *philippe.agard@nokia.com

Abstract—Today, wireless networks play a major role in personnel mobility, ubiquitous communications and the expansion of the Industry 4.0 by enabling the exponential rise of connected objects which transmit data over the air. Armies and the Defense sector at large are following this trend and, as specific use cases here require increased control, security and resilience, private LTE has become an ideal technology for the digitalization of modern Defense organizations.

In Defense, security, availability and resilience are stringent requirements that make WiFi and public LTE too weak in numerous situations. A direct control via Private LTE allows organizations to accustom the network to their own security policy, resources allocation, etc… Private LTE has therefore become a very attractive option for Defense organizations and this article discusses its benefits for the main use cases of interest and the relevant deployment models applicable.

1. INTRODUCTION

1.1
Among the many reasons why private LTE fits well the specific requirement of Defense organization, the following are worth being highlighted:

1.2 Better Control

1.2.1
With a direct thumb on their own network infrastructure, a Defense organization gets a better control on security and network engineering.

1.2.2
Controlling the subscribers database and roaming policies allows the network administrator to regulate and quickly adjust users access according to custom strategies, whilst a direct access to the infrastructure permits to monitor the protection (nodes authentication, traffic encryption) of the User, Control and Management planes, design security network architecture and deploy specific equipment (firewalls, military-grade encrptors, etc..) accordingly.

1.2.3
LTE is by design a standard that allows a configurable Quality of Service (QoS) where the LTE Quality Class Identifiers (QCl) are mapped onto pre-configurable sets of nodal parameters at multiple protocol layers; this allows the network administrator to assign QoS characteristics (scheduling priority, packet delay, packet error loss rate, etc...) adapted to specific services/applications.

1.3 Coverage & Capacity

1.3.1
As LTE technology was maturing over the past 10 years, manufacturers’ equipment capabilities as regards compactness and radio
performance have improved, opening brand new possibilities in terms of set up and use cases for Defense players. Radio base stations are now available in a wide range of form factors and can operate in tens of different frequency bands, offering radio coverage from 10's to hundreds of meters with pico-eNBs, up to more than 100 kms range with macro eNBs in specific cases. With data throughputs commonly in the range of 100's of Mb/s, LTE has become the mobile broadband technology of choice for mobile use cases requiring high bandwidth such as video applications. Furthermore, its low latency which can be as low as 10ms, enables true real-time applications which are essential to military forces in many cases (eg for voice PTT/PTV applications) and will be even more when considering AR/VR-based wireless applications.

1.3.2
The above are general characteristics that apply as well to LTE networks deployed by public operators, but a private network allows the Defense organization to optimize the design and deployment accordingly to their specific requirements, and better control the total cost of ownership (TCO) of the network.

2. DEFENSE MAIN USE CASES

2.1 National and Bases Coverage

2.1.1
Digital Transformation of Defense Forces often starts with providing advanced ICT technologies and enabling ubiquitous, secured broadband communication mobility on the Military compounds to reach the next level of efficiency in the processes and productivity. Ability to do maintenance accessing manuals on tablets at bottom of aircraft, ability to connect ships in the dock via radio connection ability to improve Perimeter protection by deploying rapidly several sensors LTE connected etc.,

2.1.2
As military bases are generally large areas, a wide zone must be covered and LTE is ideally suited for both the coverage (indoor or outdoor) and the capacity issues. LTE being on licensed spectrum offers more guarantee against interferences.
2.2 Naval LTE

2.2.1

The concept of using LTE for mobile broadband communications inside military bases can be further extended to provide LTE coverage on vessels when they are on mission and sailing far away from their home base. With a compact equipment featuring a complete LTE network and embarked on a ship, an autonomous LTE bubble can be created to ensure broadband communications on a vessel’s deck, inside the ship as well as around the ship. Adjusting radio coverage accordingly, naval groups can benefit from LTE coverage as provided by the master ship for their own communications or for ship to ship communications, using almost standard UEs. Similarly, communications with low speed and low altitude aircrafts, helicopters and drones can be transmitted over such an LTE bubble, significantly augmenting the projection capability of naval forces.

![Diagram of naval LTE](image)

**Fig. 2**

2.3 Tactical LTE

2.3.1

Military forces operating on the ground need to enable more advanced situational awareness. Extreme mobility, low weight and high compactness are qualities required when dealing with tactical use cases. Transportable equipment is in most cases enough to enable the setup of temporary camps or for at-the-halt data, voice and video communications.

2.3.2

Light LTE solution do now emerge to address moving LTE tactical bubble or man-carried LTE bubble such as in a backpack. There is no one size fits all solution, but the generally the use cases are such that the smaller the size needed, the lower the requirements in terms of coverage and capacity. LTE technology compactness, use of virtualization, makes it possible to package equipment in a medium-sized rack hardened to operate in tough conditions small
enough to fit into vehicles, with the option of using telescoping masts for extending radio coverage at the halt. Combining Pico or micro eNBs with compact servers running LTE core allows to get very small configurations that can be hand-carried or even fit within a backpack. Such setups can provide several 100’s of meters coverage for 10’s to 100’s of LTE users depending on the applications and characteristics of the equipment. These tactical bubbles can be connected to remote military assets via satellite or microwave backhaul in an ad-hoc manner, as use case dictates.

2.4 IoT & Defense 4.0

2.4.1
Since a few years the number of connected objects has grown exponentially to reach billions of devices, and the scope of Internet of Things (IoT) and analytics applications has expanded drastically in all sectors, creating new business opportunities referred to as the Industry 4.0.
2.4.2
In the Defense 4.0 IoT spawns from back-office and logistic applications like those in other sectors such as assets, wastes, energy, management and predictive maintenance, to tactical ones like collaborative assisted combat, swarm robots monitoring, unmanned vehicles remote control, etc...

2.4.3
Smart bases perfectly illustrate the Defense 4.0 trend; they integrate all digital applications that improve the performance, efficiency, and convenience of the managed assets and services of military premises and operations.

2.4.4
The release 13 of the LTE standard introduced narrowband mechanisms optimizing IoT, namely LTE-M/eMTC and NB-IoT, and releases 14 and beyond bring additional capabilities for large-scale IoT and further IoT management optimizations. All in all, the LTE all-IP architecture makes it perfectly suited for IoT and can scale from narrowband highly efficient power consumption IoT applications up to ultra-high data rates for high-performance and mass IoT services.

3. SPECTRUM CONSIDERATION

3.1
Originally, LTE is a technology designed to operate in licensed spectrum. As was the case with the previous mobile technologies (GSM, UMTS, CDMA), it has been deployed over the years by mobile service operators (MSPs) who have acquired spectrum licenses by their local regulator. An inherent benefit of this approach is the superior quality of service that can be expected from the use of dedicated and
unshared chunks of spectrum. Most defense players have spectrum that does match an existing standardized 3GPP band. In few cases though, it may not be standard spectrum and the corresponding equipment ecosystem may not exist yet. Based on the consideration that spectrum is a scarce resource, that LTE adoption’s exponential growth is further fueling the need for spectrum, and that short-range wireless technologies operating in unlicensed spectrum have tremendous success too, the idea of operating LTE in unlicensed bands has emerged. Different modes exist (LTE-U/LAA-eLAA/LWA-eLWA) to combine unlicensed with licensed spectrum and have been deployed by various operators around the globe to bring more capacity to their LTE service. Multe Fire technology has been developed to operate LTE entirely in an unlicensed band, opening new perspectives to players not owning any spectrum or for some specific use cases as for example Navy needed to operate their LTE network while in a foreign harbor. Multe Fire radio equipment is progressively becoming available from the main LTE manufacturers.

4. DEPLOYMENT MODELS

4.1
Public Safety and Defense forces have at least one thing in common: they need reliable and resilient communications systems. The approach might be different though with the growing interest of public safety players in leveraging existing homeland MSP networks, in a try to secure access to LTE anywhere they go while also optimizing their budgets (RAN sharing with owned PS core, or fully relying on MSP networks). Most often complementing this capability with their own LTE deployable gear to cope with critical situations (disasters or overload of legacy operated networks).
4.2
Defense players have even more stringent requirements as regarding privacy and confidentiality. Because communication links to the external world create by nature a risk for security (e.g., data breaches, eavesdropping or hacking), private LTE networks have become their favorite approach.

4.3
Solutions like Nokia NDAC (Nokia Digital Automation Cloud) have been designed to address such pLTE configurations more effectively. Simple to deploy and operate, NDAC allows to mix a full range of radio eNBs with various LTE core (ePC) configurations running on compact servers (DA edge) together with applications, to best serve the target use case. pLTE networks can be small tactical bubbles, LTE networks for temporary camps or a large LTE network for the coverage of a military base. All pLTE networks can be coordinated and configured via remote backhaul link to a common data center located in the cloud and fully owned and managed by defense authorities. When configured, all pLTE networks are fully autonomous and data communications remain within the pLTE created network, thus ensuring the utmost security and confidentiality during all the duration of a mission.

5. CONCLUSION

5.1
LTE is gaining grounds as a future proof Mission Critical Broadband solution in Public Safety, Homeland Security and Defense use cases. The standardization by 3GPP started in 2013 with key features like Mission Critical Services has enabled roll outs for fixed territorial networks scenarios like national coverage, and deployable/transportable versions are now in use in some armies for “tactical” broadband services complementing proprietary military radio. 5G availability makes a 3GPP based solution even more attractive, with ability to plan later updates and address next stage of extreme latency requirements (<1ms), extreme Mobile Broadband (~Gbs or more depending on spectrum available) as well as enabling to cater for very large number of IOT devices.

REFERENCES
2. https://www.3gpp.org/
Communication as a Decisive Catalyst for Jointness

Lt Col Prabhmeet Singh Manik, SM

Abstract—There is growing understanding among the military planners that human warfare is entering the stage of Information Warfare (IW). The concept of jointness among various organisations has become widespread in recent decades in Defense and civilian establishments and represents change in organizations' modes of activity in complex and challenging environments. Jointness occurs in environments characterized by networks, that is, by numerous connections between the various establishments and organizations. Communication plays an important and vital role for jointness among various organizations and is a decisive catalyst to produce an effective response to the threats and challenges in all present and future warfares.

1. INTRODUCTION

1.1
The Revolution in Military Affairs mainly to the technological and operational concepts has resulted in Militaries of major countries to respond and identify latest technologies to be incorporated in its study. RMA has identified rapid development in high technology with Information Technology (IT) at its core as the means to bring about revolutionary changes in the military field as a strategic and operational necessity to meet the challenge. There is growing understanding among the military planners that human warfare is entering the stage of Information Warfare (IW). The concept of jointness among various organisations has become widespread in recent decades in Defense and civilian establishments and represents change in organizations' modes of activity in complex and challenging environments. Jointness signifies activity or an organisation in which elements of more than one service participates. Jointness occurs in environments characterized by networks, that is, by numerous connections between the various establishments and organizations. Communication plays an important and vital role for jointness among various organisations and is a decisive catalyst to produce an effective response to the threats and challenges in all present and future warfares. Needless to emphasis that Revolution in Military Affairs (RMA) cannot occur substantively unless it is accompanied by a joint and integrated approach backed by a vigorous and robust communication plan.

2. AIM

2.1
The aim of this paper is to study the impact of Communication as a Decisive Catalyst for Jointness in Military Operations.

3. SCOPE

3.1
The scope of this study is covered in following four parts:
(a) Operational view of Jointness Impacting Communications.
(b) Reforms in Military Affairs & Communication for Joint Operations.
(c) Technologies and Aspects Enabling Jointness.
(d) The Joint Spectrum: From Non-Joint to Joint Armed Forces.
4. OPERATIONAL VIEW OF JOINTNESS IMPACTING COMMUNICATIONS

4.1
The concept of jointness, which has become widespread in recent decades in Defense, intelligence and civilian establishments, represents change in organizations’ modes of activity in complex and challenging environments. Jointness occurs in environments characterized by networks, that is, by numerous connections between the various actors. Jointness is different from Cooperation wherein later preserves the distinct organizational frameworks, their powers and areas of responsibility. Jointness, however, is a process of fusion that creates new organizational configurations and a synergy that is greater than the sum of all the existing capabilities. The word “joint” signifies any activity or an organisation in which elements of more than one service participates. Jointness was a term coined by the US armed forces to describe inter service cooperation. It’s a combination of at least two arms in the military coordinated towards one common goal. To coordinate among various arms and organizations, communication plays an important catalyst for jointness.

4.2
Fundamentally as the nature of warfare evolves, jointness is about efficiency and optimal utilisation of resources and that will dictate various requirements in terms of optimisation of force structures, acquisition processes, training methodologies and research & development on strategic capabilities is strong. If that is the governing factors then the starting point of a joint doctrine should be based on operational philosophy. The nature of war in India is different from any other nation because of the simple difference of terrain. Hence, India requires a different warfare approach altogether. A time frame needs to be indicated on where to invest. Military needs to articulate its operational philosophy through these documents more explicitly and bring about forceful jointness. The importance of technological changes that are necessary in warfare are required to be included in the Joint Doctrine of Warfare wherein Information Technology and Modern Communication Techniques incorporated in all three services plays a critical role as a decisive catalyst for Jointness in warfare.

4.3 Communication as Catalyst for Jointness.
The future war systems are likely to be dominated by unmanned systems in which Artificial Intelligence (AI) can provide multiple options for military applications for a strategic, operational and tactical level planning in many of the functions such as Intelligent and autonomous unmanned systems, data analysis, information processing and intelligence analysis, training war gaming, etc. Three principles of war, namely, Inter-Service cooperation, Economy of Effort and Unity in command and control(C2) would continue to be key imperatives of knowledge age warfare. The campaigns of Gulf War I and II has indicated that greater degree of jointness and integration achieved by the American and coalition forces was a key battle winning factor. Further, improved ISR capabilities, networked command and control elements with long-range precision strikes are best exploited by a joint and integrated effort of the three Services. Whether it is Network-Centric Warfare (NCW), Effect-Based Operations (EBO) or information warfare (IW), the synergies at operational level are best obtained by a unified effort. Needless to emphasis that Revolution in Military Affairs (RMA) cannot occur substantively unless it is accompanied by
a joint and integrated approach backed up by a robust communication plan with integrated network among various organizations.

4.4

The evolution of the joint doctrine could not have been but influenced by the fundamental elements of RMA. RMA emphasize the need for jointness, even though in practice, the required levels of jointness are lacking. Further, comparatively speaking, RMA seems to have advanced in technology in services like Indian Air Force (IAF) and Indian Navy (IN) as compared to the Indian Army (IA).

5. REFORMS IN MILITARY AFFAIRS AND COMMUNICATION FOR JOINT OPERATIONS

5.1

Militaries of major states are responding to the Revolution in Military Affairs (RMA) debate, mainly to the technological and operational concepts propounded by the US. There is growing understanding among the military planners that human warfare is entering the stage of Information Warfare (IW). The essence of this shift is provided by the revolution in information technology in the field of warfare backed by a robust communication setup.

5.2

Features of Revolution in Military Affairs. RMA is not only an important military, but also a political and strategic tool for global and regional security policies of the future. RMA has five distinctive features.

(a) First, weapons and equipment have become more intelligent oriented, where in precision guided long distance attacks are increasingly playing a critical role in operations as main form of attack.

(b) The second perspective is that the RMA has allowed force structures and systems to become more streamlined. This has been possible through rightsizing and readjusting force structures leading to force optimization with stronger combat capabilities.

(c) Third, a consequent result of above has been automation of command and control (C2) systems, which have incrementally moved from Command, Control, Communication and Intelligence (C3I), to Command, Control, Communications, Computers and Intelligence (C4I), Command, Control, Communication and Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and now Command, Control, Communication and Computers, Intelligence, Information, Surveillance and Reconnaissance (C4ISR) in order to meet the demand for real time, robust, reliable and efficient command and control systems.

(d) Fourth this has led to spatial expansion of warfare, from traditional three dimensions, i.e., land, sea, and air, to five dimensional that includes in addition, the spatial and electromagnetic dimensions. Implication of above is that anybody who controls the information will gain the initiative in high tech battlefield.

(e) Finally, and most importantly, operations are becoming more system-oriented requiring not only a high degree of system integration but the integrated application of power in all five dimensions leading to warfare being transformed into completed operations of system versus systems. This is increasingly impacting on the need for integration and jointness.
5.3 Jointmanship & Integration Among Agencies. It is in this fast changing and emerging technological environment that India has to come up with a reasonable response to the latest RMA. The underlying perception in India is that response of necessity to the RMA debate will be structured taking into account not only the changing global military trends but also its regional security environment. The fact that given close collusive relationship with China we will have to incrementally deal with technologically advanced military Pakistani military with improved information, surveillance, reconnaissance (ISR) capabilities, networked command and control elements with long range precision fires and greater degree of system integration. In such a milieu, jointmanship and integration among the Indian Armed Forces and other defence support agencies would be the two major leitmotifs of RMA under Indian conditions to meet the challenges to our security.

5.4 Need of Joint Efforts. Gaining of information and converting it into intelligence is fundamental to good planning and success in operations. The long-range precision firepower of modern weapon platforms would be of no use without information and intelligence. In fact instruments of military power derive their power from their ISR assets; without these eyes and ears they would be powerless. Attaining information superiority has become one of the most important objectives to be achieved in the era of knowledge age warfare. The concept of information superiority is somewhat analogous to similar concepts of air superiority, superiority at sea or in space. This is because proper use of information is as lethal as other kinds of power. Further, concept of information superiority leads us to attainment of decision superiority. Information operations are increasingly being considered as important as sea, land and air operations. The Information Operations (IO) could vary from physical destruction to psychological operations to computer network defense. Well conducted joint information operations with new RMA technologies, improved organizations and doctrine would greatly contribute to a successful and decisive outcome.

6. TECHNOLOGIES AND ASPECTS ENABLING JOINTNESS

6.1 The benefit of the development of technologies enabling joint military activities is that such a technology is likely to provide a mechanism for armed forces to interact and reach a deeper understanding of the nature of jointness for its importance and implementation. From this deeper understanding, guidance may be derived to enable the more effective conduct of joint military activities. In the contemporary military context joint is defined as ‘activities, operations and organizations in which elements of at least two services participate’. The key word in this definition is ‘services’, which refers to armies, navies, air forces and other paramilitary organizations including CRPF, ITBP, Coast Guards, etc. The definition of joint is service-centric and is not based on environmental mediums or domains (land, sea, air, space, etc.), therefore it determines that jointness is institutional, being based on cooperation between services regardless of whether their activities are taking place in a single domain or in many domains.
6.2
Accordingly, the term ‘joint military activities’ include joint military campaigns and operations, in both warlike and non-warlike conditions. These endeavours include the establishment and perpetuation of peacetime joint organisational structures within an armed force, the conduct of joint professional military education and training courses and the production of joint doctrine.

6.3
The Four Aspects of Jointness. The four aspects of jointness are the operational, organisational, educational and doctrinal aspects.

(a) Operational. The operational aspect is the aspect of jointness concerned directly with the conduct of campaigns and operations involving more than one service. When armies, navies and air forces have traditionally worked together it has generally been in the pursuit of campaign or operational objectives. Such cooperation has traditionally been limited to ad hoc and short term arrangements driven by operational imperatives, and joint command and control arrangements have usually been established from scratch with the onset of each new campaign or operation.

(b) Organisational. The second aspect of jointness is the organisational aspect, which involves the establishment of joint organisational structures that are not directly operational. This aspect has a much more recent lineage than the operational aspect and most joint reforms that could be assessed as falling under the remit of this aspect have occurred. Generally these reforms have been achieved by integrating, to various extents, formerly separate elements of each of the services. Often organisational integration has occurred in areas where there had previously been duplication within different services – logistics, training and personnel agencies are typical areas where joint organisational structures have been established. The integration of elements of the higher command arrangements of each service has also occurred in some militaries as an additional way to develop a more cohesive joint command structure. The key difference between the operational and organisational aspects of jointness is that the latter aspect is not directly operational, even though joint organisational reforms frequently have indirect implications for the conduct of campaigns and operations. For the purposes of subsequent analysis, the line between the operational and organisational aspects of jointness is drawn between forces conducting campaigns and operations, and declared ‘operational headquarters’.

(c) Educational. The third aspect of jointness is educational. To cultivate fledgling joint cultures, the establishment of joint military education institutions has typically accompanied the move to jointness. This is especially the case regarding mid-level and senior officer education. Sometimes joint education institutions have been established by amalgamating previously separate single service institutions. The Joint Service Command and Staff College opened by the British armed forces in 1997 is a good example of such an amalgamation. During the early 1990s joint institutions were given an expanded role and measures were taken to encourage members of each service to enrol in their courses. Additional reforms were also
implemented to encourage single service educational institutions to change their curriculums to include a greater focus on the joint components of operations. All of these reforms are elements of the educational aspect of jointness.

(d) **Doctrinal.** The doctrinal aspect involves the development and proliferation of joint doctrine, something that occurred in most Western militaries from the early 1990s. Due to the prominent operational focus that characterised post-Gulf War jointness, joint operational doctrine has been (and continues to be) the most prominent type of joint doctrine, with tactical doctrine usually remaining within the purview of single services. Often, the production of doctrine itself has coincided with the establishment of a joint doctrine development centre, either as a separate organisation or as part of an existing joint organization.

7. **THE JOINT SPECTRUM: FROM NON-JOINT TO JOINT ARMED FORCES**

7.1 Considering jointness using the four aspects—operational, organisational, educational and doctrinal—enables a determination to be made as to what constitutes a fully-joint military, a partly-joint military and a non-joint military. If each aspect is imagined on a spectrum, the absence of each aspect from an armed force would be at one end and the maximum possible progression towards achieving each aspect would be at the other. This theoretical maximum is just before the point of integration—the point at which individual services cease to exist and are replaced by a single, amalgamated service that is responsible for all operations in all domains. Figure below shows this spectrum, and the relative position and characteristics of a ‘non-joint’ force and a ‘very joint’ force. Armed forces that could be described in a similar way to the description given at the very joint end of the spectrum could be said to be ‘more joint’ than those that could be better described in a similar way to the description given at the non-joint end of the spectrum.

![Image](https://via.placeholder.com/150)

**Fig. 1: The Aspects of Jointness Imagined as a Spectrum, Showing the Relative Position and Characteristics of a Non-joint Force and a Joint Force**
The descriptions of the non-joint force and the very joint force highlight that the very joint force has several advantages over the non-joint force in terms of enhanced economies of scale while reducing organisational costs, and creating a 'joint language' through education and doctrine that perpetuates and enhances a culture of joint operational success over the longer term. Furthermore, by applying the four aspects and the spectrum itself, one can begin to evaluate the jointness or otherwise of a country's armed forces.

8. CONCLUSION

8.1

As operations during the last century have shown, Western militaries are more effective when their services achieve high levels of joint cooperation. The development of a theory of joint military activities is therefore important because such a theory is likely to provide a mechanism for these armed forces to reach a deeper understanding of the nature of jointness, why it is important and how to implement it. From this deeper understanding guidance may in turn be derived to enable the more effective conduct of future joint military activities. Yet despite ongoing and significant joint reforms within most Western militaries since the late 1980s, and the conduct of detailed historical studies of joint military operations, joint military activities theory has remained in an embryonic state. Each service exists to fight and win in its own distinct domain; even though there are several points where these domains and therefore the operational requirements of each service overlap. The aim of jointness ought to be to maximize the chances of success by fostering cooperation, creating efficiencies and capturing then implementing inter-service lessons learned. To coordinate among various arms and organizations, communication plays an important catalyst for jointness.

REFERENCES

3. The Four Aspects of Joint- A Model for Comparatively Evaluating the Extent of Jointness in Armed Forces
4. www.idsa.in – RMA and Jointness by Institute of Defence studies and Analysis.
Machine Type Communication & Internet of Everything (IoE)

Col Rajesh Kapoor

Abstract—This paper provides an overview of the development and possible use-case scenarios of the new generation of mobile communication systems known as Next Generation Mobile Network (NGMN). 5G will become a chronology platform that will enable the development of new applications, business models, industries, such as massive machine-type communications. This will be possible primarily through the creation of acceptable ecosystem that could provide a massive machine-type communication using a single platform based on the Internet of Things (IoT) concept. NGMN enables the integration of all so far known and used machine-type communications, creating an environment of smart cities and a fully networked society under the new concept of Internet of Everything (IoE). However, such network also poses specific performance requirements reflected through higher transmission speeds, higher data volumes, reduced energy consumption, higher quality of service and growth in the number of services and users of currently deployed mobile generation.

1. Introduction

1.1 Nowadays, mobile communications have a significant impact on the society and are an important factor in economic development and computerization of society. After a number of generations and the current commercialization of 4G mobile communication systems (MCS) it is expected that the upcoming 5G is going to be operable by 2020. Up to this period, 5G is emerging as one of the main fields of research and development.

1.2 The goal is to consolidate all so far known and used machine-type communications (MTC, Machine Type Communication) through a single infrastructure. MTC technology is based on the idea that machines have a growing value proportional to the number of the networked units. This would result in the concept of IoE and the possibility of creating a smart cities environment and a fully networked society by simple increasing the number of networked machines. Currently, total number of all existing networked machines is hundreds of millions, and the annual growth rate is around 25%. As a result, it is expected that by 2020 the total number of networked machines (equipment, vehicles, goods, etc.) will reach 50 billion. Therefore, network operators will be able to expand their business activities, service portfolios and increase revenues. This technology, combined with the existing ones, has a high potential for the development of future applications.

2. 5G Mobile Communication Systems

2.1 With every new MCS generation, it was possible to experience two times higher speeds of data transfer than it was in the previous generation. In NGMN system, i.e. 5G MCS, one of the main requirements are the increase of data speeds
and capacity with the significant reduction of latency level. The integration of new services and applications is just as important as increasing the speed of data transfer and/or reducing the level of latency. 5G will be the MCS that uses its architecture and functionalities to enable the full implementation of services based on the IoT concept. This will result with a completely new communications between different types of machines (M2M, D2D, V2V, etc.) regardless of whether they're mobile, far apart or interconnected with different IC access technologies.

2.2

With the advent of new services and the increase of the number of terminal devices, 5G MCS will increase the range of access requests for a mobile connection to the Internet network (MBB, Mobile Broadband). Required transmission speeds vary based on the volume of the transferable data. The range starts from a very low level for sensor systems to very high level for the transfer of Ultra High Definition (UHD) video files. These requirements are reflected in the expected level of latency that will have to be low, as for security applications (emergency services, e-call about a car accident, alarm systems e-maintenance, etc.). However, there will also be services and applications that will be latency agnostic. In addition, the size of the packets will vary from small to large, depending whether it's a smartphone applications or file transfer application, respectively.

2.3

MCS 5G will enable ubiquitous provisioning of access to a wide array of services and software solutions. As a result, this will have an impact on daily routines, thus allowing continuous progress of the overall society with a significant reduction in energy consumption.

3. PERSPECTIVES TOWARDS MASSIVE MACHINE-TYPE COMMUNICATIONS AND 5G

3.1

5G MCS will enable a complete implementation of the IoT concept, along with the advance of all machine-type communications through a single infrastructure. Although most of the applications (such as M2M) transmit a small volume of data between end-devices it is predicted that a number of these new end-devices in the next few years will reach up to 50 billion. As a result, this will make maintenance and planning of today’s telecommunications networks expensive and complicated. During the same period, an increase in the number of terminal devices will increase the volume of generated data traffic up to ten times.

4. INTERNET OF THINGS (IoT)

4.1

IoT is the concept of the information and communication network, where objects (“things”) from diverse environments are mutual connected into a single large-scale network based on the Internet Protocol (IP). As a result, all these connected objects are part of a single converged ecosystem. The IoT is the basis for the development of smart environments such as smart homes, roads, factories, cities, etc.

4.2

IoT consists of smart machines interacting with other machines, objects, things, environment and infrastructure. Therefore, M2M communication it's often associated with MTC IoT concept, which is the integral part of today's IoT concept. The common characteristic of IoT and M2M concepts is the remote device access. IoT connects the computer with the
things (machines, devices, sensors, products, etc.), systems (business applications, support systems, analytical systems, data warehouses, control systems, etc.), and people (customers, employees, partners and customers).

4.3

IoT usually integrates the sensor data with analytics and business applications to improve productivity, service, and increase production and market share. Some of the main challenges that accompany the implementation of the IoT concept include security, privacy and trust, managing heterogeneity, limited network capacity, managing large amounts of information and processing large amounts of data in order to provide useful information / services and enable the efficient regulatory policy in the field of IoT.

5. INTERNET OF EVERYTHING (IoE)

5.1

In contrast to IoT, IoE includes interconnection of people, objects, things, data and processes. IoT will reach its full potential during the next five years. In fact, IoT concept is a transitional technology. On the other hand, IoE concept encompasses a number of technologies including the IoT as a transitional technology.

5.2

The usefulness of IoE will result from the impact obtained by interconnecting people, processes, and data over IP network. IoE concept will create new opportunities for providing services to various individuals, organizations, communities and countries.

5.3

There is extraordinary potential of the IoE concept. 99.4% of physical objects that will one day be a part of the IoE concept aren’t currently interconnected. Not only that these objects (things) do not make the connection, but they aren’t even a part of the IoT world. This is primarily because there are no such services that would result with the interconnection of these devices. Connection of the objects will most commonly be performed through 5G MCS with the use of full communication functionality of machines such as the MMC, People to Machine communications (P2M), V2V, direct D2D (dD2D), etc.

6. MASSIVE MACHINE-TYPE COMMUNICATION

6.1

Through the IoE concept, MMC communication will enable the connection of tens of billions of IP-based devices through 5G MCS. For example, 5G will be a systematic part of the Smart Cities in which 5G services and applications will have an impact on smart networked households, smart/intelligent vehicles, tele surgery, fun, and time-critical applications that require an immediate reaction.

6.2

MMC concept includes a set of radio ICT and techniques, thus enabling the expected growth rate in the number of terminal devices and related services and applications. These access technologies are divided into three types:

(a) Direct access.

(b) Terminal devices connect and communicate via direct access.
7. DIRECT DEVICE TO DEVICE COMMUNICATION

7.1
The MMC communication and the supporting IoT / IoE services provided via 5G platform will tend toward the creation of a fully networked and connected society. In a fully connected ecosystem enabled by 5G, the important role will play the ability to connect objects via D2D, i.e. dD2D technology. D2D communication is implemented within the 4G MCS but it’s not widely operable, mainly because of its still limiting performance (level of latency, capacity, data rate, the level of confidence, etc). Consequently, D2D will not become a part of everyday operable technologies primarily because due to these limitations when compared with its direct competitor - V2V solutions based on VANET (Vehicular Ad-Hoc Networks) technology.

7.2
Although the VANET solutions have their disadvantages, they are developed for the specific environment and their usability in V2V communication is currently more prominent. However, the concept of NGMN and earlier NGN (Next Generation Network) system are designed for all-IP communication via single infrastructure. This will result with the convergence between different access and transmission technologies. Unlike the original D2D concept, dD2D will allow the planning and implementation of V2V communication within the IoE ecosystem. With the development and implementation of 5G, several V2V requirements will be met, such as low latency of 1ms, default 99.999% reliability of communications, high availability and dependability and low failure rates.

8. CONCLUSION

8.1
The main objective of this paper was to present an insight into future developments, possible implementation and key features of the massive machine-type communication & Internet of Everything (IoE) by introducing 5G. It is expected that in the next five years, mobile networks are going to experience a significant change compared to the current state. MTC technologies such as M2M, D2D and V2V are becoming a reality and an everyday need through the concept of IoT. Communication of all these things through the IoT concept allows them to communicate directly with and without human intervention. IoE concept will bring a significant change for the society. It will change the way people live and contribute to the higher quality of life.

REFERENCES
Joint Framework for Integrating Disparate Security Solutions

Col Munish Tuli and Lt Col Aashish Joon

Abstract—Presently all three services have deployed their own network security solutions on respective captive data networks. These security solutions are from different OEMs and therefore integrating them in a joint tri-services network environment is a challenging task. In this paper, we have analysed various challenges in integrating disparate security solutions include SIEM, IAM, PKI, DC, Patch Management and Anti-Malware and proposed a joint security framework for integrated tri-services network.

1. INTRODUCTION

1.1

Today all three services have established their own SOCs with disparate network security solutions on their captive data networks. Each service has deployed diversified security solutions of SIEM, IAM, PKI, Domain Controllers, Patch Management and Anti-Malware to strengthen cyber security posture of its data network. Since, these security solutions are from different OEMs, amalgamation of varied security solutions forms a formidable task. Therefore, there is a need to formulate a joint cyber security framework to achieve an integrated tri-services network environment.

2. INTEGRATION OF SECURITY SOLUTIONS: CHALLENGES

2.1 Different OEMs

2.1.1

Different vendors have been contracted by each service to deploy security solutions of IAM, SIEM, PKI, Domain Controller, Patch Management and Anti-Malware. Therefore, provision of interoperability between solutions of all three services was not initially conceived.

2.2 Different Policies

2.2.1

All three services have different information security policies and to achieve security cohesiveness aligning them towards a common objective needs to be carefully planned. Therefore, standardization of security policies is essential while integrating security solutions.

2.3 Different Use Case

2.3.1

All three services have different operating environments and accordingly security analysts have defined specific use cases for each service while implementing security solutions.

3. JOINT FRAMEWORK FOR INTEGRATING SECURITY SOLUTIONS

3.1

In this section we will analyse security solutions deployed by the three services and propose a joint security framework in an integrated tri-services network environment.
3.2 Security Information and Event Management (SIEM)

3.2.1
SIEM aggregates logs and events data from various security and networking devices and correlates them to provide near real time detection, reporting and monitoring of security threats in a network. Since SIEM solutions of the three services have been implemented separately, it is proposed to establish a Unified SOC wherein outputs from SIEMs of three services will be integrated to provide security monitoring at the tri-services level. To achieve Unified SOC would involve overcoming technical challenges in integrating SIEM solutions of different OEMs. Though partial integration may be feasible by integrating SIEM solutions of same OEMs to achieve a distributed SIEM architecture, full integration may not be feasible at SIEM level.

3.2.2 Security Orchestration Automation and Response (SOAR)

3.2.2.1
SOAR platforms enhance response capabilities of SIEM. SIEM identifies potential anomalous activities and generates corresponding alerts. But SIEM needs regular tuning to understand and differentiate between anomalous and normal activity thus considerable amount of time is utilized in making the tool work intelligently. Therefore, SIEM solution alone is not effective and requires support of another technology. In order to establish an efficient Unified SOC, it is proposed to integrate SOAR with SIEM solution. In SOAR platform, security alerts can be automatically responded to with all the tools and technologies needed are seamlessly orchestrated together to take appropriate response steps and actions against various cyber threats. This ensures all alerts are responded to while freeing up valuable analyst time. It is recommended that SOAR solution be layered on top of the SIEM solutions of respective services. The SOAR platform at the tri-services level will manage incident response process to each alert generated by SIEMs of each service to create a more robust, efficient and responsive Unified SOC.

3.3 Public Key Cryptography (PKI)

3.3.1
PKI is an Asymmetric Key Cryptography framework that is responsible for issue, maintenance and revocation of public key certificates over the network thereby providing confidentiality, authentication, integrity and non-repudiation services to identities of individuals, organizations and computer systems operating in a network.

3.3.2
In a strict CA hierarchy all trust emanates from a common root CA. That is, the root CA is the trust anchor for all relying parties within that domain. Although subordinate CAs may be deployed, relying parties will not rely on any certificates issued by a subordinate CA unless a valid certificate path can be traced back to the root CA. A strict hierarchy is also characterized by the fact that a subordinate CA will have one, and only one, superior. Further, subordinate CAs are not permitted to have their own self-signed certificates and only the root CA has a self-signed certificate. PKI server logs are collected by SIEM to analyse usage of Digital Signature Certificate (DSC) token, unresolved OCSP requests etc.
3.3.3
Each service has already implemented Certification Authorities (CAs) in their respective networks with large footprints of entities using digital certificates. One service can become sub-CA under root CA of other service or migrate to a CCA certified legal CA. If all three CAs are certified by the CCA, there will be a strict hierarchy amongst all the certificates generated by respective CAs as the certificates can be traced back up to the CCA. However, checking for the revocation status of the certificate will still have to be diligently planned. In the joint network environment, there will be traffic flow for request and response messages of Online Status Check Protocol (OCSP) for checking certificate status.

3.3.4
Service specific applications will send OCSP requests to its respective OCSP server (based on OCSP URL given in user digital certificate) which responds to the application with the certificate status. Tri-services applications will send requests to the concerned user service OCSP server, which responds with certificate status to the application. Therefore, a tri-services application will receive OCSP response from all three services OCSP servers depending upon the user whose certificate status needs to be verified before granting him access to the application.

3.4 Identity and Access Management (IAM)

3.4.1
IAM plays a vital role in deciding access to various resources such as applications and services by the users. Centralized identity with federated access management is a standard architecture for IAM deployment. IAM provides four functionalities of identity verification, authentication, authorisation and accountability. IAM logs are collected by SIEM to verify privilege level assigned to users, identify and analyse auto – deactivation of user accounts and analyse Single Sign On (SSO) events denied access.

3.4.2
Interoperability of IAM solutions from different OEMs can be diligently orchestrated through SAML (Security Assertion Mark-up Language) authentication. With SAML authentication, each time a user accesses an application, the authentication process is relayed to the identity provider. The user enters his credentials which are then verified by the identity provider. The identity provider returns an access or reject response in the form of SAML assertion. If authentication is success, the user is granted access to the resource, and if not, access is denied. Service specific applications will relay SAML authentication process to its respective identity server which returns SAML assertion to the application. Tri-services applications will relay SAML authentication process to the concerned users service identity server, which returns SAML assertion to the application. Therefore, a tri-services application will receive SAML assertions from all three services identity servers depending upon the user to be authenticated before granting him access to the application.

4. DOMAIN CONTROLLER

4.1
Each service has implemented Domain Controllers (DCs) in their respective captive
data networks. Single Forest Single Domain architecture has inherent advantage of reduced administrative complexity due to centralised control. In a forest there is an inherent transitive trust relationship between all its domains and replication takes place within the domain. In the proposed joint framework Primary Domain Controllers (PDCs) of each service will be integrated to form Multiple Forest Multiple Domain architecture at the tri-services level by establishing an exclusive inter forest trust relationship while DCs of each service can continue to be in Single Forest Single Domain architecture.

5. PATCH MANAGEMENT

5.1
Patch management is the process of installing latest patches (code changes) which improves the system or fixes security vulnerabilities on various systems within a network thereby enhancing cyber security posture of the entire network.

5.2
It is proposed that the three services should continue with their existing patch management solutions on their captive data networks. Patch management server logs are collected by SIEM to identify endpoints which have not been patched with latest patches and identify vulnerabilities in unpatched system. SIEM alerts generated from patch management server logs of each service are integrated with SOAR to provide integrated automated response to patch management alerts at the tri-services level.

6. ANTI-MALWARE

6.1
Anti-malware solution protects against infections caused by various types of malwares to include viruses, rootkits, ransomware, spyware, worms, trojans etc. Antimalware software uses different strategies to protect system from malicious software, including signature-based malware detection, behaviour based malware detection and sandboxing.

6.2
It is proposed that the three services should continue with their existing anti-malware solutions to protect endpoints on their captive data networks. Anti-malware server logs are collected by SIEM to track if detected viruses are cleaned properly, identify machines that are not updated to latest malware definitions, identify quarantine action failed events and identify events where user choose to delete/ignore an item. SIEM alerts generated from anti-malware server logs of each service are integrated with SOAR to provide integrated automated response to malware alerts at the tri-services level.

6.3
A diagrammatic representation of the proposed joint security framework in an integrated tri-services network environment is given at Figure 1.
7. CONCLUSION

7.1 Integration of security solutions of all three services is a challenging problem. In this paper, these challenges have been analysed and a joint security framework at a tri-services level has been proposed for integrating disparate security solutions implemented by all three services on their captive data networks.

REFERENCES

Joint Enterprise Cloud for Armed Forces

Lt Col Sumit Gupta, SM

“No force on earth can stop an idea whose time has come”
—Victor Hugo

Abstract—Jointness for its actualisation on ground would require massive changes in existing organisational structures, processes and technologies. One area which would assume greater significance towards realisation of true jointness would be of ICTEC (Information, Communication Technology, Electronics & Cyber). The emerging platform of “Cloud Computing” lends itself naturally towards the vision of joint ICTEC infrastructure balancing the twin objectives of “Maximum Efficiency & Minimum Cost”.

1. INTRODUCTION

1.1

The National Institute of Standards and Technology (NIST) defines cloud computing as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., network, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics and three service models and four deployment models”\(^1\). Figure 1 shows the framework of the NIST definition of cloud computing.

---

\(^1\) Figure 1: NIST Cloud Definition Framework\(^2\)
2. CURRENT STATUS OF INFORMATIONISATION IN ARMED FORCES

2.1

Indian armed forces have ushered into Informationisation in a big way with parallel projects across various verticals currently being in different implementation phases. As an example, Army has undertaken projects for provisioning of IT infrastructure at all levels from units to highest echelons of command, primarily to facilitate routine administrative & training requirements as also to provide authorized users access to various services over Army Data Network (ADN). Operational Information System (OIS) & Logistics Management System (LMS) are major endeavors of Indian army to facilitate its transformation into a dynamic Network-Centric Force capable of achieving Information Superiority through effective management of IT. The Air Force & Navy too have similar projects catering to the operational, training and administrative requirements peculiar to these services.

3. DRAWBACKS OF PRESENT APPROACH TO INFORMATIONISATION OF ARMED FORCES

3.1

Present approach of developing various applications to enable the armed forces to meet their objective of Net Enabled Force poised to take on the challenges of futuristic battlefield suffers from few handicaps that limits the effective utilization of IT resources at our disposal. These shortcomings are briefly covered in succeeding paragraphs:

(a) **Duplicative, Cumbersome, and Costly Application Silos.** In its exuberance to embrace IT, each arm & service has planned/implemented its own set of applications with dedicated computing & storage infrastructure & without due considerations to network bandwidth availability (which is in the domain of a separate arm & is very much a precious resource). These have led to duplicative, costly & complex infrastructures, mal-effects of which would be felt once these applications are fully operationalized.

(b) **Anti-AI (Artificial Intelligence) Approach.** AI algorithms need as much data as possible to work effectively; more the data, better it is. Current approach of informationisation locks away the data in different application silos thus depriving the armed forces of the true powers of AI.

(c) **Increasing Life Cycle Cost (LCC).** Besides the developmental costs, further operation, maintenance & management costs of these resources would be largely inefficient, costing time, money & manpower that could be applied directly towards achieving strategic initiatives.

(d) **Concerns of Interoperability.** To realize the full potential of Network Centricity in a joint operational environment as envisaged in an Integrated Theatre Command (ITC), it is rather essential that each of the individual applications are able to "seamlessly talk" to each other. However, given the disjointed conception, design & development of these applications, lacunas are surfacing in this aspect, forcing the developers to incorporate “quick fix solutions” to make the applications interoperable, which is not an ideal way to achieve the desired end state.

(e) **Greater Exposure to Cyber Threats.** The application silos being developed by individual arms & services with dedicated
computing, storage & software resources present a large intrusion surface area for “Cyber Warriors” to exploit. Further, to operate, manage & ensure cyber security checks are in place would require a pool of trained personnel with these arms & services; which in the present scenario is practically non-existent.

(f) Impediment to Jointmanship. IT is the key enabler for jointmanship to actualize in a war scenario by facilitating seamless information exchange across participating components (tri-services); however given the current issues of interoperability within the Army, the integration with Naval & Air force applications seems a distant probability.

4. STRATEGY FOR ADOPTION OF CLOUD COMPUTING IN ARMED FORCES

4.1

It would be prudent to have a planned & phased transition to cloud computing model, rather than a complete overhaul of the system in a jiffy, as it would give armed forces enough leverage to build on the successes and lessons learned from Industry cloud initiatives as they are implemented. The four concurrent steps are proposed that would enable a phased implementation of the Armed forces Joint Enterprise Cloud Environment.

4.2

Step 1: Establish Directorate of Joint Enterprise Cloud (DJEC) under the Office of CDS. DJEC would be staffed by personnel from all three services and would have the overarching authority over all three services to establish an Enterprise First approach to the funding, procurement, management and use of cloud services, through policy and process change. Each IT capability development initiative to be first scrutinized by DJEC for standardization. The DJEC would work in close coordination with Directorate General of Information Systems (DGIS) of Army and its counterparts in Navy & Air Force to ensure the aspects of interoperability are taken care of.

4.3

Step 2: Establish Core Data Centers (CDCs) & Optimize Consolidation of Existing IT Infrastructure. There is a pressing need of migrating from the existing desktop based storage, computing & applications to cloud based access to these resources to enable efficiency, economy, ease of management & reduced intrusion surface for cyber threats. This would involve establishing CDCs at command level by each service. In case Integrated Theatre Commands (ITCs) come into being, a joint CDC with each ITC is proposed to be established. Further, currently installed IT infrastructure needs to be consolidated at these Data Centers. Next step would be migration of existing applications & data to CDCs & Armed forces Joint Enterprise Cloud Environment.

4.4

Step 3: Establish the Armed Forces Joint Enterprise Cloud Infrastructure. As CDCs are established, a Joint Enterprise Cloud Infrastructure would be incorporated in these and cloud functions such as Infrastructure as a Service (IaaS), Software as a Service (SaaS) & Platform as a Service (PaaS) will be added. It is fair to assume that apart from armed forces other organizations such as Border Security Force (BSF), Central Reserve Police Force (CRPF), Assam Rifles (AR), Defence Research & Development Organisation (DRDO), Intelligence agencies & agencies dealing with National Critical Information Infrastructure (NCII) would have deployed their own cloud
infrastructure. In such a multi-provider cloud environment there would be a requirement of a cloud service broker with both a technical & an organizational component to manage the delivery of cloud services amongst various government agencies. It is recommended that an organization working under Central Government be the nodal agency to perform this role and in pursuance of same suitable organizational structure & processes need to be established.

4.5

**Step 4: Deliver Cloud Service.** Following cloud services will be delivered:

(a) **Joint Enterprise File Storage.** The DJEC will implement joint enterprise file storage as a capability to enable global access to data and files by an authorized user, from anywhere and from any device.

(b) **Joint Enterprise Directory Services.** The DJEC will implement joint enterprise directory services to make data visible, discoverable, and accessible.

(c) **Unified Capabilities.** The DJEC will take necessary steps to migrate legacy voice, video and data collaboration services to Everything over IP (EoIP); standardize and consolidate each arm/service application silos’ convergence efforts across Armed Forces to reduce cost and streamline management; enhance wireless and mobility support keeping in view projects like Mobile Cellular Communication System (MCCS) & Tactical Communication System (TCS), Air Force Cellular Network (AFCEL); and provide real-time collaboration (assured, integrated voice, video, and data services).

(d) **Joint Enterprise Messaging.** The DJEC will provide a set of Joint Enterprise Messaging capabilities that includes, at a minimum, Instant Messaging (IM), chat, email (as replacement to present Army Wide Area Network (AWAN) based message exchange), and web conferencing (as replacement to currently deployed non-standardized video streaming/ video conferencing solutions).

(e) **Identity and Access Management (IdAM) Services.** The DJEC will implement enterprise-wide IdAM services that are focused on managing digital identity, authenticating users, authorizing access to resources, and using data tagging to support and enforce access control policies throughout the enterprise.

4.6

The DJEC will continue to improve these services, provide additional cloud services, and incorporate cloud services provided by individual Armed forces components as they emerge.

5. **RECOMMENDED DEPLOYMENT MODEL FOR ARMED FORCES**

5.1

**Establishment of Core Data Centres (CDCs).** As recommended in Para 15 above it is proposed to establish CDCs at command level by each service in the transition phase towards jointness. As part of Project Network For Spectrum (NFS), CDCs are already being established at Comd level by each service. Once the Integrated Theatre commands (ITCs) get operationalised in times to come, it is recommended that resources available with
service specific CDCs be amalgamated to form a joint CDC at theatre level.

5.2

Centralization vs Decentralization.

Cloud computing is essentially a concept of Centralization – moving everything from the desktop (user) to the cloud (service provider). Internet connectivity is assumed to be available to the user at all the times. However, in armed forces network availability cannot be assured during times of crisis as network resources would be subjected to degradation by the adversary by carrying out cyber or electronic attacks against network nodes as also the physical destruction of critical nodes by long range vectors. Thus armed forces need to strike a right balance between centralization of resources to improve efficiency and realize all the benefits of cloud computing & decentralization to optimally function during periods of “Blackout” (No Network Connectivity). In addition to network availability, bandwidth availability in mobile operations would also be limited owing to reliance on Radio Frequency (RF) spectrum. Exponential rise in the number of sensors and networking of these with information processing nodes and shooters in a joint operational scenario would further demand extremely judicious usage of available RF spectrum. Thus greater reliance need to be placed on having Edge Computing capabilities to support the warfighter at the tactical edge. Edge computing would also reduce the amount of info flow between various nodes thus putting lesser strain on limited bandwidth availability in the battlefield.

5.3

Establishment of Cloudlets at all Levels.

It is recommended to establish mini data centres or cloudlets at all levels form unit upward to cater for the decentralization requirements of Armed Forces. Each organizational hierarchy (battalion, brigade, division, corps, Command in army and similarly in navy & air force) need to consolidate the current IT infrastructure at these cloudlets. The cloudlets would provision adequate cloud services for optimal functioning & storage at each level with capacities commensurate to the size of formation & “Blackout” period expected. All the cloudlets across the three services will be natural extension of CDCs and would operate according to same operational, business, and IT Service Management processes to ensure that they function as a single, logically seamless computing environment meeting all requirements for graceful fail over, disaster recovery, continuity of operations, security, resiliency, and load balancing. Once the Integrated Battle Groups (IBGs) get operationalised in times to come, resources from the cloudlets be redistributed to align to the new organisational structures.

5.4

Network Resources.

There would be a requirement of seamlessly integrating the network resources utilizing the present media as well as futuristic projects as Army Static Switched Communication Network (ASCON) Phase IV, Network For Spectrum (NFS), Mobile Cellular Communication System (MCCS), Tactical Communication System (TCS), Airforce
Network (AFNET), Navy Enterprise Wide Network, Defence Communication Network (DCN) to provide connectivity between army, navy & air force clouds to form an armed forces community cloud.

5.5

Deployment Model. Given the public, private, hybrid & community deployment models currently in vogue in the cloud computing world & army’s sensitivity to its information & also the need for moving into a jointmanship era, a community deployment model is recommended with army, navy & airforce as the stakeholders.

6. CONCLUSION

6.1

The cloud computing is where the internet is moving to & many large corporations are investing heavily in this field to maintain their competitiveness. Armed forces too need to migrate to the cloud environment; albeit with due caution & security procedures in place to reap the enormous benefits this evolving paradigm of computing offers.
Unified Cyber Security Risk Management Framework for Enhancing Jointness of Operations

Lt Col Sudipto Roy

Abstract—With the implementation of jointness across all war fighting platform, there will be an increasing concern that all systems containing information technology will be vulnerable to intelligence exploitation and offensive attack through cyberspace. There is a requirement to analyse the life-cycle management to improve cyber security in all joint military systems. We also need to focus in identifying some fundamental principles of sound cyber security management and ensure their compliance with the current state of cyber security laws and policies. This paper has been divided into four different sections, namely, Cyber Security Management, Challenges for Managing Cyber security, Implementation Challenges and finally the recommendations. This paper takes a holistic look on the cyber security management of all military systems under joint operations in the entire lifecycle, i.e., right from the research and development stage to the disposal stage. Finally the paper is concluded with twelve different suggestions that can be implemented to enhance cyber security in the joint operations.

1. INTRODUCTION

1.1 Understanding Jointness of Operations. The very effectiveness of any military operations rests on a fulcrum called jointness. All modern day warfare has employed military force during conflict purely in the form of individual and independent military service components. Great generals have always possessed a vision that only through a single, unified commander vested with authority over all assigned forces and across all war-fighting domains, could hope to realize greatest military efficacy and success. Recent military failures can be attributable in part to the inability of the different military services to work together cooperatively and coherently. The nature and complexity of the contemporary security environment have transformed considerably, making jointness, as manifested by strategically minded, critically thinking, joint war fighters, all the more important.

1.2 Importance of Cyber Security Risk Management in Joint Operations. With the implementation of jointness across all war fighting platform, there will be an increasing concern that all systems containing information technology will be vulnerable to intelligence exploitation and offensive attack through cyberspace. In this paper, we will analyse how the life-cycle management can improve cyber security in all joint military systems. The focus primarily will be on the subset of all procured systems for which the joint command controlling the jointness of operations, will have some control in the form of designs, architectures, protocols, and interfaces (e.g., weapon systems, platform information technology), [1] as opposed to commercial, off-the-shelf information technology and business systems.
1.3 Fundamental Principles of Sound Cyber Security Management. This paper focuses in identifying some fundamental principles of sound cyber security management and comparing them with the current state of cyber security laws and policies. The desired outcomes of any cyber security management is aimed at limiting the adversary intelligence exploitation through cyberspace to an acceptable level and to maintain an acceptable operational functionality/survivability even when attacked offensively through cyberspace. The outcome of all Cyber security management, needs to be achieved continuously throughout the life cycle of a military system, from research and development through disposal. All phases are important, but the development and sustainment stages are particularly critical. The former because design decisions are made that can limit options in the future, and the latter because most systems reside in sustainment for most of their life cycle [2].

1.4 Operational Risk Reduction. The overall operational risk reduction will come from a combination of system security engineering, assessment of how mission assurance is affected and embracing adaptive solutions since the cyber security environment is rapidly changing. A multiple layers security management will contribute to mitigating vulnerabilities. [3] The adopted defensive measures should deny access to the systems and should be backed by a robust and resilient design so that when attacked, the system degrades gracefully and recovers rapidly to an acceptable level of functional performance.

2. CYBER SECURITY MANAGEMENT

2.1 Cyberspace the Most Challenging Domain. The most challenging domain for military systems in joint operations challenging is going to be cyberspace. Most modern military systems are so intimately intertwined with cyberspace that they depend on it for their fundamental operations. Many are further connected, either directly or indirectly, to other military systems, forming a complex system of systems whose capabilities are interdependent. The extensive dependence on cyberspace and the networking of military systems creates many enhanced and synergistic capabilities, but also leads to numerous potential vulnerabilities to military systems and operations from adversary intelligence exploitation and attacks through cyberspace. Adversaries can potentially use the domain of cyberspace in various ways to challenge the military systems deployed in joint operations [4]. They can collect intelligence on these systems to steal technology and accelerate their own capabilities. They can use this intelligence to develop countermeasures. And they can use cyberspace as a means to directly attack our military systems. Together, these pose significant risks to operational mission accomplishment.

2.2 Defining the Scope of Cyberspace. Ensuring that military systems and their underlying information systems operate with acceptably low risk and adequately support operational missions in the face of existing and potential future advanced cyber threats, lies in the realm of cyber security. Cyberspace is a very vast domain.
However, in the scope of the paper we will adopt a simpler and a goal-oriented definition. This will allow us to apply it clearly and usefully to military systems and information systems. [5] For the purposes of this paper, we use the term cyber security to mean limiting adversary intelligence exploitation to an acceptable level and ensuring an acceptable level of operational functionality/survivability even when attacked offensively through cyberspace. Acceptable level of system risk is determined by mission assurance management decisions. In short, this objective-oriented definition of cyber security means having effective counter cyber exploitation methods and survivability from attacks through cyberspace.

2.3 Defining Military Systems. In this paper, we will focus on military systems which are procured by the government. In addition, we will also assume that since the government is involved in the procurement, it has some control over design, architectures, protocols, and interfaces. The acquisition/life-cycle management community plays a significant role in cyber security for military systems. This paper will examine how to improve cyber security for military systems throughout their life cycles, including the phases of research and development, procurement, test, and sustainment. This paper avoids addressing specific technical solutions or proposals for security controls. [6] Rather, it will address how policy changes, organizational roles and responsibilities, and monitoring and feedback can be adjusted to provide more coherent and integrated cyber security management in joint operations.

2.4 Achieving Counter Cyber Exploitation in Acquisition Stage

2.4.1 Cyber Exploitation of Military System. Cyber exploitation of a military system is the extraction of information from or about that system by an adversary. Exploitation can be done by penetrating and extracting information from joint command databases, and can be done by accessing the military system itself [7]. An adversary can use this information for a range of purposes, including stealing technology, assessing joint capabilities, developing countermeasures to joint military systems, and preparing intelligence for an offensive attack against the military system.

2.4.2 Achieving Success in Cyber Exploitation. For cyber exploitation to be successful, an adversary needs to gain access to useful information and exfiltrate that information before being detected and blocked. Access can be gained through software infiltration or by implants in firmware or hardware introduced through the supply chain. These access points can, in principle, be indirect via a less critical system that has some information exchange with the system containing the more critical information [8]. Hence, to have effective counter cyber exploitation, the system owner needs to identify the most critical information, and the adversary needs to be denied access to that information; if the adversary gains access to critical information, he must be detected and blocked from successfully exfiltrating it.
2.5 Instituting Counter Offensive Cyber Operations

2.5.1 Defining Offensive Cyber Operations. Offensive cyber operations aim to do harm to a military system (or via a military system) by attacking through cyberspace. An offensive attack against a military system can, in theory, do any harm that can be inflicted by the software controls of the system. Damage can come in the form of the owner partially or fully losing the ability to use the system, the loss of active control of the military system, or the adversary taking full control of the system and using it according to his own ends [9]. The latter could result in using control to cause self-destruction or attack personnel or another system.

2.5.2 Exploiting a Military System. To successfully attack software, firmware or hardware through cyberspace, an adversary needs access to it and thereafter a flaw to exploit, that affects the ability to carry out the mission. The capability to do so generally entails deep knowledge of the military system being attacked and how it functions. It is probably a fair estimate that the more consequential the offensive cyber-attack, the more knowledge the adversary tends to need. Some of that knowledge will generally need to come from effective intelligence collection, including cyber exploitation, thus linking counter cyber exploitation and counter offensive cyber operations.

2.5.3 Facets of Countering Offensive. Countering offensive attacks through cyberspace has two facets [10]. First, preventing attack requires limiting access, limiting flaws whose exploitation could significantly affect an operational mission (e.g., software assurance), and limiting the ability of an adversary to learn about our own systems and missions. Goals and methods of this facet overlap considerably with the goals and methods of counter cyber exploitation. Second, operating at an acceptable level of functionality after an attack occurs requires a military system design that can absorb and recover from an attack. The ability of a system to absorb an attack but still function at some acceptable level is often called robustness. The subsequent ability to recover from an attack by restoring either partial or full mission functionality is often called resiliency.

2.5.4 Layered Approach to Cyber Security. Cyber security against offensive cyber-attacks, has to be provided in a layered manner. The first layer is defense. If the defense is breached and an attack occurs, the attack is met by a robust military system, and whatever degradation in function that military system suffers, it recovers quickly by being resilient [11]. These ends can be achieved by combinations of redundancy, diversity, dynamic adaptation and replacement of components when they fail, surgical deletion of infected components to stop contagion, architectural considerations for robustness and resiliency, sharing of resources with the adversary to deter attack, and protection/defensive measures. At the military-system level, like the case of counter cyber exploitation, the defensive layer is achieved by integrated security engineering of these techniques in the design phase.

2.5.5 Importance Strong Systems Engineering. Robust and resilient military systems arise from strong systems engineering with an understanding of how humans interact with those systems and further guided by functional performance requirements. Functional
performance requirements for robust and resilient systems differ from those aimed at defense, such as security controls placed on the perimeter of a system to deny access. Those for defense contribute only to defense and depend on the threat environment. Requirements for robustness and resiliency are not reactive or outward looking, they do not emerge from the threats that adversaries pose [12]. They are proactive and emerge from the need for continuing functionality of the system. Cyber robustness and cyber resiliency are in this sense no different from other survivability requirements and are the outcomes based on operational requirements and not on regulatory standards.

2.6 Managing Cyber Security Risk in Joint Operations

2.6.1 Components of Cyber Security Risk. Cyber security risk to an operational mission is defined as the product of three different components, namely:

(a) Vulnerabilities of systems.
(b) Threats to those systems.
(c) The impact to operational missions if those threats exploit system vulnerabilities.

2.6.2 Striking a Balance amongst all Three Components. Cyber security management of the risks of cyber exploitation and cyber-attack requires a balance and integration among all three components of risk. The management of each of these three components of risk is somewhat different. The goal of minimizing vulnerabilities to systems by identifying potential vulnerabilities and their mitigations in the form of denying access and having robust and resilient designs, is the primary responsibility of the life-cycle management. The goal of minimizing adverse operational mission impact and ensuring operational mission accomplishment, is the responsibility of the mission owner [13]. These two goals occasionally come into conflict and create tension in cyber security management.

2.6.3 Policies and Organizational Constructs. Policies and organizational constructs need to recognize and resolve this tension. This tension arises from two sources. Firstly, there are numerous instances in which cyber security can be achieved to some degree by either changing the system or changing how the system is used. Overcoming poor operational practices can require quite elaborate and expensive design solutions. Which solution to pursue, or what combination of solutions, is a decision that spans the stakeholders of the life-cycle management community and mission owners.

2.6.4 System Supporting Operational Mission. Secondly, how critical a system vulnerability might be depends on how that system is used to support operational mission. Missions are accomplished by a combination of doctrine, organization, training, materiel, leadership and education, personnel, and facilities. Mission assurance is not the same as each system maximizing its cyber security. For some systems, more risk will be accepted, either because that system is less critical than others to operational missions or because its potential vulnerabilities are less than another system’s. Information for making decisions regarding accepting mission risk extends beyond the purview of a standalone military system. Effective cyber security management will
require careful coordination and integration of efforts among multiple stakeholders [14].

2.6.5
Assessment of System Vulnerabilities. Finally, the assessment of system vulnerabilities and mission impact must be done in light of the threat environment. The threat information needs to flow continuously to stakeholders to support decisions throughout the life cycle of the military system. Some of that information early in the development phase will be more general and less certain. As the system design matures, information needs to be more specific and timely so that countermeasures can be effectively employed.

3. CHALLENGES FOR MANAGING CYBERSECURITY

3.1
In this section, we first discuss challenges posed by inherent attributes of cyber security before moving on to general management challenges faced by any endeavour. Further, we will be outlining a proposed framework of general principles for sound cyber security management, which will serve as a baseline for comparison with the current scenario.

3.2
Systems Integral to Design. Firstly, the challenges in implementing effective cyber security are technical and involve attributes of systems that are integral to their design. Modern military systems are so complex that only specialists can understand the detailed operations of the protocols, identify critical vulnerabilities, and understand how to address these vulnerabilities without compromising functionality. Many of these details are specific to each military system, and therefore the technical knowledge is confined to a very limited number of experts.

3.3
Intertwining between Functionality and Cybersecurity. Secondly, functionality and cyber security are intertwined. Quite a number of cyber vulnerabilities are the result of features deliberately designed into systems. That is not to say that engineers aim to make vulnerable systems, but during design, engineers make trades between functionality and security and are willing to accept certain levels of vulnerabilities in order to achieve some functionality [15].

3.4
Rapidly Evolving Threat Vector. Thirdly, the threats of exploitation and attack through cyberspace are rapidly evolving and adapting to countermeasures. Capabilities of potential adversaries are growing, and the changing technologies introduce new vulnerabilities over time. This evolution means that static solutions for cyber security management are unlikely to be effective; cyber security solutions need to be adaptive. Creating defensive barriers in the form of security overlays that respond to discovered vulnerabilities is by nature insufficient to protect against future, unknown threat vectors.

3.5
Inherent Advantage of Attacker. Fourthly, in cyber space the attacker has inherent advantage over the defender. The adversary needs to find only one weakness, such as a single access point. The defender needs to mitigate against all plausible threats for all potential vulnerabilities. Because the aggressor needs to find just one path for access and the defender needs to block all possible paths, defensive measures also tend to be more
expensive than the tools they attempt to stop, putting the defensive side on the wrong side of cost considerations [16].

3.6 Imbalance between Offense and Defense. Fifthly, this imbalance between the offense and defense in the cyber domain implies that it is unwise to assume that complete cyber security can be achieved. Some potential vulnerabilities that can be exploited or attacked will always persist. The goals of counter cyber exploitation are, for example, controlling critical information by identifying it, restricting access to it, and preventing its theft. It is not possible to reduce the amount of critical information to zero. Nor does it appear safe to assume that access can be unequivocally denied [17]. The question is how much security is enough given finite resources and mission needs.

3.7 Risk Mitigation Decision Making. Sixthly and finally, risk mitigation decisions for cyber security are not easily partitioned. Systems are sufficiently interconnected that accepting a vulnerability in one system can introduce a vulnerability into another system. For example, accepting risk of an adversary accessing a maintenance device through an intermittent Internet connection potentially introduces this vulnerability to a military system when that maintenance device is connected to the military system. Hence, critical vulnerabilities can be introduced in small programs or in noncritical components and in a diverse range of targets. Concentrating effort on vulnerability reduction in only large or critical systems is insufficient [18].

3.8 Organization Level Support for Innovation. The cyber security challenges of the evolving threat environment and the changing technologies stress the need for adaptive solutions and an organization that supports and facilitates innovation. These challenges contraindicate that effective cyber security solutions will emerge solely from prescribed rules and policies, specifically in the form of security controls. Reactive, defensive barriers meant to deny access have struggled to keep up with the evolving threat. Although the most common means to try to reduce cyber exploitation is defensive barriers to deny access, these barriers are most effective when they are part of the integrated design of the system than when they are appended after design. Security controls enveloping a system poorly designed from a security standpoint are unlikely to be successful; controls integrated with a secure architectural design have great promise. Effective cyber security management is most likely to be achieved through risk mitigation guided by mission assurance goals and achieved by adaptive solutions integrated into the design phase, rather than by prescribed rules.

3.9 Effective Organisational Design. The tendency toward a dynamic environment suggests that cyber security is most effectively managed by an organizational design that emphasizes identifying cyber security solutions via coordination and collaboration of workers rather than prescribing standardized solutions. The strong tendency toward complexity suggests that it is unlikely that the organization will identify successful solutions from the top down. Highly formalized rules for achieving cyber security imposed on the engineering level from above will impede innovative, adaptive outcomes for cyber security. Decentralized decision making for implementation to the levels in the organization possessing the appropriate expertise is indicated. Higher
levels in the hierarchy should set clear goals of what should be accomplished, but devolve decisions of how to accomplish those goals to well-trained system security engineers. And finally, the weaker tendency toward diversity suggests that cyber security might very well require more than one organizational unit to be effectively managed, perhaps managing weapon systems/platform information systems and information technology systems separately [19].

3.10 Feedback and Control. Continuous monitoring of how well desired outcomes are being achieved is essential for sound decision making. What is monitored and evaluated in an organization sets incentives and accountability structures and therefore can implicitly set the organization’s goals. If those implicit goals do not align with the organization’s desired outcomes, it is unlikely those outcomes will be attained. Cyber security management can be understood as a process-control loop. A process-control loop runs from the state of cyber security, to feedback mechanisms for monitoring it, to decision makers, to the actions (designs, policies, and practices) under their control, which in turn adjust the state of cyber security. This process control loop depicts standard management practices of a continuous process of monitoring how well the enterprise is operating, making decisions to adjust those operations, taking actions to adjust the enterprise, then examining the outcomes of those decisions. There is also a feedback loop that monitors whether the actions directed by management are being properly implemented. Decision makers at high levels in the Joint Operations HQ need feedback on cyber security that captures the success of cyber security measures in meeting mission assurance goals and need to look out at a longer timeframe, monitoring trends over time. Decision makers at lower levels like system engineers, need more technical feedback regarding the performance of systems and current threats, and need more rapid responses than the higher-level leaders do. The goals and priorities for cyber security and mission assurance are important for shaping the right feedback for highest-level leaders [20].

4. IMPLEMENTATION CHALLENGES

4.1 Changing Dynamics of Cyber Security Environment. Our first challenge is that the cyber security environment will be complex, rapidly changing, and difficult to predict, but the policies governing cyber security has to be better suited to simple, stable, and predictable environments, which will lead to significant gaps in cyber security management. This will have four consequences of concern which have been summarised below:

(a) The prescribed solutions for military system cyber security in the form of controls which are not as comprehensive for providing security as sound system security engineering demands them to be.

(b) The processes and security controls will be developed principally with information technology systems in mind, not military systems, and hence solutions will not be well tailored.
(c) The strategic goal of mission assurance will diminish in favour of tactical security controls.

(d) In relying on standardized and formalized security controls as the means by which cyber security is to be accomplished, the policy telegraphs to the enterprise that the implicit goal of cyber security is compliance with security controls.

4.3 Vigilance in Life Cycle of Military System.

The second possible challenge is that the implementation of cyber security is not going to be continuously vigilant throughout the life cycle of a military system, but instead will be triggered by acquisition events, mostly during procurement, resulting in incomplete coverage of cyber security issues by policy. This consequences of concern that this challenge will pose have been summarised below:

(a) These programmatic events will come late in the design process, and therefore will have little leverage to influence some critical design decisions that will affect cyber security.

(b) Systems in programs beyond procurement, being sustained or disposed, will get diminished attention relative to those in procurement.

(c) This policy structure will lead to imbalanced risk assessment by favouring system vulnerability assessments over mission impact and threat.

(d) Management, oversight, and budgeting within the joint operations HQs will have to be strongly structured around programs. Cyber security vulnerabilities will cross program boundaries, creating a misalignment between the challenge and its management.

4.4 Accountability for Military System.

The third challenge in cyber security management in joint operations deals with the control of and accountability for military system cyber security which are spread over numerous organizations. This will give rise to poor integration, resulting in diminished accountability and diminished unity of command and control for cyber security. These overlapping roles, and presence of a cyber security-focused apex authorizing official at the national level, will create ambiguities in decision authority and accountability. It will be, for example, unclear who can make the final decision regarding risk to a mission: the commander of joint operations or the authorizing official at the Government level. Similarly, who will be held accountable if a cyber security incident occur, the program manager, the authorizing official, or the operational commander?

4.5 Monitoring and Feedback for Cyber security.

The fourth challenge will be in monitoring and feedback for cyber security to ensure its completeness, coordination, and sufficiency for effective decision-making or accountability. This challenge will have three consequences of concern:

(a) This may lead to critical gaps in the feedback mechanism since it will not capture all systems, and will be unable to probe the consequences of cyber security shortfalls, and thus will not be produced in a form for effective decision-making.

(b) If there is a lack of comprehensive program or a system oriented feedback on cyber security, the impact of cyber security on operational missions will stand in stark contrast to the abundance of feedback on cost and schedule...
performance. This imbalance will create an incentive structure for program managers and program executive officers which will favour emphasis on cost and schedule over performance, specifically cyber security.

(c) These deficiencies in feedback on cyber security will inhibit individual accountability.

5. RECOMMENDATIONS

5.1
Two underlying themes emerge through these challenges posed by cyber security management in joint operations. Firstly, cyber security risk management will not adequately capture the impact to operational missions and secondly, cyber security is mainly added onto systems, not designed in. As partial redress for these challenges of concern following 12 recommendations are being suggested.

(a) Defining Cyber Security Goals. Define cyber security goals and desired outcomes for military systems within the joint operational environment, which shall remain consistent with national defence issuances.

(b) Realign Roles and Responsibilities. Realign functional roles and responsibilities for cyber security risk assessment around a balance of system vulnerability, threat, and operational mission impact and empower the joint operational HQ to integrate and adjudicate among stakeholders.

(c) Increase Accountability. Assign authorizing officials a portfolio of systems and ensure that all systems comprehensively fall under some authorizing official throughout their life cycles.

(d) Redefining Policies. Adopt, within the joint operational HQ, policies that encourage program offices to supplement the required security controls with more comprehensive cyber security measures, including sound system security engineering.

(e) Innovation and Adaptation. Foster innovation and adaptation in cyber security by decentralizing in any policy about system security engineering implementation within individual programs.

(f) Simplifying the Complexity. Efforts in reducing the overall complexity of the cyber security problem by explicitly assessing the cyber security risk/functional benefit trade-off for all interconnections of military systems in cyberspace.

(g) Expert Group. Create a group of experts in cyber security that can be matrixes as needed within the lifecycle community, making resources available to small programs and those in sustainment.

(h) Addressing Legacy Systems. Establish an enterprise-directed prioritization for assessing and addressing cyber security issues in legacy systems.

(i) Continuous Assessment. Close feedback gaps and increase the visibility of cyber security by producing a regular, continuous assessment summarizing the state of cyber security for every program and holding program managers accountable for a response to issues.

(j) Dedicated Team for Cyber security Product Acquisitions. Create cyber security teams within the joint operations HQs that are dedicated to acquisition/lifecycle management.

(k) Individual Accountability. Hold individuals accountable for infractions of cyber security policies.
6. CONCLUSION

6.1

It may be appreciated that these recommendations, even if fully implemented, would not completely solve the challenges of cyber security during joint operations. Further, some of these policies would necessarily require additional resources and a suitably skilled workforce to carry out the responsibilities, commitments that are difficult to make in a constrained fiscal environment. The fact is that there are no quick or easy fixes for achieving world-class cyber security. However, by adopting these recommendations, the joint operational HQ would take a large step toward more effective cyber security of its military systems throughout their life cycles.

REFERENCES


Enhancing Cyber Security Posture by Leveraging Technologies Like Big Data, Artificial Intelligence and Block Chain Technologies

Lt Col Apurva Bhatnagar

Abstract—Security challenges to joint defence networks have been a matter of concern to the National Security within the last two decades. Defence telecommunication infrastructure that provides the necessary backbone for information exchange such as voice, video, data, and Intranet connectivity have been found to be particularly vulnerable to various forms of attacks. Some of these attacks could lead to Denial of Service, loss of integrity and confidentiality of network services. Protecting these networks from attacks is thus an important aspect that cannot be ignored. This paper suggests utilization of latest technologies to address some of the important security challenges to current telecommunication networks and recommends leveraging these technologies that can be implemented to mitigate not only infrastructural insecurity but the overall Cyber Security posture.

1. INTRODUCTION

1.1

With automation to ITisation of various organizations like government, military, other private industries, there has been an enormous increase in the Data storage, handling, assimilation, collation and adopted security measures. Related to the criticality of these measures and the vital data, Cyber Security Posture of an organization becomes paramount important. A significant portion of that data can be sensitive information, whether that be operational plans, deployment, financial details, personal information, or other types of data for which unauthorized access or exposure could have severe consequences if compromised. Organizations transmit sensitive data across networks and to other devices in the course of routine or sharing important data and Cyber Security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the quantum, complexity and types of cyber attacks grow, organizations especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive data and personnel information. As early as March 2013, the nation’s top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, surpassing even terrorism.

1.2

Improving Cyber security posture is emerging as the top priority because of several predominant reasons as under:

(a) The large volumes of data requiring Data Analytics, and increased complexity of the cyber-attacks/breaches.
(b) Increased data migration to network interconnections increasing the vulnerability of data.

(c) BYOD and cloud services enable access of enterprise applications via personal devices increasing susceptibility of systems. Unauthorized users can easily hack organization networks once they crack devices. Tri services has been striving hard to ensure personal devices are not connected over organization network or other networks are brought into Organization premises. Despite measures like Air gap, cyber violations are predominant.

(d) Tightly integrated supply chains like Defence Accounts, vendors or other civil-military type organizations increase risk from the weakest link.

(e) Cybercrime has become a service and hence it is difficult to trace malware.

(f) Lack of preparedness to make quick changes in processes and policies, in case of a cyber attack. This is an essential skill particularly in case of a highly sophisticated attack, which has the ability to bypass detection until after cyber attackers have breached the defenses.

1.3

Cyber security should no longer be viewed as a function of Information Technology or Information security alone. It needs to form an integral part of culture and strategy of the organization. It should be reflected in each and every facet of the organization, right from the strategy to the behavior of an individual in the Area of Responsibility. With so much dependence on data flow and communication between processes, components and sub-systems, data integrity and systems integrity assume critical dimensions. Manual supervision of various processes is neither feasible nor effective. Even patching security flaws from time to time is not practical. Data by itself needs to be both abstracted and secured through different tools and techniques and here is how this paper suggests leveraging the latest technologies like Blockchain, AI and Big Data Analytics. Cyber security is the core challenge when it comes to risk management. People, Process and Technology. The later, Technology offers very stimulating and useful tools to survive in the cyber ecosystem. Nothing is entirely unhackable, but there are some emerging technologies that can help organizations address this challenge. Some of these Force Multiplier technologies are Blockchain, Artificial Intelligence (AI) and Big Data.

(a) **Blockchain.** Computer technology and the internet have disrupted the old way of office functioning. New procedures continue to come up and working models of yesteryears Standard Operating Procedures are all but forgotten. But these efficient changes are not without a price; technology introduces vulnerabilities in organizations. Every system with a connection to the internet or external network is exploited by hackers. However, technology may, at last, have an answer to the menace posed by cyber criminals. As the strategies used by cybercriminals continue to evolve, security experts have turned to Blockchain for a solution.

As defined in Wikipedia, Blockchain technology is labeled as a peer to peer network with a shared, distributed ledger which records all data transactions across multiple networks. The core benefit of using Blockchain is that users can make secure network
communication onto a Blockchain irrespective of the organization. Blockchain technology can prevent a variety of data breaches, cyber attacks, identity thefts and any malicious intent in network. Blockchain ensures that the data remains private and secure in all the blocks it creates to maintain transparency.

(b) **Artificial Intelligence and Machine Learning.** In computer science, Artificial Intelligence (AI), sometimes called machine intelligence, is intelligence demonstrated by machines, in contrast to the natural intelligence displayed by humans. Colloquially, the term 'Artificial Intelligence' is often used to describe machines (or computers) that mimic ‘cognitive’ functions that humans associate with the human mind, such as ‘learning’ and ‘problem solving’.

Artificial Intelligence has become the foremost focus of Cyber security as a solution. One of the most important reasons to use AI for Cyber security is the potential of Natural Language Processing (NLP). Systems that are powered by AI can automatically collect data by scanning the data over the network. These kinds of AI systems use NLP for selecting valuable information from the scanned data that provide insights indicating cyber-attacks, mitigation and anomalies based on which they create prevention strategies on processing.

Alternatively, AI will help organization create a real-time, dynamic and global authenticated framework and system that adjusts the access rights based on location or network. This will also have a Multi-factor authentication to prevent cyber threats. Not only this, the intelligent systems will monitor user information to analyze user behavior, device usage, network activities, location and application data. Using such information, the system will change any user’s access rights automatically to ensure the data is secure on remote networks.

Artificial Intelligence previously occupied the realm of science fiction, but is now a mainstay in helping organization better secure themselves. As computing power increases and Machine Learning becomes more advanced, ever more powerful analytics tools can help forecast where hackers might strike next. If an organization can predict where an attack might focus in the future, it can better prepare for a possible cyber attack and ideally deflect it. When used in concert with advanced authentication and encryption techniques, analytics can provide organization with formidable tools to help keep their data safe.

Artificial Intelligence (AI) and Machine Learning (ML) techniques are emerging as promising solution providers, which have the potential to improve network service and in-house processing in financial institutions, banks and especially Defence sector. In the view of growing success-rate of Research and Development of AI and ML based tools and technologies in various application domains, many Defence organizations are now turning to develop automated self-learning algorithms for improved and efficient security solutions.

(c) **Big Data.** Big Data is a technology that has come into existence in recent past. Its applications, ease of access and accuracy have made it very popular in diverse fields. A 2016 definition states that “Big Data represents the information assets
characterized by such a high volume, velocity and variety to require specific technology and analytical methods for its transformation into value”. Similarly, Kaplan and Haenlein define Big Data as “data sets characterized by huge amounts (volume) of frequently updated data (velocity) in various formats, such as numeric, textual, or images/videos (variety).” Additionally, a new V, veracity, is added by some organizations to describe it, a revision challenged by some industry authorities. The three Vs (volume, variety and velocity) have been further expanded to other complementary characteristics of Big Data:

(i) **Machine Learning.** Big Data often doesn’t ask why and simply detects patterns.

(ii) **Digital footprint.** Big Data is often a cost-free byproduct of digital interaction.

(d) The main components and ecosystem of Big Data are as under:

(i) Techniques for analyzing data, such as A/B testing, machine learning and Natural Language Processing (NLP).

(ii) Big Data technologies, like business intelligence, cloud computing and databases.

(iii) Visualization, such as charts, graphs and other displays of the data.

2. **LEVERAGING OF EMERGING TECHNOLOGIES TO ENHANCE CYBER SECURITY POSTURE**

2.1 **Blockchain and Cyber Security.**

Blockchain refers to a list of records, known as blocks that are linked by cryptography. Blockchain has three main characteristics:

(i) **Decentralization.** It is not owned by any one party.

(ii) **Transparency.** Hence data cannot be tracked, maintaining the privacy of transacting parties.

(iii) **Immutability.** Data inside a Blockchain cannot be tampered with.

2.2

Blockchain utilizes encryption and hashing to store immutable records and many of the existing Cyber security solutions utilize very similar technology as well. The majority of existing security measures rely on a single trusted authority to verify information or store encrypted data. This leaves the system vulnerable to attack, and many bad actors could focus their efforts on a single target to commit Denial of Service attacks, inject malicious information and extort data through theft or blackmail. Blockchains have the upper hand over current security measures in that true Blockchains are decentralized and do not require the authority or trust of an individual member of the network. The system does not require trust because each node, or member, has a complete copy of all the historic information available and just through achieving consensus of the majority will more data be added to the chain of previous information. As outlined in other sections of this paper, this is achieved in many different ways, but the bottom line is, many members of a network who have access to the same information will be able to secure that group far better than a group made up of one leader and a host of members who rely on the leader for their information, particularly when bad actors could come in the form of group members or even as the leaders themselves.
2.3
A recent example of use of Blockchain technology is NASA that decided to implement Blockchain to improve their Cyber security, avoid Denial of Service and other attacks on air traffic services.

2.4
The cryptographic hash, which links the blocks, is highly resistant to attack and cannot be inverted or modified. This has special relevance to organization like Defence that stores and shares sensitive data, transact and maintain privacy. Though Blockchain was first invented for Bitcoin, its features make it an apt foundation for Cyber security technologies. In fact, large organizations are slowly warming up to the idea of adopting Blockchain security. For example, in 2017, Lockheed Martin decided to adopt Blockchain as part of its Cyber security strategy. The company contracted Guardtime Federal, the world’s largest Blockchain Cyber security firm, to provide the service. Ron Bessire, VP Engineering and Technology at Lockheed Martin saw this move as a chance to ‘enhance data integrity, speed problem discovery and mitigation’ and ultimately, speed up software development and delivery of final products.

2.5
(a) Based on the most security-focused Blockchain applications identified in RQ1, Blockchain was applied to improve Cyber Security in data storage and sharing, network security, private user data, navigation and utility of World Wide Web with details as under:

(i) **Data storage and sharing.** Both public and private distributed ledgers are used to eliminate a single source of failure within a given storage ecosystem, protecting its data from tampering. That is, Blockchain helps to ensure that data stored in the cloud remains resistant to unauthorized changes, hash lists allow for searching of data that can be maintained and stored securely, and data exchanged can be verified as being the same from dispatch to receipt. In a nutshell, Blockchain improves data storage and sharing security by creating a decentralized network that uses client-side encryption in which data owners will have full traceable control of their data.

(ii) **Network security.** The majority of works in this category use Blockchains to improve Software Defined Networks (SDNs) and use containers for authenticating critical data to be stored in a decentralized and robust manner. In such works, Blockchain-enabled architecture of SDN controllers using a cluster structure is used. The architecture uses public and private Blockchains for P2P communication between nodes in the network and SDN controllers to make the Blockchain appropriate for addressing network security issues.

(iii) **Private user data.** Comparing with other categories, the application of Blockchain for improving data privacy has been less discussed. The reason could be due to the irreversibility nature of Blockchain (everybody has a copy of the ledger), which makes it hard to be used for privacy purposes, particularly in data protection. In
current approaches, typical user device preferences are encrypted and stored on the Blockchain to be retrieved only by that user. Also, they explore differences between Blockchain Proof of Work and Proof of Credibility consensus mechanisms, where nodes are given a score to determine their credibility dependent on the number of connections to other trusted nodes.

(iv) **Navigation and utility of the World Wide Web.** In present day, the www is inevitable. Substantial tasks in defence offices these days are Internet dependent like e-procurement (GeM), e-ticketing or NIC e-mail. Blockchain can be used to improve the validity of the wireless Internet access points connected by storing and monitoring the access control data on a local ledger. Also, Blockchain is used to help navigating to the correct web page through accurate DNS records, safely utilizing web applications and communicating with others through secure, encrypted methods. To implement these solutions, the idea of consortium Blockchain has been used, in which the consensus process is controlled by a preselected set of nodes in the network.

(v) **Blockchain for AI data security.** In modern computing ecosystem, data is captured from various sources and transmitted among devices through the networks. Artificial Intelligence (AI) and its derivatives have been used as powerful tools to analyze and process the captured data to achieve effective reasoning in addressing security issues. Although AI is powerful and can be engaged with distributed computing, deceptive analysis would be generated when corrupted or dishonest data is intentionally or unintentionally integrated by a malicious third-party based on adversarial inputs. Blockchain as a popular ledger technology has the potential to be leveraged in different areas of the cyber space. Block chain attempts to reduce transaction risks and unintentional leakage of information, owing to its characteristics such as decentralization, verifiability and immutability for ensuring the authenticity, reliability and integrity of data. When the credibility and reliability of data can be ensured, more secure and trustworthy outcomes can be produced by AI. A future research direction could be the exploration of Blockchain for the security of AI data in Defence network.

2.6 **(a) Artificial Intelligence and Cyber Security.** Artificial Intelligence (AI) is another technology that has started impacting government departments and Defence organizations in a major way. It is an area of computer science that helps building solutions with human like intelligence and can carry out complex tasks independently. AI applications are based on neural networks, Machine learning, deep learning and Natural
Language Processing (NLP) algorithms. Machines act like humans only after they are trained well to accomplish specific activities by processing huge amounts of data and identifying patterns in it. The growing interest and value proposition of the technology is resulting in Defence procurements trying to explore AI in most of their service propositions.

2.7

Major initiatives in the field of AI have been taken by Google, Apple, Amazon and others. Government of India has appreciated the immense potential of AI and has made significant investments to use it for better governance and service delivery as illustrated below:

(a) PM Narendra Modi Government has set up an AI task force, appointed by Ministry of Communication and IT in order to prepare India for the upcoming Industrial Revolution 4.0 through a Public-Private Partnership.

(b) The AI Task Force of the Ministry of Defence has shared their final report on how AI can aid in gaining military superiority and the strategic implications of AI from a National Security Perspective.

(c) Niti Ayog has come up with India’s strategy on AI for the development of the following sectors on focus: health care, agriculture, education, smart cities and infrastructure, and smart mobility and transformation.

2.8

AI has the potential to make Cyber security more efficient and responsive against ever increasing threats and improve the Cyber security posture of any defence organization. Some of the Cyber security areas which are amenable to AI are described in succeeding paras:

2.9

(a) Threat monitoring, detection and response. AI and Machine Learning (ML) allows the systems to monitor a wider range of evolving threat vectors rather than monitoring threats against previously identified signatures. Machine learning can track anomalous behavior easily and help in predictive analysis of threats and attacks. Complex analytics using historical data combined with clustering, clipping, data visualization etc can be carried out without human intervention and allow security administrators to respond in near real time to security events and incidents. This will take threat detection and alert generation to the next level.

(i) Audit. ML can increase efficiency of configuration management, configuration audit and Cyber Security Audits by removing human errors and biases. These solutions can enhance the performance and reduce the risk in internal audits by reviewing a larger data set (for example evaluating all casualties published in a year) as compared to evaluating a representative sample as done in conventional internal audits against known internal control red flags, thereby ensuring audit completeness and quality reports. A CSAT (Cyber Security Audit tool) has been put in place at HQ DG Assam Rifles justifying the above.

(ii) Secure code review. NLP
techniques (Natural Language Processing algorithms) are utilized in automated code review for better detection and reporting of bad coding practices or security vulnerabilities. Automating code reviews can help reduce costs, ensure code health and increase productivity by focusing on the most harmful vulnerabilities.

(iii) **Access management and network monitoring.** Access management is another area where AI and ML can increase efficiency and effectiveness. Cyber security of systems, applications and data bases can be improved through continuous learning and updation of rules. They can also aid in monitoring network traffic and identifying any abnormal activity and raising alarms or taking pre-emptive actions to block any traffic which can harm the networks or applications, thereby integrating the functionalities provided by multiple security tools.

(iv) **Data discovery, classification and loss detection/prevention.** ML techniques can be used to enhance offerings by typical Data Loss Prevention (DLP) solutions by automating classification, monitoring and prevention of sensitive data loss by using predictive models to identify sensitive personal or strategic information and tracking access patterns to these data sets from new/unusual activity from existing sources.

(v) **Vulnerability assessment and penetration testing.** AI based vulnerability scanning applications are able to crawl dynamic pages, detect vulnerabilities which otherwise require human intelligence, thereby reducing cost and increasing efficiency and reducing false positives.

(vi) **Automated network analysis.** AI is a perfect fit for Machine Learning system due to the sheer volume of available data that requires analysis. So monitoring communication is a good way to detect malware.

2.10
Al-based applications could potentially reduce backlogs, cut costs, overcome resource constraints, free network Admin from mundane tasks, improve the accuracy of projections, inject intelligence into scores of processes and systems and handle many other tasks humans can’t easily do on our own, such as predicting fraudulent access, identifying malicious intent and sifting through millions of documents in real time for the most relevant content.

2.11

(a) **Big Data and Cyber Security.** Big Data can store large amounts of data and help analysts examine, observe, and detect irregularities within a network. That makes Big Data analytics an appealing idea to help escape cybercrimes. The security-related information available from Big Data reduces the time required to detect and resolve an issue, allowing cyber analysts to predict and avoid the possibilities of intrusion and invasion. Insights from Big Data analytics tools can be used to detect Cyber security threats, including malware/ransomware attacks, compromised and weak devices, and malicious insider programs. This is where Big Data analytics looks most promising in improving Cyber security.
Enhancing Cyber Security Posture by Leveraging Technologies Like Big Data, Artificial Intelligence and Block Chain Technologies

(b) **Intelligent risk management.** To improve the Cyber security efforts, the tools must be backed by intelligent risk-management insights that Big Data experts can easily interpret. The key purpose of using these automation tools should be to make the data available to analysts more easily and quickly. This approach will allow our experts to source, categorize, and handle security threats without delay.

(c) **Threat visualization.** Big Data analytics programs can help us foresee the class and intensity of Cyber security threats. One can weigh the complexity of a possible attack by evaluating data sources and patterns. These tools also allow one to use current and historical data to get statistical understandings of which trends are acceptable and which are not.

(d) **Predictive models.** Intelligent Big Data analysis enables experts to build a predictive model that can issue an alert as soon as it sees an entry point for a Cyber security attack. Machine learning and Artificial Intelligence can play a major role in developing such a mechanism. Analytics-based solution enables to predict and gear up for possible events in the process.

2.12 Infrastructure penetration testing will give insight for complete database and process and help keep intruders at bay. Penetration testing is a simulated malware attack against computer systems and network to check for exploitable vulnerabilities. It is like a mock-drill exercise to check the capabilities of our processes and existing analytics solutions. Penetration testing has become an essential step to protect IT infrastructure and critical data.

2.13 Big Data analytics solutions, backed by Machine Learning and Artificial Intelligence, give hope that information and processes can be kept secure in the face of a Cyber security breach and hacking. Employing the power of Big Data, we can improve our data-management techniques and cyberthreat-detection mechanisms.

2.14 Politics as an example is emerging as one of the key markets of Data Analytics firms. Cambridge Analytica was increasingly engaged in helping politicians to understand voter behavior through data (later found to be stolen), Donald Trump was allegedly one of its clients. Indian politicians have also been catching up. Several political parties have opted for the services of Data Analytics firms to understand voter behavior for the 2019 Lok Sabha elections. In the Indian context, information privacy has been a bone of contention between the present government and the opposition over the Aadhaar Bill. Aadhaar database has been repeatedly proven to be prone and vulnerable to attacks. A single breach in its security could expose vital information of Indian citizens.

2.15 Threats envisaged while implementing Blockchain, AI and Big Data technologies for effective Cyber security posture. With inherent minor drawbacks that have been identified till date, these technologies have following risks/challenges:

(a) **Security risks in Blockchain.** Although Blockchain holds immense promise and potential, it remains vulnerable to cyber threats and risks as mentioned below with suggestive approach:

(i) **Key Management.** Private keys are used to sign transactions, and
hence anyone with the private key corresponding to an address, can sign a transaction and transfer value to another address or value it off-chain. Having misplaced keys, lost assets cannot be recovered as private keys cannot be recovered. The way AWAN/ AFNET are managed, a nodal agency can take care of this issue.

(ii) **Software coding error/ protocol vulnerabilities.** Most Blockchains are developed by enthusiasts that neither possess a security or audit certificate, nor follow secure coding practices. Often, an exchange may expose their hardware and software to threats. The recommendation in such a case would be of a SAG approved Secure Code/ Secrecy.

(iii) **Identity based attack.** Blockchains are not immune from identity-based attacks. Such attacks could be employed to take over a majority of the nodes in a network and undermine the consensus validation and distributed architecture protections of a network. The basic Cyber Security measures in place can avoid such attack.

(iv) **Sophisticated consensus based attacks.** If, and when, a hacker gains control of at least 51% of the mining hash power in the ecosystem, the property of immutability is compromised. This gives the hacker power to alter and reverse information. Though rare, this possibility can be taken care of by continuous monitoring the networks.

(v) **Evolving attack vectors.** One longer-term risk that is gaining attention is the possibility of quantum computing based attacks that leverage enhanced computational power to weaken or compromise existing cryptographic algorithms used in existing IT systems and in Block chains. With evolving times, the cryptographic algorithm can be updated to address this issue.

(b) **Security and privacy risks in AI.**

(i) **Data manipulation.** AI and Machine learning systems make better predictions by analysing huge amounts of data. But if the learning data sets or algorithms can be manipulated, it can lead to potentially disastrous results for sectors specifically in Defence. Big Data/ Block Chain can assist in avoiding data manipulation.

(ii) **Protection of training data.** Majority of the training data fed into a system can consist of sensitive military information for functioning. Hackers can gain access to such confidential data by utilizing reverse engineering. Block Chain can ensure protection of such data.

(iii) **Unauthorized access.** Lack of strong access control, credential management and privilege account administration can lead to abuse of system functionalities and system availability by accessing the Machine learning algorithm data source and training method. Defence organizations have a strong access control already in place.

(iv) **Unmasked PII.** Personally Identifiable Information in unmasked form being used in an AI...
platform can lead to compromise of the data. Hence organizations need to ensure masking/ encryption of the PII.

(v) **Regulatory and compliance issues.** Although analysis of huge amounts of data leads to more accuracy in providing core services, but getting adequate consent for data collection, processing and storage in order to comply to regulations pose a challenge. A well defined Nodal Agency will address all such issues.

(c) **Security and privacy risks in Big Data Analysis.** Big Data security comes with its concerns and challenges, and to be able to mitigate, its pertinent to get acquainted with them.

(i) **Vulnerability to fake data generation.** Before proceeding to all the operational security challenges of Big Data, there is a concern of fake data generation. To deliberately undermine the quality of Big Data analysis, intruders can fabricate data and ‘pour’ it into our data lake. For instance, if an Ordnance Factory uses sensor data to detect malfunctioning production processes, intruders can penetrate the system and make the sensors show fake results, say, wrong temperatures. This way, one can fail to notice alarming trends and miss the opportunity to solve problems before serious damage is caused. Such challenges can be solved through applying fraud detection approach.

(ii) **Potential presence of untrusted mappers.** Once Big Data is collected, it undergoes parallel processing. One of the methods used here is Map Reduce paradigm. When the data is split into numerous bulks, a mapper processes them and allocates to particular storage options. If an outsider has access to mappers’ code, they can change the settings of the existing mappers or add ‘alien’ ones. This way, the data processing can be effectively ruined and intruders can make mappers produce inadequate lists of key/value pairs. Which is why the results brought up by the Reduce process will be faulty. Besides, intruders can get access to sensitive information.

The problem here is that getting such access may not be too difficult since generally Big Data technologies dont provide an additional security layer to protect data. They usually tend to rely on perimeter security systems which are well strengthened in Defence organizations over a period of time.

(iii) **Troubles of cryptographic protection.** Although encryption is a well-known way of protecting sensitive information, it is further on the list of Big Data security issues. Despite the possibility to encrypt Big Data and the essentiality of doing so, this security measure is often ignored. Sensitive data is generally stored in the cloud without any encrypted protection. And the reason for acting so recklessly is constant encryptions and decryptions of huge data slows things down, which entails the loss of Big Data’s initial advantage i.e. Speed. With the planning of Data Centres by defence organizations this issue will be adequately addressed.
(iv) **Possibility of sensitive information mining.** Perimeter-based security is typically used for Big Data protection. It means that all ‘points of entry and exit’ are secured. Data can be better protected by adding extra perimeters. Also, system’s security could benefit from anonymization. If a compromised network for example gets personal data of a users with absent names, addresses and telephones, they can do practically no harm.

(v) **Data provenance difficulties.** Data provenance, or historical records about data complicates matters even more. Since its job is to document the source of data and all manipulations performed with it, user can only image what a gigantic collection of metadata that can be. Big Data is not small in volume itself. Every data item it contains has detailed information about its origin and the ways it was influenced (which is difficult to get in the first place).

For now, data provenance is a broad Big Data concern. From security perspective, it is crucial because unauthorized changes in metadata can lead to the wrong data sets, which will make it difficult to find needed information and untraceable data sources can be a huge impediment to finding the roots of security breaches and fake data generation cases.

(vi) **Absent security audits.** Big data security audits in the organization can give awareness of security gaps. And although it is advised to perform on a regular basis, this recommendation is rarely met in reality like the present day Cyber security Audits. Working with Big data has enough challenges and concerns as it is, and an audit would only add to the list. Besides, the lack of time, resources, qualified personnel or clarity in Admin-side security requirements makes such audits even more unrealistic. _A religious approach on these will ensure no lapse._

### 3. CONCLUSION

**3.1**

This paper has identified the scope rendered by the latest technology solutions that can contribute to enhance the Cyber Security posture of our organizations. The initial keyword searches for this analysis paper highlight Blockchain or Big data as a standalone technology that bring with it an exorbitant array of possible solutions for finance, logistics, healthcare and Cyber Security. This paper has focused solely on leveraging Block Chain, Big Data and AI for Cyber Security. Undoubtedly, there are worthy applications for Blockchian, Big Data and AI, however, a decentralized, trustless system cannot by itself solve all problems one may uncover in the field of Cyber Security and hence an amalgamated solution utilizing Blockchain applications, Big Data Analytics and AI Machine Learning or NLP for Cyber Security has been suggested and diagrammatically represented as under:
REFERENCES

1. Wikipedia.
3. Recent advances in Blockchain Technology by Dr. NV Narendra Kumar.
4. Cyber Security for Industry 4.0 by ASSOCHAM.
5. AI in Cyber Security by Forbes.
Practical Solution for Secure Network in a Quantum Computing ERA

Anindita Banerjee$^1$ and M T Karunakaran$^2$
$^{1,2}$QuNu Labs Pvt Ltd, MG Road, Bangalore, India
E-mail: $^1$anindita@qunulabs.in, $^2$mtk@qunulabs.in

Abstract—Data security in a network is a major concern in quantum era. One of the major challenges faced by quantum technology is to integrate itself seamlessly into present cryptographic infrastructure. The encryption algorithms prevalent today should be revisited from the perspective of threat from a quantum computer. In this paper, we demonstrate a practical demonstration and integration of a Differential Phase Shift Quantum Key Distribution (DPS QKD) protocol with commercial router cum encryptor. This QKD protocol is based on a family of Distributed Phase Reference protocol which is best suited for fiber transmission. We have achieved with 1 GHz pulse repetition rate in conjunction with gated single photon detectors, a sifted key rate of 600 Kb/s and secure key rate of 271 Kb/s at 40 km. The quantum bit error rate in our QKD system is less than 4% for the present implementation. We have validated the randomness of the final secure keys generated from QKD in NIST test suite and it has passed all the 15 tests. The QKD system was integrated with a commercial router cum encryptor and we have successfully performed data transmission from a source router to a destination router.

1. INTRODUCTION

1.1

Cryptography is an art of secret writing. The primary objective of cryptography is to protect the authenticity, integrity, and confidentiality of the information being sent. The message (plaintext) is encrypted by an encryption algorithm using an encryption key and delivered to the recipient through a conventional channel in the form of a cryptogram. The encryption algorithm is again applied in an inverse manner to retrieve the message from the cryptogram. The cryptographic key is the most vital part of any cryptographic process, it needs to remain private to ensure any secure communication. All the public key infrastructures use asymmetric keys comprising of public key and private key. The certification authority gives the private key to the key-requester while the public key can be shared over public channel. These keys are used for various cryptographic purposes like encryption-decryption, creation-verification of digital signatures, key transport etc. All the cryptographic algorithms that utilizes these keys for encryption-decryption or any other cryptographic tasks are based on mathematical algorithms ensuring computational security to our data. This computation security is based on the capability of classical computers. In quantum information theory, the information is processed by the laws of quantum mechanics which provides huge computational power and there are quantum algorithms which can break prevalent classical cryptographic algorithms like Diffie–Hellman (DH), Rivest Shamir Adleman (RSA) and Elliptic-curve cryptography (ECC) on a large-scale quantum computer. The threat lies if the encrypted data-in-transit is copied today then, it can be later decrypted by anyone who will have an access to the quantum computer. Therefore, the efforts by global standardization bodies are towards making present cryptographic backbone quantum-safe. A prospective candidate for quantum-safe encryption is Quantum Key
Distribution (QKD) which is one the most mature fields of Quantum Information Theory. The theoretical security of the QKD protocols are based on the fundamental principles of quantum physics. The composability [1] of QKD allows the keys to be used for other cryptographic primitives for enabling forward security. Differential Phase Shift (DPS) QKD is one of the most prominent QKD protocols in Differential Phase Reference (DPR) QKD protocol family. It can be implemented using standard telecommunication fiber and off-the-shelf components. With respect to QKD performance, DPS has a major advantage over other QKD protocols [2,3] using weak coherent state. The reason being, it is insensitive to multi-photon states. Considering the photon-number-splitting (PNS) attack, the secure key rate of DPS QKD is close to BB84 when performed with an ideal source, in other words it outperforms BB84 protocol with coherent source. In this work, we have authenticated the QKD nodes (Alice and Bob) from 2-universal hash family with prior shared keys required for the same. We have implemented a QKD protocol in fiber medium and performed sifting, error correction using cascade, privacy amplification [4] and finally key reconciliation. In section 2, we have mathematically explained the QKD protocol, in section 3 we have briefly discussed the eavesdropping techniques on quantum channel, in section 4 we have explained our experimental setup, in section 5 we have discussed the quantum-safe network and integration in the commercial router system and in section 6 we have concluded our work.

Fig. 1. Schematic of DPS QKD. The intensity modulator (IM) generates the pulses, phase modulator (PM) modulates the optical signal, thereafter it is attenuated by an attenuator (ATT) and passed through a quantum channel (QC). Bob has DLI is Delay line interferometer (DLI) and he detects the photons using InGaAs based Single Photon Detector (DPD).
2. QKD PROTOCOL

2.1

In QKD, the carriers of binary information are a quanta of light. Ideally, it is a single photon Fock state. Single photon sources are difficult to realize experimentally, this is the reason that QKD is mostly implemented by faint laser pulse/weak coherent source. This kind of source obeys Poisson statistics. We have demonstrated the DPS QKD protocol using weak coherent source between sender Node 1 (Alice) and receiver Node 2 (Bob). The schematic is presented in Fig. 1. Each pulse is randomly phase modulated by phase 0 or π by a phase modulator according to the random numbers which are generated by a random number generator. These random numbers form Alice’s raw key. She applies a π phase when the raw key is 1 and 0 phase when raw key is 0. She attenuates the Weak Coherent Pulses (WCP) to a mean photon number of $\mu = 0.1\mu = 0.1$. Alice sends them to Bob through a quantum channel (QC). Bob receives the travel photons, demodulates them through Delay Line Interferometer (DLI) and detects them randomly. Precisely, the WCPs that reaches the Bob’s side enters the one-bit DLI which comprises of two beam splitters and an optical delay of 1-bit in one of it’s paths. After interference at the second beam splitter the photon is detected by either (ideally) of the two single photon detectors obeying the laws of interference. Bob announces the time-slot where he has received the detection. Alice computes her sifted key from Bob’s announcement. Bob randomly select a small fraction of keys to give an estimate of the error rate. If the error rate does not exceed the threshold error rate then Bob initiates the post processing algorithms like error correction, privacy amplification and key reconciliation to finally generate secure keys which can be used for cryptographic purposes. Mathematically, this train of weak coherent states is represented by

$$\left| \psi \right> = \otimes_{i=1}^{n_p} e^{i(\phi_r + \phi_i)} |\alpha\rangle_{s_i}$$

$$= \otimes_{i=1}^{n_p} (-1)^{s_i} e^{i\phi_r} |\alpha\rangle_{s_i}$$

(1)

2.2

where, $\phi_r$ is the reference phase, $\phi_i$ is the phase induced on the weak coherent state $|\alpha\rangle$ by the phase modulator and $n_p$ is the number of pulses in the coherence time. Bob can detect an event at different time-slots say $j^{th}$ time-slot due to superposition of $n_j$ and $n_{j+1}$ coherent pulses. Valid time-slot is when detection occurs at $1 < j < n_p - 1$. When valid detection occurs then Alice calculates the sifted key as $s_j \otimes s_{j+1}$ and Bob’s sifted key is generated from the detector which has clicked, if detector which clicks on Logic 0 (1) has detected an event then sifted key is 0 (1). Thereafter, Alice and Bob perform error correction and privacy amplification to arrive at final secure key. We can define a bosonic operator as $\hat{\psi} = \frac{1}{\sqrt{2}} e^{\frac{\beta}{2} + \frac{1}{2} s_{n_p}} e^{i\phi_r} a_{n_p}$ where, $a_{n_p}^\dagger$ is the creation operator for a photon in time-slot $n_p$.

We assume that the time-slots do not overlap and hence these operators can commute with each other. A weak coherent state can be written as $|\alpha\rangle_n = e^{\frac{|\alpha|^2}{2}} \sum_{i=0}^{\infty} \frac{|\alpha|^i}{\sqrt{i!}} |n\rangle$, therefore, we can write the state in equation (1) as

$$|\psi\rangle = \sqrt{P(j)} e^{ij\phi_r} \left( \frac{\psi^\dagger}{\sqrt{j!}} |0\rangle \right)$$

$$= \sqrt{P(j)} e^{ij\phi_r} |\psi_j\rangle$$

2.3

where, $P(j)$ is the Poisson distribution with an average photon number $\mu_{eff} = n_p \mu$. If we consider coherence time to be infinite then we can represent the state as
where \( n_{ts} \) is the number of pulses in the coherence time of the laser, \( \phi_k \) is the phase of the time-slot and \( k \) is the time-slot. Let us consider that there are just 3 pulses in the coherence time, thus equation becomes

\[
|\psi\rangle = \left[ \frac{1}{\sqrt{3}} e^{i\phi_1} |1\rangle_1 + e^{i\phi_2} |2\rangle_2 + e^{i\phi_3} |3\rangle_3 \right] \otimes \cdots \otimes \left[ \frac{1}{\sqrt{3}} \sum_{k=1}^{3} e^{i\phi_k} |k\rangle_{pn} \right].
\]

Basic assumption is that Eve does not possess the phase reference thus, the state appears as that to be averaged over the different values of phase resulting in a mixed state

\[
\rho = \sum_{j=0}^{\infty} P(j) |\psi_j\rangle\langle\psi_j|.
\]

### 3. EAVESDROPPING ON DPS

#### 3.1 The average number of photons per pulse is \( \mu \leq 0.1 \). Thus, the number of photons is much smaller than the number of phase difference i.e. \( ph < n_{ts} - 1 \). We can safely interpret that the total wave-function cannot be recreated with measurements. Thus, security of DPS is based on the non-orthogonality of a wave-function spanned by many time-slots. This forms the basis of security of DPS QKD. We will review the security of the protocol from the perspective of realistic attacks on the protocol and security loopholes due to non-ideal implementation.

#### 3.2 Intercept and resend attack: Intercept and resend (IR) attack is a type of Individual attack. Eve will have a setup similar to that of Bob. She will intersect and measure all pulses. If she detects any photon in a particular time say at \( t \) then, she will resend a pair of WCPor a photon in superposition of two pulses with similar phase difference between them. If Bob measures them at that particular time then, he cannot detect Eve but if he detects them at times \( t \pm 1 \) then it induces 25% error at Bob’s detection setup. If Eve attacks only 4\( e \) of the photons, then Eve can learn 2\( e \) of the fraction and will not have any information from a fraction 1 - 2\( e \).

### 3.3 Beam Splitter Attack: In beam splitter attack (BS) [5], Eve will place a beam splitter in the quantum channel (as the name goes). Eve has to apply a strategy which can have a lossless channel or substitute the quantum channel from beam splitter to Bob by a lossless channel. She will obtain the fraction of photons equal to channel loss without disturbing the communication rate. The probability that Eve will know the value of bit at a particular time given Bob detected a photon at that time is

\[
\mu(1 - T) \approx \mu \text{ without quantum memory and } 2\mu(1 - T) \approx \mu \text{ with quantum memory, where } T \text{ is the transmission efficiency of channel.}
\]

#### 3.4 Photon-number-splitting Attack: In Photon-number-splitting (PNS) attack [6], Eve measures the photon number using state preserving operation. She can store \( \mu_{eff} T \) in her quantum memory and send \( \mu_{eff}(1 - T) \) to Bob. She will measure it after Bob reveals the time of detections. How much information is gone to Eve from each photon she stores? If Eve has \( k \) photons then she has \( k \) copies of the state \( \hat{\psi}|0\rangle \) which she can measure later. Eve entangles her probe with the sent photons and measures this probe after Bob’s announcement. This is a general positive-operator valued measurement (POVM) attack on single photons. Since, Eve does not know the phase reference hence it will be sent as

\[
\rho = \sum_{\phi_1 \phi_2 \cdots \phi_k} p(j \phi_1 \phi_2 \cdots \phi_k) |\psi_j\rangle\langle\psi_j|.
\]
3.5 Comparison with BB84

(a) In DPS QKD Eve’s information from PNS attack is independent on channel loss. It is a function of $\mu$. Final key rate decreases linearly with channel loss. Hence its robustness against PNS attack is evident.

(b) In BB84, Eve’s information from PNS attack is dependent of channel loss. Thus, if losses are higher then Eve can send multi-photon fractions and stop single photon states. In other words as loss increases Eve can have information over large fraction of key. Hence, final key rate is a quadratic function of channel loss. In Fig. 2 we have shown the key rates with distance for an ideal source, weak coherent source and decoy for BB84 and compared it with DPS QKD (considering restricted attack) using standard experimental parameters.

3.6 Sequential Attack: Sequential attack (SA)[7] is a type of IR attack. Eve places measurement device very close to Alice. She waits for $k$ consecutive clicks and then constructs $k + 1$ time-slot state. The error induced by it is

$$e_{seq} = \frac{1}{2(k+1)}$$

This happens because of probability of measuring side time bins is $\frac{1}{k+1}$ hence error is $\frac{1}{2(k+1)}$. The probability of $k$ consecutive clicks is $p_k = \mu^k$. Therefore, probability of observing $k$ consecutive clicks decreases with $k$ consecutive clicks. Eve needs to conserve overall detection rate thus, $p_k \geq \mu T$. This gives an upper bound for $k$. Eve knows anything if it clicks for $2 < k < k + 1$ with probability $\frac{1}{k+1}$. (since $k$ and $k + 2$ will give random
result). The average collision probability is
\[ P_c = P_{c_0}^n = \left( \frac{1}{2} \right)^{n(1-2ke)} \]
Compression factor is
\[ \tau = \log_{10} P_c^n = 1 - 2ke = 1 - 2e \left( \log_{10} T + 1 \right) \]
According to a study [3,7] it is advantageous to do individual attack (IA) than SA and that security against IA implies security against SA. Eve can employ different strategies to reduce the error rate. She can modulate the envelope of the pulse block so that the amplitudes of the end pulses are smaller than that of the central pulses. A lot of research has been done on sequential attacks on DPS QKD. Several studies have been reported on sequential attacks. However, the strategy [8] that utilizes Unambiguous State Discrimination (USD) for phase differences and optimized pulse envelope, is considered threatening for long-distance DPS QKD. However, to combat this attack, solutions like decoy strategy and strategic phase modulation at Alice Node can be exploited to combat the sequential attacks based on intensity modulation.

3.7 Unconditional Security: Coherent attacks are the most challenging attack on any QKD systems and the security against it is difficult to prove. Several studies have been reported on different strategies of coherent attack on DPS QKD where they attack: pairs of adjacent pulses, noiseless DPS QKD and block randomization. In[3] it is analyzed that COW and DPS are similar in QKD performance however, DPS is somewhat better than COW [9]. The scientific proof of any QKD protocol is dependent upon construction of the QKD scheme and in its realistic implementation. In every security proof some assumptions will be considered and it is very important to see that these assumptions do not open any security loophole from product perspective. It is to be noted that unconditional security by coherent state based DPS QKD is proven in [10] using complementarity approach.

3.8 Quantum Hacking: There are certain demonstrations of quantum hacking on DPS QKD based on inefficient detectors. These hacking [11,12] can fall into IR attack. It exploits the drawback like detector efficiency mismatch, functioning of detector, thermal effects etc. These are basically the side channel attacks. These can be prevented by effective monitoring of the transmission and error detection. Security patches i.e. by strategic detection setup, adding optical components at Bob’s side, monitoring the power, are effective in preventing such hacking. Eve also needs to plan execution of such attacks for which she makes some assumptions of the QKD system. We can conclude that these side channel attacks can be detected by proper countermeasures and effective monitoring.

4. EXPERIMENTAL SETUP

4.1 In Fig. 3, we have shown the experimental setup, we have used a 1550 nm continuous wave laser. It is passed through Lithium Niobate (LiNbO\textsubscript{3}) Intensity Modulator (IM) to generate 1 GHz train of pulses with 400ps width. Chromatic dispersion of DLI is 1ps/nm and SMF fiber is 18 ps/(nm.km). We find that the chromatic dispersion has negligible effect. The train of pulses are phase modulated by (LiNbO\textsubscript{3}) based phase modulator at random and thereafter, strongly attenuated using variable optical attenuators (VOA). The weak coherent source is then passed through the quantum channel which is a standard telecommunication fiber to reach Bob. The random numbers for phase modulation are generated from a random number generator (PRNG). The train of WCP travel to Bob system via QC. At Bob’s side we have a Mach-Zehnder interferometer with 1 ns delay which is fine tuned to match the path difference between consecutive WCPs to cause interference.
The WCP are randomly detected by single photon detectors. Probability of detector getting clicks is $p_{\text{click}} = p_{\text{sig}} + p_{\text{dark}} - p_{\text{sig}}p_{\text{dark}}$. However, the probability of simultaneous click due to signal and dark count i.e. $p_{\text{sig}}p_{\text{dark}}$ is very small. Therefore, $p_{\text{click}} \approx p_{\text{sig}} + p_{\text{dark}}$.

The probability of signal $p_{\text{sig}}$ is $\mu T$, where the channel transmission is given by $T = 10^{-10 (al + L_{\text{DLI}})}$, $al$ is the fiber attenuation, $L$ is the distance and $L_{\text{DLI}}$ is the total loss from Bob’s optics. The Quantum Bit Error Rate (QBER) is an important parameter in QKD protocol and it depends on the electronics, optical error and detector parameters. We have considered following errors:

$$QBER_{\text{Total}} = QBER_{\text{photon}} + QBER_{\text{phasejitter}} + QBER_{\text{darkcount}} + QBER_{\text{phase}}$$

The total $QBER_{\text{Total}}$ is estimated to be 3.9%.

The secure key rates for DPS QKD is given by $R_{\text{sec}} = R_{\text{sif}} (\tau + f(e)h(e))$ where sifted key is obtained by $R_{\text{sif}} = \mu T v$. Secure key rate considering realistic attack (IR attack and BS attack with quantum memory) is given by $R_{\text{sec}} = R_{\text{sif}} (1 - 2\mu (1 - T) - 2e + f(e)h(e))$

Secure key rate considering general individual attack (PNS attack) is given by $R_{\text{sec}} = R_{\text{sif}} \left( -\frac{1}{2} \left[ 1 - (1 - T) \right] \log_2 \left[ 1 - e^2 - \frac{(1-e)T}{2} + f(e)h(e) \right] \right)$

. Secure key rate for sequential attack is given by $R_{\text{sec}} = R_{\text{sif}} \left( 1 - 2e (\log_\mu T + 1) - f(e)h(e) \right)$

We have calculated the sifted and secure key rates based on the experimental parameters shown in Table 1a. In Fig. 4, we have presented a test case where we have shown the SPD counts when Alice sent Logic 0 continuously (00000 i.e. a fixed pattern). We find that port 1 is always giving constructive interference while port 2 is always giving destructive interference. When we change to 01010 pattern from Alice side, we find that port 1 always shows destructive interference and port 2 shows constructive interference, this is shown in Fig. 5. After generating secure keys, we have ensured the randomness of the key through NIST test suite [13] because the keys will be used for cryptographic purposes. In Fig. 6, we have shown the NIST test results on the keys after key reconciliation process. The computing elements CE1 (Alice side) and CE2
(Bob side), address the sifting, authenticity, error correction, privacy amplification and reconciliation activities. This subsystem also implements quantum enabled Internet Protocol Security (IPsec) and VPN protocols for communicating between Alice and Bob over a standard internet network. In Fig 7, we have shown the sifted and secure key rates for different distances. We have also specified the key rates in Table 1b.

**Table 1**: (a) Parameters of Critical Components in the QKD Experiment and (b) Summary of QKD Experiment

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mean photon number</td>
<td>0.1</td>
</tr>
<tr>
<td>Pulse width of WCS</td>
<td>400ps</td>
</tr>
<tr>
<td>Optical loss at Bob</td>
<td>4 dB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distance (km)</th>
<th>Sifted key (kbit/s)</th>
<th>Secure key rate</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Restricted (kbit/s)</td>
<td>Individual (kbit/s)</td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>1585</td>
<td>694</td>
<td>326</td>
</tr>
<tr>
<td>40</td>
<td>631</td>
<td>271</td>
<td>122</td>
</tr>
<tr>
<td>60</td>
<td>251</td>
<td>104</td>
<td>41</td>
</tr>
<tr>
<td>80</td>
<td>100</td>
<td>37</td>
<td>9</td>
</tr>
<tr>
<td>100</td>
<td>40</td>
<td>11</td>
<td>-</td>
</tr>
</tbody>
</table>

*Table 1 (Contd.)...

**Fig. 4**: Counts at (a) Port1 and (b) Port2 of the DLI when Alice raw keys has generated only logic 00000. (fixed pattern is given).

**Fig. 5**: Counts at (a) Port1 and (b) Port2 of the DLI when Alice raw keys has generated only logic 010101 (fixed pattern is given).
Fig. 6: Results of the NIST Tests Applied to the Final Secure Keys

Fig. 7: Key Rate vs Distance for DPS QKD
5. QUANTUM SAFE NETWORK

5.1
Transforming present network security into quantum-safe is one of the biggest challenges faced by International standardization bodies like ETSI, NIST, CSA etc. The QKD has been successfully demonstrated, deployed, and applications in industry and government are growing. We present below application and scenarios from technical perspective. We have presented the integration of our product with commercial router thereby demonstrating point to point QKD within 40 km.

5.2 Application 1: Key Generation in a QKD Network

5.2.1
QKD network comprises of multiple nodes that are connected to form a quantum network. With our present system we can generate secure keys at a modest rate till 80 km. The nodes may contain multiple ‘Alice’ and ‘Bob’ combinations depending on the network topology. These nodes contain QKD stack that communicates with the adjacent nodes and learns about the routes required for reaching other nodes. The information transfer needs to happen between entities R1 and R3, which has to be encrypted. R1 requests key from QN1 for encrypting the data. QN1 passes key K1 to R1. R3 will request QN4 for corresponding key. QN1 finds the route to QN4 through the network (QN1-QN2-QN3-QN4). Using quantum hopping technique, key gets transferred to QN4. QN4 further transfers key K1 to R3. R3 after receiving the key K1 from QN4, decrypts the information.

5.2.2
We have configured our system for implementation of the trusted node concept [14] as presented in Fig. 8 to increase the distance. The scalability of the computing element and flexible architecture in our product allowed us to evaluate point-to-multipoint QKD networking and multi-hopping scheme integration of classic cryptography with quantum cryptography to ensure quantum-safe key management across all different layers of information and communication technology.

![Fig. 8: QKD Network with Trusted Nodes](image-url)
5.3 Application 2: Quantum Key Transportation between end Applications

5.3.1
To understand the key transfer from one quantum node to the other, where two end applications are asking for the quantum keys between them, consider the scenario depicted in figure. In this scenario, user ‘A’ wants to communicate with a user ‘B’ securely. The Quantum key (QKey) from quantum node (QN1) is produced and transported to the end quantum node (QN3). Application ‘A’ asks for a QKey to QN1 via KMIP interface. The QN1 finds the route to reach ‘B’ and selects the best route via QNs QN1→QN2→QN3. QN1 generates QKey ‘K1’ with QN2. QKey ‘K1’ is passed to R1. QN2 and QN3 create a VPN using QKeys with strengthened hash function. After which using OTP1 send key ‘K1’ to QN3. QN3 transfers QKey to R3.

5.4 Application 3

5.4.1
We have implemented a few solutions based on ETSI recommendations [15].

5.4.2 Layer 2
(a) As a key exchange protocol for PPP
(b) In IEEE 802.1MACsec
(c) QKD link-encryptor for encrypting traffic on an Ethernet of fiber channel link
(d) QKD link-encryptor as VPN tunnel
5.4.3 Layer 3

IPsec defines the architecture for security services for IP network traffic. It includes 3 main protocols: Internet Key Exchange protocol (IKE), Authentication Header protocol (AH) and Encapsulating Security Payload protocol (ESP). IKE is used to manage the cryptographic keys and also initiate the security associations required for the secure data transfer. AH and ESP will provide the necessary integrity and confidentiality required for the data being transferred. QKD solves the key distribution problem by allowing the exchange of a cryptographic key between two remote parties with absolute security, guaranteed by the laws of quantum physics. So, to combine the advantages of QKD with the structure of the IPsec, the key exchange in IKE (Phase 1 and 2) should be replaced by the QKD system to provide the secure key on both end points. These keys can be used to create a session (Handshake) between the two nodes with the Security associations discussed and also the authentication and encryption supported by these keys. The DH, RSA are the currently used public key exchange algorithms that depend on the computational complexity of factorization of the multiplication of two huge prime numbers, which increases exponentially with the size of the prime number. This complexity can be brought down exponentially using Shor’s algorithm after the onset of quantum computers, thus making the key exchange unreliable. Also, the current standard method of hashing (SHA2) is an extended version (increased tag length from 160 to 256) of the already failed SHA1 algorithm which had a weak collision avoidance probability. This should be replaced by an Information theoretically secure universal hashing algorithm which provides for the mapping of every key bit used for the authentication with every bit of the message thus providing maximum randomness for the input key length. Modified IKE to provide shared session keys for security association in IPsec protocol.

5.5 Application 5: Practical Demonstration for Point to Point QKD

5.5.1 Layer 4

(session keys): We have successfully integrated our QKD with a commercially available router and this is shown in Fig. 9. The keys are requested by the source router as and when needed. The quantum node at the source end provides the key to the source router along with the key ID. The source router communicates the key ID to the destination router. The destination QKD passes the corresponding key. In this technique, both the source router and destination router will refer to the same key in a secure way while encrypting data-in-transit.
**Fig. 10: Integration of QNU QKD with Commercial Routers cum Encryptor**
5.6 Application 4: Highly Secure

5.6.1

In Fig. 11, we have presented an application for secure defense communication. The entire network can be quantum secured in the prescribed manner which is connected from Army Office 1 to Army Office 2. The quantum channel and classical channel are depicted differently as they serve different purposes. The keys generated by QKD are symmetric and information theoretic secure with composable security framework. This will be shared securely to encryptor/decryptor, which can then be shared with different applications that will want to access the keys.

6. CONCLUSIONS

6.1

We have performed a 1 GHz pulse rate DPS-QKD experiment utilizing InGaAs detectors. We have successfully generated random quantum keys which can be used for any cryptographic purposes. We have also discussed the present security status of DPS QKD including theoretical and implementation security. This protocol is recognized by ETSI and is in the process of becoming as one of the standards for QKD protocol. We have also brought forth the requirement for transition from current cryptosystem into quantum safe encryption as per the ETSI recommendations. We particularly emphasize on transition of classical network security to quantum-safe network security and moving forward in that direction we have reported the integration of our system with commercial router and successfully performed data transmission from a source router to a destination router.

REFERENCES


15. Quantum Safe Cryptography; Case Studies and Deployment Scenarios, ETSI GR QSC 003 V1.1.1 (2017-02)
Future of Cryptography: Quantum Key Distribution through Micro-Satellites

Col Kapil Jaiswal

Abstract—Information security is becoming a critical issue in satellite constellations, because the amount of critical and valuable data to be communicated is increasing. Satellites based Quantum Communication (Q.Comn) is the most efficient way to achieve intrinsically hack-proof secure Quantum Key Distribution (QKD) because unavoidable losses restrict scaling up fiber based Q.Comn. The recent advancement in satellite technology are indicative of real potential to allow a global scale QKD. Recently a 600-kg Q.Comn satellite has been launched into orbit successfully demonstrating quantum teleportation experiments. However, it remains a greater challenge to demonstrate Q.Comn with a small-size and low-cost satellite. If Q.Comn could be achieved using a micro-satellite, the paradigm of satellite communications would change. This paper assesses the latest advancement in satellite technology in conjunction with an iterative Size, Weight and Power (SWaP) optimization process to do feasibility analysis for designing simplest, smallest, lightest and least power-consuming satellite system capable of Q.Comn with an operationally viable key rate.

1. INTRODUCTION

1.1 The security of quantum communication (Q.Comn) is based on fundamental and immutable laws of physics and not on the hope that a problem is too difficult for an adversary to solve. Naturally, this future-proof and unconditionally secure communication technology has a large impact on global communications. Attempts to overcome the limits imposed by losses and create a global satellite based network are underway. However these efforts are gigantic and involve incredibly complex ultra-modern satellites which are extremely expensive. Whereas smaller mini / micro satellites based on CubeSats architecture can be constructed and launched for a fraction of the bigger satellite cost. The study of previous long distance implementations via optical fiber [1], free space terrestrial links [2] and the successful 600 kg class [3] large satellites is undertaken. By analyzing the results of these proof-of-concept missions and evaluating their performance in both the uplink and the downlink scenario, it is assessed that benefits due to the fractionally larger key rate during downlink are completely outweighed by the lower cost, ease of operation and simplicity offered by an uplink to the satellite. Additionally, an uplink allows for a larger variety of implementable Q.Comn protocols (i.e., future-proof nature). This is because many different Q.Comn Protocols (e.g.,E91 [4], BB84 [5], decoy state protocol (DSP) [6], BBM [7], B92 [8]) rely on nearly identical detection schemes for the receiver and can thus all be implemented on mini satellites.

1.2 The timing resolution of the single photon detectors enables pulse-position-modulation in classical communication from ground to space, with exceptionally fast data rates. The present generation extremely sensitive single photon detectors with exceptional cadence and narrow FOV are proposed for Q.Comn and drive the design for the satellite infrastructure.
2. QUANTUM COMMUNICATION PROTOCOLS

2.1
Two most common Q.Comm protocols E91 [4] and the Decoy State Protocol (DSP) [6] are considered in this study. In both, information is encoded in the polarization state of single photons at the ground station (Alice) who then sends these states to the satellite (Bob). Bob measures the polarization of the received photons in a set of randomly chosen bases. The protocol is divided into several individual “trials”. In each trial, one state is sent and received. The techniques used to identify each trial depend on experimental implementation and protocol. To ensure that the key is secure, Alice and Bob perform statistical tests (i.e., compute the Quantum Bit Error Rate (QBER $E$) and/or perform a Bell test) on the data they measured from several trials. Thus, they also need a form of (insecure but authenticated) classical communication. To obtain the key, Alice and Bob need various post-processing (PP) steps that vary between protocols. Importantly, the larger the measured QBER, the more information an eavesdropper (Eve) could, in principle, obtain about the key. Thus the number of secure bits of key that can be exchanged per second depends on the QBER. The key difference between the protocols is that E91 exploits quantum entanglement of photons to obtain mutually shared randomness (the key) between the two parties. In DSP however, Alice encodes information by randomly choosing the polarization of an emitted weak coherent pulse. Alice must also randomly choose the average intensity of each pulse (to designate it as a signal or decoy pulse) in order to avoid a photon number splitting attack. Thus each protocol needs a different source on ground as seen in Fig. 1.

3. EXPERIMENTAL INFRASTRUCTURE AND MINI SATELLITE

3.1
The proposed experimental setup will consist of a Optical Ground Station (OGS), which is connected either to one arm of a source of polarization entangled photon pairs (for Q.Comm protocol E91) or to a pulsed laser with randomly chosen polarization and mean photon number for each pulse (for Q.Comm protocol DSP). The signal photons are transmitted to the CubeSat in a 500 km low-earth orbit (LEO) via a free-space link. OGS and CubeSat point beacon lasers at each other for precise attitude control. The quantum signal is analyzed on board the CubeSat using a randomly switched half-wave plate (HWP) and a polarizing beam splitter (PBS). Measurement outcome, basis choice and time tag of each event are recorded. Information about the latter two is transmitted to the OGS using a classical radio frequency (RF) link. The OGS identifies the matching bits using a cross-correlation analysis and tells the CubeSat which ones to use. Both disregard the other bits, perform post-processing and then share a sifted key.
4. **LINK BUDGET & ERROR CALCULATION**

4.1 The security proofs for both E91 and DSP show that a secure key can be exchanged only if the QBER $E$ is below a certain value. For E91, the overall limit is $11.0\%$ assuming optimal classical PP with error correction efficiency $f = 1$. Realistic PP techniques limit to $10.2\%$, assuming a PP efficiency of $f = 1.1$. For DSP with the same $f$ and assuming the standard values, the limit of is $6.2\%$, requirements can be reformulated in terms of the more familiar Signal to Noise Ratio (SNR) as

\[
SNR = \frac{1}{E} - 1. 
\]

The secure key rate (i.e., bits per second) for E91 protocol $R_{E91}^s$ is

\[
R_{E91}^s \geq \frac{1}{2} \frac{Q_{E91}}{\tau} \left[ 1 - (1+f)H_2(E_{E91}) \right], 
\]

where $Q$ is the bit error rate, $\tau$ is the transmission time, and $H_2$ is the binary entropy function.

The secure key rate for DSP protocol is

\[
R_{DSP}^s \geq \frac{1}{4} R_{DSP} \left[ Q_{DSP} (1 - H_2(E_{DSP})) - f Q_{DSP} H_2(E_{DSP}) \right]. 
\]

4.2 where the factor $\frac{1}{4}$ is due to the fact that only half of the photons are measured in the right basis and another half are non-usable decoy.
states. Rep is the repetition rate of the DSP source. Analogous to Eq.2. The total link loss to the satellite, \( \Lambda_B \), for E91 (DSP) must be better than \(-62.7 \text{ dB} \) (-61.2 dB) in order to obtain a secure key, i.e. achieve a SNR of more than 8.8. Accounting for losses in the apparatus of Alice and Bob, the maximum tolerable link loss \( \Lambda_L \) from sending lens to receiving lens alone, is \(-43.6 \text{ dB} \) (-42.2 dB) for E91 (DSP).

5. PRELIMINARY DESIGN

5.1

The advantage of the uplink scenario is that most of the mission’s complexity is ground based and multiple protocols/experiments can be implemented. Consequently, to better assess the Q.COMm over CubeSat design problem, first the design of the optical ground station (OGS, Sec. 5.1) is analysed and then that of the CubeSat (Sec. 5.2). Fig. 1 shows an overview of the experiment consisting of space and ground segments. Fig. 2 shows a block diagram of all payload components necessary for the Q.COMm mission.

5.2 The Ground Segment

The design constraint of support of at least two Q.COMm protocols by proposed CubeSat mission, each of which require different sources within the OGS is enforced from initial modeling stage. E.g. the E91 protocol requires an entangled photon source with a pair production rate \( R_{PE91} = 100 \text{ Mcps} \) and an intrinsic heralding efficiency \( \Lambda_H = 85\% \) (-0.7 dB). For Alice to detect these extreme count rates on ground, using multiplexed arrays of superconducting nano wire single photon detectors (SNSPDs) with a detection efficiency \( \eta_A \) of 70\% (85\% for one single SNSPD without multiplexing) and a total timing jitter (including electronics) \( t_A \) of 16ps (15 ps for the SNSPD alone) is proposed. This results in a total \( \Lambda_A = \eta_A \cdot \Lambda_H = 60\% \) (-2.3 dB) and a ground based detector noise rate of less than 100 cps which is ignored in comparison to the total E91 singles rate of \( R_A \approx 60 \text{ Mcps} \). Similarly, the DSP requires a source capable of producing a controllable mean photon number per pulse \( \mu_{DSP} \approx 0.64 \) (0.1) for the signal (decoy) pulse where 50\% of all pulses carry a signal with a repetition rate of \( >1 \text{ GHz} \).

5.3 The CubeSat

5.3.1

The basic block diagram of the mini satellite based on CubeSat architecture is shown in Figure 2. Components in brown are those used for quantum communication while those in green relate to the pointing, acquisition and tracking system. Other essential subsystems are blue. (TTM: Time Tagging Module, RNG: Random Number Generator). The subsystems can also be classified based on the type of components used as indicated by the grey dashed lines. All components are fixed to the CubeSat frame, communicate with the main CPU and supply/draw power to/from the CubeSat bus (all of which are not shown). The CubeSat requires several subsystems as listed in Table 2.

5.3.2

For a 3U CubeSat, these components must fit within 0.0032 m\(^3\), weigh less than 4 kg and consume less than 21Wh per orbit (with expandable \( \approx 30\times30 \text{ cm}^2 \) off-the-shelf solar panels). Through an iterative process of SWaP design and analysis the requirements of the CubeSat have been optimized based on the available technology. This section discusses the tradeoffs, design choices and compromises are discussed in Sec. 5.3. Here focus is on the quantum payload which consists of receiving telescope, basis choice, polarization analysis and detection subsystems (see Fig. 3). All optical losses are estimated within the CubeSat (between telescope and detectors) to be \( \Lambda_{OB} = -1.0 \text{ dB} \), using only standard commercially available devices.
5.3.3

The signal and beacon beams from ground are collected by a Cass grain-type mirror telescope. The back side of the secondary mirror carries the earth-facing beacon laser necessary for tracking of the CubeSat. The input Signal and beacon are separated by a dichroic mirror (DM). The latter is tracked with a fast quadrant detector for precise attitude sensing and clock synchronization while the former passes a binary liquid-crystal-based half-wave plate switch (LC-HWP). It randomly shifts the polarization of incoming photons by either 0 or π. This effectively acts as a measurement basis switch in combination with the polarizing beam splitter (PBS) separating horizontally (vertically) polarized photons by transmitting (reflecting) them. The second PBS is used for enhanced extinction ratios. Long pass (LP) and interference filters (IF) are used to block out stray light and the photons are detected by silicon-based avalanche photo diodes (APD).
5.3.4

\( R_{BG} \) are the erroneous measurement clicks due to near-infrared noise photons originating from the ground area which are not blocked by the spectral filters. If the orbit height is fixed (chosen 500 km), \( R_{BG} \) can only be reduced by reducing the field of view (FOV = \( d_B / f_B \) where \( f_B \) is the CubeSat telescope’s effective focal length). This has two additional benefits: A long \( f_B \) improves the polarizing beam splitter’s (PBS) extinction ratio since it reduces the divergence of the impinging beam within the PBS. More importantly, a small \( d_B \) strongly reduces the radiation damage to the detector due to its small cross sectional area. However, the FOV must be large enough to maintain the OGS in view despite the pointing errors of the CubeSat.

5.3.5

To achieve an optimal \( f_B \) a Cassegrain-type reflector is a good choice for the receiving telescope despite the increased telescope loss \( \Lambda_T \) due to the secondary mirror (which is estimated to be -1.5 dB in total). This is because the overall design is lightweight and the required \( f_B \) of 40 cm can be realized with a 10 cm long telescope. The telescope covers the CubeSat’s quadratic \( Z^+ \) surface of about 9 x 9 cm. For simplicity, calculations assume a circular telescope with \( D_B = 10 \) cm.

5.4 Preliminary SWaP Analysis

5.4.1

The results of Size, Weight and Power (SWaP) analysis along with a complete list of subsystems and their control circuits is given below in Table 2. “Energy per orbit” refers to consumption per one full orbit while performing a quantum measurement and takes into account different operation times for each device. The strict limitations of SWaP consumption pose significant challenges to the satellite design. Using commercially available products, optimization of the secure key rate produced by the CubeSat while adhering to the standard restrictions has been done. Results are shown in Table 2. Further customizing of certain parts would significantly lower the total SWaP consumption. The only component that would have to be modified is the time tagger, which is however within reach of current technology. A standard 3U CubeSat is 10x10x34.1 cm excluding the solar panels (with a maximum protrusion limit of 6.5 mm). Another way to gain more space would be to use the less common 4U standard (10x10x45.4 cm).

5.4.2

Exploded view of preliminary 3U CubeSat design is shown in left part of Figure 4. The solar panels as well as any electric connections have been omitted for clarity. The optical elements shown in the red box are out of scale. The right part of Figure 4 depicts Artistic depiction of the 3U CubeSat with expandable solar panels in bird-wing configuration. They are mounted to the sun-facing side of the CubeSat, the other three long sides of the surface can be covered with radiators for detector cooling.

5.4.3

The CubeSat standard weight limit is 4 kg for a 3U, however this requirement can be relaxed to 5 kg depending on the launch provider, which is useful if an operational lifetime of more than 6 months is desired. The operational lifetime is mainly limited by radiation damage to the CubeSat, especially the APDs. Thus, heavier shielding (not included in the current SWaP) would improve operational life times at the cost of a tighter weight budget. The type of solar panels and the orbit of the CubeSat limit the total power production per orbit to 21Wh. Only 87% of this
value is consumed. The satellite is within line of sight of the OGS for a maximum of 11 min (if it passes with 0° inclination), of which at most 220 s can be used for key generation. Thus most subsystems only operate for a fraction of each orbit. Together these consume 17.5 Wh while the always-on systems (attitude control, UHF-band communications, GPS and main computer) consume a further 13.5 Wh per orbit. The CubeSat must operate only at night to avoid excessive background counts. Thus a large set of batteries are necessary. To preserve battery life and provide a safety margin it is assumed that the batteries are never drained by more than 30%. Thus a total battery capacity of at least 58 Wh is needed. The proposed design provides for 60 Wh. The CubeSat consumes a total of 31.9 Wh per orbit but its solar panels can only produce 21 Wh. This means that the CubeSat is capable of a Q.Comn link roughly once every 1.5 orbits.

Table 2: SWaP Analysis

<table>
<thead>
<tr>
<th>Subsystem name</th>
<th>Size (U)</th>
<th>Weight (g)</th>
<th>Peak power (mW)</th>
<th>Energy per orbit (mWh)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Optics + Detection</td>
<td>Telescope</td>
<td>400</td>
<td>9000</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Shutter</td>
<td>200</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Dichroic mirror + PBSs</td>
<td>200</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Phase shifter</td>
<td>200</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Detectors + Shielding</td>
<td>200</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Detector cooling (Peltier)</td>
<td>50</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Ground tracking photo diodes</td>
<td>200</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Measurement control</td>
<td>Phase shifter circuit (100s)</td>
<td>0.05</td>
<td>75</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>Peltier circuit</td>
<td>0.01</td>
<td>50</td>
<td>1000</td>
</tr>
<tr>
<td></td>
<td>Detector circuit (AGI)</td>
<td>0.07</td>
<td>50</td>
<td>150</td>
</tr>
<tr>
<td></td>
<td>Photo diode circuit</td>
<td>0.03</td>
<td>100</td>
<td>500</td>
</tr>
<tr>
<td></td>
<td>Time tagging electronics</td>
<td>0.2</td>
<td>150</td>
<td>19000</td>
</tr>
<tr>
<td>Positioning</td>
<td>Beacon + electronics</td>
<td>0.01</td>
<td>70</td>
<td>1000</td>
</tr>
<tr>
<td></td>
<td>XACT attitude control</td>
<td>0.5</td>
<td>900</td>
<td>2000</td>
</tr>
<tr>
<td></td>
<td>GPS + main computer</td>
<td>0.2</td>
<td>200</td>
<td>1000</td>
</tr>
<tr>
<td>RF Communication</td>
<td>S-band + UHF transceiver</td>
<td>0.26</td>
<td>314</td>
<td>6000</td>
</tr>
<tr>
<td></td>
<td>Antennas</td>
<td>0.07</td>
<td>100</td>
<td>60</td>
</tr>
<tr>
<td>Energy</td>
<td>Batteries</td>
<td>0.1</td>
<td>200</td>
<td>67000</td>
</tr>
<tr>
<td></td>
<td>Solar cells</td>
<td>-</td>
<td>450</td>
<td>31000</td>
</tr>
<tr>
<td></td>
<td>Radiator</td>
<td>-</td>
<td>200</td>
<td>-</td>
</tr>
<tr>
<td></td>
<td>Frame</td>
<td>-</td>
<td>250</td>
<td>-</td>
</tr>
<tr>
<td>Total consumption</td>
<td>7.75</td>
<td>1300</td>
<td>12700</td>
<td>13900</td>
</tr>
<tr>
<td>Available</td>
<td>3.15</td>
<td>6000</td>
<td>97000</td>
<td>112000</td>
</tr>
</tbody>
</table>

Fig. 4: Design of LEO 3U CubeSat for Optical Link
6. PERFORMANCE ANALYSIS

6.1
Having specified the key parameters for the design of proposed CubeSat, the estimate on the amount of secret key the satellite could acquire with two sufficiently separated OGS (Section 6.2) is calculated, for that estimate of the data storage and transmission needs (Section 6.1), was also calculated.

6.2 On Board Computing Requirements

6.2.1
The classical post processing required to obtain a secure key is not trivial and dictates the choice of the on board processing capabilities of the CubeSat. The first step is to identify coincidence events. This is commonly done by computing a timing cross-correlation histogram which can be a computationally intensive task. It is recommended that the CubeSat share the timing of all its detection events with the OGS. The OGS can identify coincidence events and notify the CubeSat. This minimizes the amount of data transferred and the amount of calculations the CubeSat needs to perform. The on board processing of all the $n_{tag}$ time tags should be less than $18n_{tag}$ operations in the worst case. Calculating a sifted a key of length $m_{key}$ is estimated to require roughly $m_{key}$ bits of memory and $15m_{key}$ operations to complete.

6.2.2
Error correction requires additional memory and computational power. About 10 to 20 MB of memory is sufficient for this when using algorithms based on low density parity check codes. In the worst case it is estimated that all these PP steps will require $\approx 258$ million operations per second to calculate the secure key in real time. This can easily be handled by a commercially available space certified on-board computer (OBC) with an ARM9 processor running at 400MHz with enough spare processing power for other satellite tasks.

6.3 Expected Secure Key Rates

6.3.1
The study shows that shown that Q.Comn with a 3U CubeSat is feasible in principle. Observations in existing OGS show that an $r_0$ of larger than 5 cm can be achieved or more than 227 nights per year or 62% of the time. Therefore, assuming a circular orbit with 30° orbital inclination, it can be calculated that for a total of 44,300 s or 12:20 h, each year the link quality is sufficient to perform Q.Comn. The average inclination in zenith as seen from the OGS, $\varphi$, is 28.3°. Computing for such an average orbit and taking the $r_0$ measurements of into account, the total key acquired in one year would therefore amount to 4.0 Mbit (13.0 Mbit) for E91 (DSP).

7. CONCLUSION

7.1
Q.Comn offers the highest security possible. However, it is expensive and communication distances are limited. This complete feasibility study has shown that it is possible to achieve Q.Comn over thousands of kilometers using a relatively cheap and easy to construct mini satellite using CubeSat architecture. By miniaturizing the design, optimizing power consumption and minimizing the weight, full-fledged commercial global Q.Comn can be achieved with a simple 3U CubeSat. This theoretical assessment study can be used as guidelines for building a Q.Comn mission which includes selection guides for the components, trade-offs and optimizations for the secure key rate, choice of orbits etc. Analysis of laser
based alignment advancement suggest that the fine pointing capabilities of CubeSats no longer limit their applicability for Q.Comn and optical links.

7.2

Using proposed CubeSat design, a pair of ground stations can exchange $13 \times 10^6$ absolutely secure bits/year. Key expansion protocols can be used to grow the key with only marginal security implications. A commercially viable Q.Comn satellite needs significant classical computation power, data storage and classical communication bandwidth. This study has evaluated all these requirements and outlined strategies to achieve all this with minimal resources. In the current design, the CubeSat is a trusted node and has the potential for usage scenarios like QKD between multiple entities of critical organizations.

REFERENCES
2. Ursin, R., Tiefenbacher et al.: Free-space distribution of entanglement and single photons over 144 km.
3. Yin, J., Cao, Satellite-based entanglement distribution over 1200 kilometers 356(6343), 1140(1144).
Abstract—Network forensic tools based on deep Packet Inspection (DPI) technology are crucial network level operational security controls for protecting networks from emerging and sophisticated attacks. However, it is becoming increasingly difficult to implement DPI based network forensic systems effectively due to the rising need for more complex analysis, along with the unstoppable growth in the volume of network traffic that these systems must inspect. To address these challenges, future cost effective anomaly detection technologies must exploit the power of emerging highly concurrent multi-core platforms. Unfortunately, current systems severely limit their use of parallelism by either resorting to coarse-grained load-balancing or incapability of Linux kernel network stack to make use of multi core efficiently. In this paper we proposed a comprehensive approach that introduces parallelism across all multi-core commodity CPUs like Intel X86 or ARM. We investigate kernel independent network application strategies that take existing DPI analyses and anomaly detection systems, automatically parallelize their processing over multi-core hardware.

1. INTRODUCTION

1.1
Cyber security is both national and economic security issue. Governments & institutions are waging worldwide battle in cyber space every day to protect critical infrastructure and intellectual properties. Today’s wars have become borderless due to uncontrolled distribution of internet networks. Once systems are connected to the outside wide area networks (WAN), the threat scenarios also multifold. Every IT enabled mature organizations are prone to such attacks if no proper security controls are in place. In order to counter threats, every security focused organization must equipped with computer incident response teams. This entity may consists of single individual or small group of people highly expert in computer and network security. Whenever any security breach noticed these teams conducts thorough investigations. During their investigation they collect rich amount of network data, analyzes this data to find compromised assets, owners of the asset, point of intrusion, time of intrusion and quantifies data loss. In this complete process, investigators requires sophisticated forensic tools and software. One of such tool is deep packet inspection based network forensic tool which provides ability to examine protocol headers and payload of packets. It enables specific action such as anomaly detection along with the guaranteeing the transmission quality can be perform on them.

2. TECHNICAL CHALLENGES FOR HIGH PERFORMANCE NETWORK FORENSICS ON COMMODITY HARDWARE

Today there are various challenges to carry network forensics because of the explosive growth of Internet and high bandwidth applications, in terms of both host and network speed results in rapidly increasing network load. Additionally, network speed tends to
increase faster speed than CPU and memory speed causing gap between network and end system speed. For example today 10Gbps Ethernet interface is widely used in industries but general purpose processors along with software running on them through conventional approach are incapable of process such speed data. Hence there is need to exploit full potential of existing cost effective multi-core functionality of general purpose processors. In one of the research observation it is found that, performance of Linux kernel’s networking stack doesn’t scale with respect to increase in number of cores because of following reasons:

(a) Linux kernel handles incoming network packets with interrupt driven methodology which adds unnecessary packet processing overheads.

(b) Prior versions of Linux kernel networks stacks are not multi queue aware.

(c) Inefficient usages of memory for packet intensive processing applications.

(d) Per packet processing performance degradation on smaller packet size networking data.

Linux network stack is good for general purpose networking solution, but not for applications that require high-speed packet processing such as packet analysis and anomaly detection systems on high speed network interfaces.

### 2.1 Data Storage Challenges

Although storing data has become cheaper over a last decade there is always challenge for indexing such huge data and efficiently access it in a real time. A normal 100 Mbps line for a month can generate a packet log of 3TB. It may contain approximately 500,000 attacks[1]. Making sense of this volume of information is incredibly difficult with current tooling. Most of forensics tools have difficulty with this size of data. However it’s not only just size and scale but also today there are no good technological solution available to provide comprehensive view of network data in terms of threats, sessions, protocols and files.

### 2.2 Visualizing and Querying Data for Intelligence Gathering

The flow of data traffic among systems on the network, the exchange of information and services between countries, are examples of causally connected measurable events in a network [2]. Understanding the behavior of such networks often requires the ability to discover temporal connections among the events in a large data set. The problem is that relevant events are hard to identify automatically, so the investigator must organize events into a narrative sequence by hand. The investigation process often requires backtracking and multiple comparisons, which is not well supported by current forensics tools. There is need of new interactive visualization techniques for analyzing, organizing, and presenting network event data at multiple levels of detail for the purpose of forensic analysis - tracking down causal sequences of importance.

### 2.3 Behavior and Pattern Anomaly Detection Bottlenecks

The collection of raw packet data is useless unless it has used for generating security inference and detecting unwanted malicious traffic behavior. Performance of the tools used for analyzing anomalous behavior and matching on such real time huge traffic also limited with their single core oriented design.
3. DESIGN OBJECTIVES

3.1

By keeping technological challenges discussed in previous section in mind, following design objectives can be decided for high performance network forensics and intrusion detection systems.

(a) To fully exploit multi core functionality of commodity hardware for high speed packet processing.

(b) To design and develop cost effective packet capture and deep packet inspection engine on commodity hardware.

(c) To design and implement methodology and APIs for huge data storing, querying and real time processing.

(d) To design and implement intuitive network data visualization technique for huge data.

(e) To flag or alert anomalous traffic behavior based on data mining and ‘never seen before’ traffic.

(f) To design and develop service oriented architecture for network security solution.

(g) To identify application protocols, traffic pattern and metadata.

4. ARCHITECTURE & METHODOLOGY FOR HIGH PERFORMANCE NETWORK FORENSICS USING DEEP PACKET INSPECTION

Figure 1 shows network level operational deployment diagram of solution for high performance anomaly detection and deep packet inspection. One of its interface is connected to network tap which captures every in and out high capacity packet traffic. Figure 2 describes architecture of performance anomaly detection and deep packet inspection server. This has following sub-components.

4.1 High Performance IDS and DPI Engine

This block performs highly scalable multi core architecture for packet processing. Each core performs following sub-functionalities.

(a) **Packet capture:** This is user space packet capture module using Intel’s DPDK library[4]. To overcome limitations of traditional slow path packet processing, Intel developed open source framework named Data Plane Development Kit (DPDK). This framework creates set of libraries for specific hardware/software environment through the creation of environment abstraction layer (EAL).

(b) **Packet Analysis:** This block performs packet decode, protocol identification and anomaly detection.

(c) **Logging:** This performs full indexed network payload data, session metadata and alert logging.
4.2 Data Processing APIs and Rendering Engine

In order to scale and reuse its core functionality data processing APIs facilitate service oriented architecture which can be used by other security control systems. This is based on open source Packetpig APIs which does deep packet inspection, file extraction, feature extraction, operating system detection, and other deep network analysis. Packetpig’s analysis of full packet captures focuses on providing as much context as possible to the analyst.

4.3 Packet Logging in Big Data Storage

Apache Hadoop[3] is optimized around cheap storage and data locality putting spindles next to processor cores. To analyze full packet captures, Apache Pig – a dataflow scripting interface on top of Hadoop can be added. The length of retention of data can be based on the amount of data flowing through the network each day and the window of time one want to be able to peer into the past.
5. CONCLUSION

5.1

Traditional network defenses such as UTM/SIEM have limited visibility over ongoing network activity. In order to improve efficiency of security administrator to identify successful attack and successively speeding up of response time depends on the use of forensics tools effectively. Current network packet forensic tools on commodity hardware have limitation to scale for higher throughput due to inherent architecture of traditional Linux network stack. Utilization of multi-core features provided in modern CPUs is must for processing packets at higher throughput. In this paper, we studied the importance of deep packet inspection technology to counter advanced network threats, enlisted technological challenges to implement high performance packet processing network forensic tools on commodity hardware and successively proposed a multi-core, scalable high performance software architecture for network forensics to overcome those technological challenges.

REFERENCES

1. Supporting the Visualization and Forensic Analysis of Network Events, Doantam Phan, Ph.D. Dissertation, Stanford University, December 2007
3. hadoop.apache.org/
4. https://dpdk.org/
HR Strategies in Support of Joint ICT Structures

Brig Ramesh Balan

“Military institutions do not transform, people do; and in so doing, they transform the institution”

—Stephen Peter Rosen
(Winning the Next War: Innovation and the Modern Military)

Abstract—Joint officer management and training will evolve in accordance with the kind of jointness that we choose to adopt. Whichever way we go, this would undoubtedly be a key result area to prepare for future wars. Early adoption of relevant measures will only enhance joint warfighting capabilities, and grow an increasing number of officers well rounded in joint matters. HR strategies for Joint ICT Structures will constitute a critical area worthy of our collective attention.

1. INTRODUCTION

1.1
The character of war and warfare is continually changing. Paradoxically, “what got us here, won’t take us there”. So serious introspection is due. For some time now, we have all accepted that jointness is the inclusive mantra for emerging conventional kinetic battlefield scenarios of the future. Perhaps even in the non-contact warfare domain. But what is “jointness”? In this analysis the term is used to mean the effective integration of the combat capabilities of the Services. To that effect, most advanced militaries have become more joint over the last few decades.

1.2
Therefore, the entire war-fighting machinery, cutting across Service and cultural barriers, will need to rapidly gear up, to operate in mutual synchronisation. While man and machine both will be important, the man behind the machine will clearly be vital. Irrefutably, human capital will need to be invested into, managed, trained, educated, empowered and harvested. By corollary, this implies that the three Services will need consciously decide how they wish to transform.

1.3
But this will require us to rise above conventional mindsets and our service-specific scripting, to re-frame the questions we ask, with a spirit of honest inquiry and the resolve to implement. We will need to confront change and embrace it.

2. DEALING WITH HR

2.1
Dealing with HR has always been a big task. Typically, the scope of HR in the Armed Forces extends to military personnel of all ranks as also defence civilians. However, to limit the scope of the current discussion, this Analysis will restrict itself only to officers, that too in a joint ICT context. That said, preparing officers for joint service – in the right numbers and with the right kind of expertise and experience – will
require us to define and implement a strategic approach for joint officer management. Such an approach would identify needs for education and experience in joint matters and establish personnel policies and practices to ensure that officers with the required knowledge, skills, and experience are available to meet those needs. It would, in other words, focus on aligning the need with the supply.

2.2

Hesitant steps towards jointness and reform of higher defence structures have manifested merely as sporadic responses to external stimuli, rather than panning out as a well thought through plan. Our inheritance in jointness is a legacy of ad hoc and archaic structures such as the JOC, JAAOC and such like; essentially joint bodies and structures which are hastily put together in the face of a crisis / emergency and dissipate thereafter. No institutional memory. No persistence. In fact as on date, other than HQ IDS, HQ ANC, certain training establishments, DSCC, DCN and SI units, barely any joint structures exist.

2.3

Since structures have not emerged, staffing of joint establishments has not evolved beyond “a collection of borrowed military manpower” posted to apportioned billets determined by bureaucratic selection and assignment procedures. These officers serve their tenures worth roughly 2.5 to 3 -years as ‘purple-men’, before they revert for advancement within their own Services. Is that good enough to win us the next war?

2.4

A difficult choice therefore stares us in the face. Should we take the bull by the horns and adopt a top-down, integrated approach to ushering in jointness, culminating in the creation of Integrated Theatre Commands? In the case of the U.S., such drastic reforms were encompassed in the Goldwater-Nichols Department of Defense Reorganization Act of 1986. But are we actually ready that? And is it the only viable way?

2.5

Every country has to pick its own pace and approach. In matters of jointness, respecting and accommodating cultural sensibilities is perhaps just as important as knowing and pursuing what is right. Presumably, our senior hierarchy is already seized of this. But the inevitable reform that will need to follow, will require the patronage of wise leadership, resolute will and collective involvement. It will have to cut across the three Services and touch Doctrine, Organisation, Training, Equipment and Personnel aspects.

3. JOINT OFFICER MANAGEMENT

3.1

Bluntly put, the crux of the problem wrt joint officer management in India is that we have grown with single service scripting. To the bulk of us jointness is a superimposed construct, not an ingrained belief. No doubt there is a slow process of acculturation which is unconsciously in progress, when an officer serves in a joint establishment. As far as the Services are concerned there is an increasing acceptance of joint establishments – particularly in matters related to budget and procurement, and Doctrine, Organisation and Training. Joint Intelligence is faring reasonably well for two reasons, viz one - it draws upon a potent and performing SI (with an established organizational culture) or certain others (constituted of the very best in terms of talent and exposure); and two - it received a boost after Operation Vijay and enjoys a position...
of pre-eminence. Joint Operations and Force Development however remain the Holy Grail. Well that may not be bad, in the life of a 72 year young nation; clearly a lot more needs to be accomplished.

3.2

From the perspective of the MS / Personnel Branches of respective Service, joint billets are filled against QR, which indicate minimum acceptable eligibility criteria. Nonetheless, a considered opinion would be that joint billets are still not at the totem position. Part of the reason for that is that we do not have HR policies that are truly joint / integrated, rather they are an amalgamation of extant single service policies as applicable to respective personnel contributed by that Service. But can HR policies really be joint / integrated, when each Service recruits, commissions and trains HR/ talent principally to meet its own known commitments? In fact given the numbers being commissioned annually for a variety of socio-economic reasons, we are merely apportioning what is available rather than exceeding commissioning targets. Overall, this probably is a natural outcome of the way we are organized / structured, and in effect the way we think and operate. Unless this root issue is addressed, tangible dividends may not yield.

3.3

But it is difficult to change that unless a comprehensive analysis of the joint HR context is undertaken; where numbers are matched - criteria to billet – against a typical single service career progression path. A mere qualitative examination and the resultant recommendation will just not suffice. As an illustration, let’s consider that a policy decision is taken making a ‘minimum one tenure joint exposure’ mandatory for promotions to two star rank. Now this will call for the entire career progression path of a promotable one star officer, to be so structured that that a joint exposure can be earned at the right stages. But, a numbers check will show that we just do not have the required number of joint billets to achieve that. So the emergent alternatives would be to either make such an eligibility criterion desirable rather than essential, or to accept some notional joint-billet equivalence, or accord discretionary waivers where due so that individual officers do not suffer. Each such alternative measure would dilute the primary purpose of laying down such an eligibility criterion to begin with. It could also happen that it just is not in scheme of things for an IAF flyer to serve in a joint billet to be eligible to become a two star; or for a naval officer to choose a joint billet vis a vis wet listing and sea-time. Why should he? And why should the IN or IAF espouse such a career progression path at the cost of its own Service priorities? While it may be possible for the IA to provide joint service exposure to say a deserving ASC officer in a joint billet – stemming from reasons of say cadre management in Colonels rank, cultural sensibilities and prior exposure may make him completely unsuitable to run writ over General Cadre officers serving in IA-specific billets. In a nutshell, we have a bundle of contradictions staring us! Notwithstanding, it may well be worth our while to frame Joint Officer Management provisions.

3.4

The intent of the joint officer management provisions would be to enhance the quality, stability, and experience of officers in joint assignments, which in turn would improve the performance and effectiveness of joint operations. Some issues relevant in our context can be flagged as follows:-
(a) **Fluctuating Pattern of Wastage:**
Intake pattern and speed of promotions in respective single Service will need to be mutually harmonized. Now this is a tall order, for reasons of individual vagaries when taken batch-wise and Service-wise. Even if a common datum line is assumed to begin with, all cadets will clearly not have the same date of birth and consequently the same date of retirement for a given period of service. No Service can forecast precisely how many will get commissioned each year, and how many will get wasted out on account of premature retirements or for being below acceptable medical category and so on. So it will be clearly be difficult to preserve a harmonized intake and promotion pattern in the face of fluctuating wastages. As a consequence, officers across the Services, may not come up for promotion at the same time.

(b) **Joint Service Specialisation?**
Tenure-lengths, rotation philosophy, a normalized career progression path and relative importance of joint service billets *vis a vis* individual service billets will also need to be addressed and standardized. Apart from the mechanics of fulfilling such a challenging ask, it poses a fundamental question – will we be commissioned as joint Service officers, who will specialize in one of the three single Services or rather will we continue to be commissioned as single Service Officers (from one of IA, IN and IAF), some of who will do a joint Service specialization? Another relevant question in this context is whether we would have our respective arm/service/branch as areas of parallel specialisation (*vis a vis* joint) or whether these would be nested as a super-specialisation under and beyond jointness? While some areas of specialization already cut across Service boundaries (e.g. SI and Medical services), certain others potentially can cut across Service lines with minimal tinkering e.g. IT & Communication, Cyber, Space, Aviation, UAVs, Imagery, Strategic Missiles and so on. Concurrently, whereas certain common comparable domains can be adapted with effort e.g. Administration, Logistics, AD and Gunnery, some core areas across the Services, cannot easily meld e.g. infantry or armoured, fighter/transport aircraft flying, and sailing ships and submarines, being distinct in their characteristics.

(c) **Criteria Appointments:** While all the three Services largely conform to a model of unit interspersed with staff duty, the quantum of time spent in each kind of billet and the service bracket in which these billets are tenable may differ. The model of Adequate Exercise / Criteria Appointment (deemed as critical to be considered by the Selection Boards) adopted by each Service may differ. In the IA and IN, command of a body of troops or a ship/unit is deemed *sine qua non*, it may pale in significance to individual demonstrated competence in flying, for say the IAF. Perhaps, the Services will need to understand and accept different modes of evaluation for equivalent ranks, based on job-specific requirements.

(d) **Miscellaneous Issues:** Certain miscellaneous aspects which will need harmonization include skill and talent retention measures, identification of AE criteria, premature release, re-employment, promotion and other selection boards, and handling of non-empanelled officers, deputations,
designation of assignments as Extended/ High Tech, High Tech (Specialised) or Sensitive as per commonly evolved yardsticks, ACRs, complaints and representations, (including an acceptable internal oversight mechanism), legal aspects, applicability of a Jt Service Act vis a vis say the Army Act, Inter-Arm-Branch-and-Service-Transfers, uniform norms for commissioning (across different entry types and genders), postings (regular; compassionate ground, last leg and spouse coordinated), inter-service-cross-attachments (in staff and regimental billets), and employment (staff, regimental, extra-regimental, instructional and foreign assignments), punishments, discipline, vigilance, honours, awards and welfare matters, cadre management issues for principal and support cadre etc. While a mere mention has been made of these issues, there is no gainsaying that these HR matters will require considerable deliberation and discussion for viable common tri-Service norms to emerge.

3.5

Signallers across the Three Services: Let's go further and assume for the moment that the Gordian knot has been cut, that Joint Officer Provisions have successfully been framed. Two thoughts are relevant in this context. The Joint Officer Provisions per se could be based on a lead Service model, e.g. that of the IA and modified thereafter based on context-specific best practices followed by the other two Services. Alternatively, they could be framed de novo – a herculean effort by any account. The second concern relates to identification of job-specific QR based on the felt need in the emerging joint environment. Let us carry forward the latter issue. Assume that a Joint ICT Cadre is raised, subsuming within itself personnel from the Corps of Signals, Naval Signallers and some numbers of Electrical Officers and a subset of the AE (L) from the IAF. Just for the record it is important to observe that the IAF has two types of Aeronautical Engineers, some of who are commissioned into the cadre of Electrical Engineers. This cadre handles IAF Signals (less radio) apart from Radars, Airframe electrical and electronics as also oversees repairs in the affected area. Presumably they also handle IT support. Handling the radio set is tackled by pilots and ATC officers, whereas the AE (L) look into its repairs. So who is the specialist Signaller from the IAF with whom the IA can readily relate and find equivalence? The Naval Signaller is from the Executive Cadre akin to IA's General Cadre. He does not handle IT support which falls into the lap of the Electrical Engineer, along with repairs to all electrical and electronics on board a ship. The IA's Signaller is a distinct breed in this context. Someone from a supporting, rather an enabling arm, a hybrid who has chosen to evolve himself with combat proficiency - operationally, procedurally and technologically; someone who embraces telecom and IT with equal elan. In sum, each of the three Services throws up its own flavor of ICT-specialized HR ... for reasons unique to each of the Services. While, it would not be a cake-walk to cull out viable QRs for joint ICT billets, however, jointness in this cadre will still be achievable by careful selection and training / professional military education and suitable acculturation.

3.6

The Joint Signaller: One may say OK, but why put in such effort? The rationale is simple. Communications and IT constitute the nervous system of an organisation. Can one imagine a Joint establishment without the ability to transmit orders / receive feedback to/from its single service components, or upwards to its
superiors or laterally to its peers? The essence of C4I2SR and NCW lies in this communication and IT. Of course it will need to go beyond the physical domain and extend into the informational, cognitive and social domains as well. With the appointment of CDS having finally been announced, it is only logical for this dimension to be explored and given a concrete shape. Should we then have Joint Service Signal Units and HQ? Can we continue to function in an ad hoc manner based on loose collaboration? Where is the organizational flexibility and resilience with the IA, IN and IAF to tackle these kind of requirements. Can we look at a lead service model? As the largest Service IA may be expected to play a lead role in this regard. That may be good to start with but sustainability and growth will require something beyond that. It also does not require Einstein-ian brilliance to figure out that joint training and acculturation will be critical to make such an overall arrangement work effectively, be reliable and responsive to meet war-like scenarios.

4. JOINT PROFESSIONAL MILITARY EDUCATION (PME) AND TRAINING

4.1 Skilled officers, like all other professional men, are products of continuous and laborious study, training, and experience. There is no shortcut to the peculiar type of knowledge and ability they must possess. Trained officers constitute the most vitally essential element in modern war, and the only one that under no circumstance can be improvised or extemporized. In the Service community, we identify two key components of PME: train for certainty and educate for uncertainty. Both are required, albeit in the right proportions at calibrated intervals, spread across the career span of an officer, as they fulfil complementary roles. While Training drills a candidate in tackling specified, repetitive tasks, Education prepares him to think through issues that may not lend themselves to typical solutions.

4.2 While individual Services run a number of training courses for their own officers, iconic institutions like the NDA, DSSC, IAT, CDM and NDC run certain well established joint courses – which make a huge value-addition in a number of ways, not the least of which is joint acculturation. Premier institutions such as the three War Colleges organize cross-Service visits and run the renowned Joint Capsule and Core programmes.

4.3 In the joint ICT context, courses on Joint Electronic Warfare (JEW) and Frequency Spectrum Management (FSM) have traditionally been run, by rotation by each of the three Services. There are a number of ways, however, in which we could do better. The JEW course for instance needs to go beyond sharing and understanding how each of the three Services wages EW (communication and non-communication) in their own Service-specific contexts. The key issue is to ideate how we may fight joint in the EW domain, by working towards a common objective. Switching tracks, the FSM course spends considerable time on nuances related to peace-time spectrum management. Wouldn't it be better to address the spectrum requirement of a typical joint operation for communication and non-communication needs so that at least that one aspect is stitched up? This will include progressive improvement of syllabi to address practical concerns, nomination of a single venue, so that ownership is taken by at least one institution; and institutional memory is accreted, streamlining
the nomination of Directing Staff from all three Services, compilation of training material, implementation of distance learning packages, instituting measures for on-line access to pre-course and course material which would be equally accessible to officers from across the three Services, development of joint ICT training infrastructure, enhanced availability of ‘in-service’ ICT equipment, adherence to common joint procedures, and so on.

5. RECOMMENDATIONS

5.1

Apropos above, the following steps are recommended:

(a) Arrive at an early decision wrt the shape of future joint structures, viz, status quo, lead Service / Command or integrated theatre Commands.

(b) Contingent on the preceding decision, develop and adopt a strategic approach to HR aspects in support of Joint (ICT) Structures.

(c) Evolve joint officer management provisions. Test-bed them in the context of the HR work-force for Joint ICT structures.

(d) Give a fillip to professional military education and training in Joint ICT context.

6. CONCLUSION

6.1

All indications are that future wars, whether in the conventional kinetic or the non-contact domains will be fought joint. With the HR aspects remaining just as important as ever, considerable attention will need to be paid to management of personnel in the joint context. In order to fight together there is a need to train jointly, the objective being to prepare officers/men for present and future conflicts. This would lead to a common understanding of doctrines, concepts, each other’s Service competencies, capabilities, strengths and limitations and evolution of new joint ones.

REFERENCES

4. ib id.
Utilizing Decentralized Technology for HRM Advancement

Avnish Singh Jat¹, Rajkumar Pandey² and Akshay Singh³

¹IT Consultant,
Kriptech Systems Engineering Pvt. Ltd.

²Managing Director,
Kriptech Systems Engineering Pvt. Ltd.

³Project Manager.
Kriptech Systems Engineering Pvt. Ltd.

E-mail: ¹avnishsinghjat@gmail.com, ²rajkumar.pandey@kripalub.com
³akshay.singh@kripalub.com

Abstract—This paper aims to uncover the conceivable outcomes of utilizing the blockchain innovation in the field of HRM, featuring its advantages and potential issues for the HRM business procedures. A literature review has been led to distinguish the present status of utilization of Information Technology in the area of Human Resource Management and how Blockchain can help accomplish a shrewd, savvy, effective, straightforward and secure industrial facility administration framework. The fundamental ideas and components of the blockchain innovation, for example, hashing, DLT, and smart contracts, are talked about. Revealing a few issues in the HRM business forms, the paper looks at blockchain-based arrangements. Future research headings have additionally been recognized and upheld.

1. INTRODUCTION

1.1

Business improvement procedures and plans must be firmly connected and start with HR. The changed spotlight puts new requests on both HR experts and the product they use. New innovative arrangements are being looked for the more productive execution of business forms in the field of HR the executives. The progress to the utilization of business process the executive’s frameworks, cloud advancements and portable applications, BI advances and artificial intelligence is common.

1.2

Simultaneously, as of late there has been a developing spotlight on blockchain innovation. Up to this point, it has been basically connected with cryptographic forms of money, and today it is would have liked to improve exercises in different parts, including monetary administrations, human services, coordination and government sectors. Perceiving the advantages of blockchain, the EU is attempting to build up the innovation: in February 2018, the purported Blockchain Observatory and Forum, with Maria Gabriel, Commissioner for the Digital Economy and Digital Society, characterizing it as a key distinct advantage that can change numerous parts and carry numerous advantages to Union residents (Europa.eu, 2018). In his discourse to the scholastic network, Chinese President Xi Jinping additionally gave uncommon consideration to blockchain, saying that innovation is critical to the intensity of the Chinese economy (Coindesk.com, 2018). A basic overview of interaction with blockchain decentralized application can be seen in Fig. 1.
1.3 Blockchain is in the insight of US tech giants, including IBM and Microsoft, which effectively offer explicit arrangements and apparatuses for structure blockchain-based applications. In this specific circumstance, the reason for this article is likewise set out: to investigate the conceivable outcomes of utilizing blockchain innovation in business forms in the field of HR the executives, recognizing a few focal points and potential issues in its usage. To achieve this, it is first important to break down the business forms in the field of HR the board and blockchain instruments.

2. EXTENSION AND TASKS OF HUMAN RESOURCE MANAGEMENT

2.1 Human Resource centres around the individuals who work or will work in the association as its most significant resource and in its advancement incorporates parts of human capital administration, which spotlights on methodologies for dealing with the workforce, upgrading it and the business advantages of it (Bershin, 2015), and ability the board, which causes to notice pulling in, creating, spurring and holding appropriate representatives (Medved, 2015). There are various perspectives...
with respect to the number, name and substance of business forms in the field of HR the board. As indicated by the creator, as a beginning stage for their distinguishing proof can be utilized the general plan for grouping of business forms, based on which they can be partitioned into administrative, primary and supporting (Filippova and Filipov, 2009) (Fig. 1). Specifically, the board procedures may incorporate those for making systems and plans for human asset the executives, controlling exercises and creating different reports, planning authoritative structures and positions. The principle procedures are the “centre” of human asset the board. The advancement of the administration idea and the innovations for HR the board ponder straightforwardly the improvement of the primary procedures in this field and bring forth new ones. The primary procedures are aimed at the workers of the association and furnish them with some particular outcome or administration. Instances of significant business forms in HRM are: enlistment; naming a representative and placing him in the activity; in-organization preparing; ability improvement and the executives; advancement of pioneers; execution the executives; estimating the work done; worker accreditation; overseeing leave demands; retirement and that’s only the tip of the iceberg.

3. UTILIZATION OF BLOCKCHAIN FOR HUMAN RESOURCE MANAGEMENT

3.1
Blockchain is a data structure: it comprises of information hinders that structure a backlink. The structure and support of the blockchain chain depends on hashing, which is one of its key components. In cryptographic hash capacities, contributions of any length are changed over to yield strings of a similar length. Yield strings are called hash esteems or hashes. An essential prerequisite for cryptographic hash capacities is that the first information can’t be recouped from the hash - for example that it can’t be unscrambled. It is likewise not allowable to have distinctive information hash esteems. Cryptographic hash capacities can utilize various calculations. For instance, Bitcoin utilizes SHA-256 and Ethereum utilizes KACCAK-256 (SHA3-256). The two calculations speak to the produced hashes as 64-digit hexadecimal numbers. In FIG. 1 demonstrates the hash esteems of a few unique spellings for “HR” as indicated by SHA-256 and SHA3-256, separately. As the model shows, the produced qualities are a similar length - 64 characters, and each adjustment in info brings about an alternate hash esteem.

![Hash values according to SHA256](image)

<table>
<thead>
<tr>
<th>Hash values according to SHA256</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HUMAN RESOURCES</strong></td>
</tr>
<tr>
<td>Human Resources</td>
</tr>
<tr>
<td>378351d07011d622ed374e5004f27e5f</td>
</tr>
<tr>
<td>Human Resources</td>
</tr>
<tr>
<td>3e6ae9e2f46ed964779d0380a196a49</td>
</tr>
<tr>
<td>DPA76471cBFD2cD46F08c1D6C46e07A2</td>
</tr>
<tr>
<td>Cryptographic</td>
</tr>
<tr>
<td>EBDA4567C1843B572BF935305FA6A1264</td>
</tr>
<tr>
<td>97C491BF452AE73C80835B85519B719</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Hash values according to SHA3-256</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>HUMAN RESOURCES</strong></td>
</tr>
<tr>
<td>Human Resources</td>
</tr>
<tr>
<td>61c15db785d16351b78e4a96920b3d3</td>
</tr>
<tr>
<td>534eCFAE45A76B949CEBBB959c7A504D</td>
</tr>
<tr>
<td>Human Resources</td>
</tr>
<tr>
<td>70EB4470CC543CFDF01B0843647E94B8C1</td>
</tr>
<tr>
<td>EEF8BBFE74AFF070D47B307D43339</td>
</tr>
<tr>
<td>Cryptographic</td>
</tr>
<tr>
<td>9436678C1E80C7ABDBDE10B6516D5400</td>
</tr>
<tr>
<td>F64B6490DD324C10DA0C7113F4E760</td>
</tr>
</tbody>
</table>

**Fig. 2: (generated by emn178.github)**

3.2
One of the significant difficulties for HR experts is finding the correct experts who, with their insight, capabilities and abilities, can fit well into the organization and add to its prosperity. As indicated by an investigation via CareerBuilder (2016), a HR counselling firm directed in Chicago and Atlanta in 2016,
75% of businesses concede they have enlisted wrong representatives in the most recent year, i.e. they had an “awful contract”. Also, the normal expense of enlisting an ineligible worker is $17,000, going between $ 11,000 for independent companies and $ 24,000 for enormous organizations. The impact of poor procuring is communicated in: lower efficiency and lower nature of work performed by the worker concerned; exercise in futility looking and preparing another representative; extra time for different workers, client protests; falling apart work environment atmosphere and the sky is the limit from there. Comparative information for 2017 (again for the USA) is being sent out by another counseling firm - Robert Half. As indicated by their study, 81% of businesses confess to enlisting blunders, and it takes a normal of 17 weeks to address such a mix-up (Half, 2017). Another major issue is that the length of enrolment and enlistment procedures has expanded altogether as of late. While by 2010 its normal term is 13 days (www.fastcompany.com, 2015), by 2017 it is 23.7 days (Chamberlain, 2017).

3.3
As indicated by a review by DHI Group, which keeps up particular quest for new employment locales, it sets aside the most effort to contract profoundly qualified authorities, for example, building staff (62 days), business and frameworks experts (57 days), IT masters (56 days), IT pros promoting and publicizing (54 days) (Bika, nd).

3.4
Various experts (Crichton, 2018; Thygesen, 2017) refer to the absence of trust between bosses, from one perspective, and occupation candidates and representatives, on the other, which prompts wrong administration choices and defilement (incorporating into the choice and enlistment of reasonable workers) ruins correspondence in the working environment, demotivates representatives and makes them increasingly capable. For instance, endorsements, certificates and suggestions given by candidates assume a significant job in the determination of representatives. Checking them takes quite a while. It is no special case when occupation candidates give off base data about their capabilities and pragmatic experience. As per an examination via CareerBuilder (2014), directed in the US (Chicago), about 60% of managers lie in candidates’ CVs - as far as positions held, exercises performed, duties and results accomplished, scholarly degree, college participation, praises got and so on. Counterfeit confirmations and endorsements are frequently displayed. As per the overview, such misrepresentation is especially normal in areas, for example, social insurance (63%) and budgetary administrations (73%), where procuring untalented staff can have genuine outcomes.

3.5
The approval of the information given by occupation candidates is confused by the expanded versatility and globalization of the workforce, just as by the expanding decent variety of preparing and capability structures. U.S. Research The Bureau of Labor Statistics (2016) points out that recent college grads matured 25-34 years remain in one occupation at a normal of 2.8 years, which is almost multiple times not as much as individuals matured 55-64. Comparative wonders are seen in our nation.

3.6
This reasonable propensity to change employments all the more frequently (thus to talk, at the spot and nation of living arrangement) requires rehashed keeps an
eye on the application reports, for example, the dangers of distortion and extortion are likewise expanding. To beat such issues, one needs to think unusually, including to search for arrangements in some rising data advancements, for example, blockchain and DLT. They achieve various advantages to business procedures and information (Hooper, 2018; Voshmgir and Kalinov, 2017; Filipova, 2018), which are communicated in:

(a) Trust that is kept up by all partners, ie. it is decentralized. It’s about the alleged. “Trustless trust”: without confiding in any of the members in the blockchain, the client can believe the aftereffect of the information preparing.

(b) Transparency and follow-up coming about because of the constancy of data, the maintenance of various duplicates and the requirement for agreement.

(c) Higher security coming about because of information hashing and connects between squares in the chain, just as from the requirement for agreement in including information and evolving applications (counting shrewd agreements).

(d) Reliability that is expected to DLT and keeping up indistinguishable duplicates of the chain over all hubs.

(e) Higher effectiveness and lower cost. The requirement for middle people (because of which business procedures are quickened) is decreased, just as the work expenses of filing and securing data.

**Fig. 3: Blockchain Network Architecture**
3.7
These focal points make it conceivable to defeat the previously mentioned issues in the centre business procedures of HR the executives. To address them, various new companies are endeavouring to actualize blockchain-based frameworks to check data for occupation candidates - incl. recognitions, authentications, proficient experience and different subtleties. For instance, the APPII stage (www.appilio, n.d.) empowers work searchers to assemble a supposed. A “shrewd profile” that portrays subtleties of their preparation and expert accomplishments. After check by past bosses and preparing establishments that are enrolled as accomplices in the framework, the information is recorded in blockchain, making it difficult to misrepresent it. Buyer recognizable proof is accommodated more noteworthy security: they are caught utilizing a versatile application, and this picture is contrasted with a photograph from an official archive, (for example, an ID card or international ID). For their commitment to the improvement of the stage, clients get tokens that they can use for courses and preparing, for instance. Simultaneously, a few colleges, for example, the Massachusetts Institute of Technology - MIT, are creating ventures to hold understudies’ confirmations in blockchain.

3.8
Through the Blockcerts Wallet versatile application, understudies get a checked and fake duplicate of their certificate that they can impart to businesses and different partners (Durant and Trachy, 2017).

3.9
There are as of now various ventures for blockchain-based quest for new employment frameworks. A case of a fascinating plan of action is the Aworker venture - an Ethereum blockchain-based quest for new employment stage and the utilization of shrewd agreements (Cherkasov, 2018). Its makers intend to build up a worldwide stage for assessing work searchers’ expert abilities. For every up-and-comer, a “notoriety” is framed, which develops as they check and add new aptitudes to their profile. The framework positions applicants by their notoriety, and the individuals who are among the best in the field get additional focuses. Organizations, thus, approach solid data about occupation candidates. What’s more, some routine enlisting exercises are mechanized through savvy contracts. Stage administrations are paid with work tokens: the more clients the framework has, the higher their worth.

3.10
A comparative undertaking is likewise being worked on in Bulgaria: the makers of the Ethereum blockchain-based Open Source stage have the aspiration to create “straightforward” connects between the scholarly community, understudies and organizations oversaw through shrewd agreements (www.os.university, 2018). It is visualized to utilize advanced portfolios in which clients can store archives, for example, recognitions, authentications, and so on that have been confirmed and approved through the instruments of blockchain innovation. Through coordinating calculations, jobseekers can rapidly locate a reasonable situation for their capabilities and bosses can discover appropriate competitors. The stage administrations are utilized against EDU tokens. Along these lines, such choices, in view of open or private blockchain, can essentially abbreviate the enrolment procedure, while additionally taking care of the issues of trust and discovering reasonable applicants. It is simpler to check the character of the candidates, their capabilities and expert experience.
3.11

Indeed, even the broadly utilized proposals or the consistent update of the CV with respect to the most recent patterns in a territory, for example, data innovation, are never again required. The candidate’s confirmed blockchain capabilities, aptitudes, experience and accomplishments are more important to bosses than both the best CV and the best proposals. Simultaneously, the odds of applicants with high expert aptitudes and a decent notoriety to get a new line of work reasonable for them are expanding. An assortment of data about workers can be put away in the blockchain even after they have been employed - incl. archives, for example, business contracts, endorsements, authentications and occupation change, sets of expectations, and so on. At times, savvy agreements can be utilized to oversee such records - for instance, after specific conditions have been met, (for example, a fixed term of work and fruitful accreditation), the representative is consequently elevated from junior to senior expert, changing his activity title and individually his compensation.

3.12

Along these lines, the level of mechanization of business procedures can be expanded in blockchain-based frameworks. Blockchain can likewise store some exchange information, for example, medicinal declarations and assessments, expenses paid, charges and commitments paid, excursions for work and occasions, and so forth. Checked data about the work performed can likewise be held - for instance, finished exchanges, phone assembles and conferences with customers, and so on., which takes into consideration a progressively exact bookkeeping of the individual commitment of representatives. This plan is particularly appropriate for organizations offering adaptable work plans -, for example, teleworking, low maintenance and venture work, or utilizing different outside partners. Keeping up representative data and important business procedures requires the connection between various jobs and offices - HR expert, worker, bookkeeper, administrator, social insurance expert, and the sky is the limit from there.

3.13

Coordination between them is bolstered by blockchain, accord systems and disseminated applications. Once put away and confirmed, the realness of the significant information is ensured, and the requirement for rehashed keeps an eye on their legitimacy is dispensed with and reference data is encouraged. Because of the constancy of the data, the danger of forging and messing with the information is decreased. For such purposes, because of the need to limit and control access to data, it is increasingly suitable to utilize a private blockchain.

3.14

As per various HR experts (Brown and Smit, 2017; Zielinski, 2017; The HR Observer, 2018), blockchain is additionally a suitable innovation when paying representatives’ pay rates - particularly in worldwide organizations, at work eth with specialists and universal instalments. Normally, worldwide instalments are slower, exchanges are progressively costly and are dependent upon various guidelines - for instance, in connection to illegal tax avoidance and the prerequisite to know the beneficiary (KYC). Blockchain encourages the exchange of assets, as a rule by picking one of the well-known cryptographic forms of money - Bitcoin, Ethereum. In doing as such, steady exchange data is held, which may encourage ensuing checks by administrative specialists. In addition to the fact that transactions are quicker, progressively solid and less expensive. One model is the Bitwage instalment framework (www.pymnts.com, 2016), which joins blockchain, portable and cloud innovations. Instalments are made in Bitcoin and the stage bolsters nearby cash change. The Australian
organization Chrono Bank additionally utilizes blockchain innovation to pay representatives taking a shot at transient agreements or low maintenance (Chronobank.io, 2018), which is normal for the supposed. gig economy - a model that is winding up more broadly utilized and favored by youngsters.

3.15
In spite of the fact that blockchain innovation offers different open doors for improving HR business forms, it ought to be borne as a top priority that its usage isn’t a simple assignment. In spite of its points of interest, it is another innovation and needs adequate experience and well-prepared masters to assemble and keep up such frameworks. There may even be obscure dangers of utilizing it. Fruitful undertakings here require cautious examination and reengineering of HR business forms, considering existing business and specialized dangers (Filipova, 2018, p.89). In doing as such, it is important to watch the current legitimate standards - incl. the acceptability of cryptographic money exchanges, the prerequisites of information security orders, for example, the European General Data Protection Regulation (GDPR), and so forth. It is likewise essential to appropriately decipher the ideas of "keen agreement" and "full trust" that frequently go with blockchain. As noticed, the keen agreement has no lawful power - it is programming, and it does what the software engineer put in it. Blockchain trust depends on the best possible working of cryptographic calculations and circulated applications. As such, blockchain lessens the impact of the human factor; yet for good or not, it can’t be totally kept away from.

4. CONCLUSION
4.1
The expanding obligations of HR experts and the significance of business forms for HR the organisation require sufficient digitalisation. It is no happenstance that as of late various driving IT sellers have concentrated on structure answers for atomate HR. For reasons unknown, this is one of the most open regions for IT concentrated of late. The enthusiasm of HR experts and innovation organizations in the utilization of blockchain innovation in HR procedures is as of now a reality. It would like to quicken business forms and lessen their worth, while expecting a superior business result that can have an assortment of appearances: incl. finding and employing the “right” experts and overseeing data and associations with them viably. Regardless of whether these desires are reasonable and whether blockchain will in a general sense change HR action will demonstrate what’s to come. Notwithstanding, it ought to be borne as a primary concern that ventures around there are in the beginning times of their advancement, and their further achievement depends, in any case, on whether and to what degree work candidates, representatives and businesses trust them.

REFERENCES