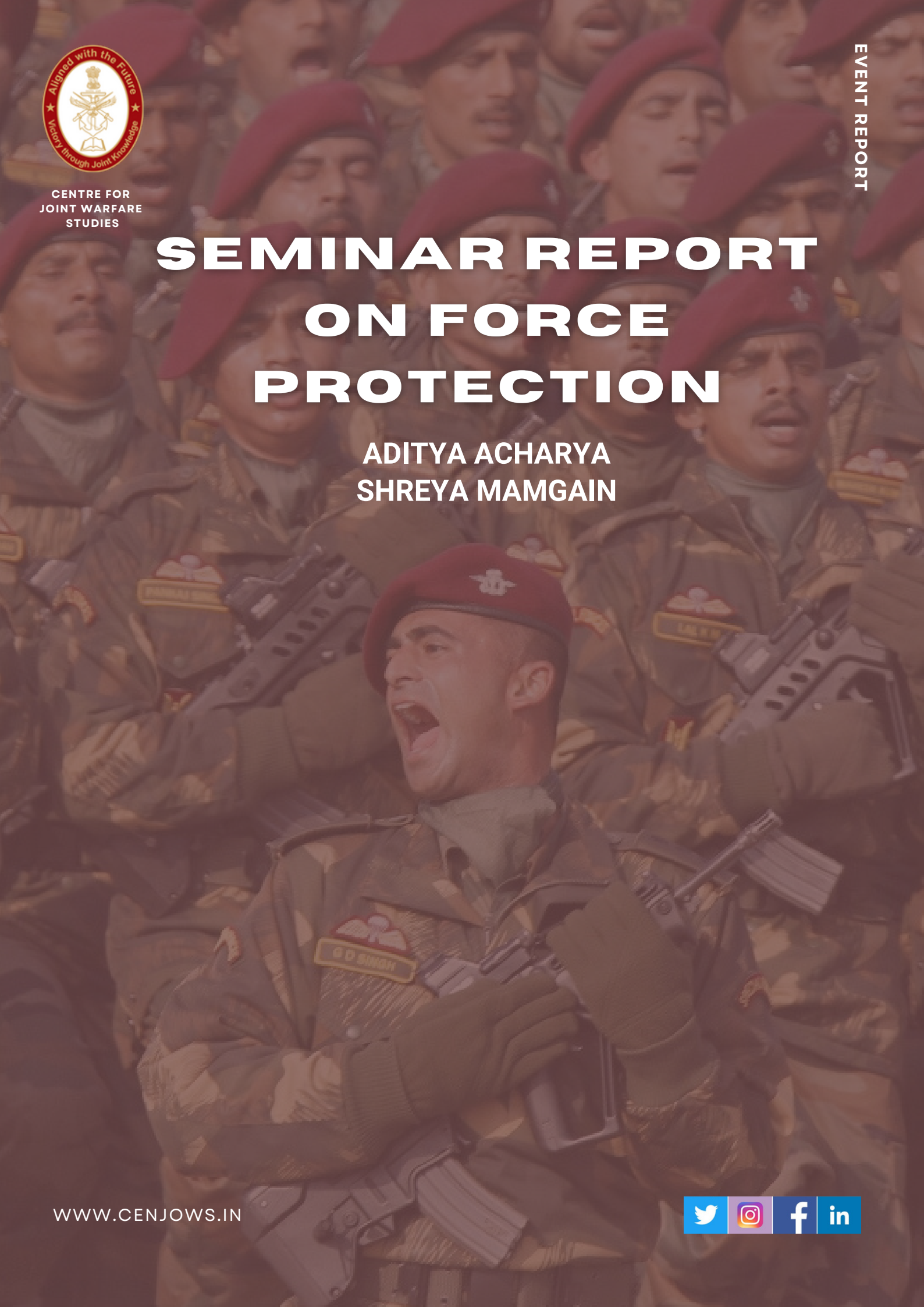

CENTRE FOR JOINT WARFARE STUDIES

EVENT REPORT

SEMINAR REPORT ON FORCE PROTECTION

ADITYA ACHARYA
SHREYA MAMGAIN

WWW.CENJOWS.IN

SEMINAR REPORT ON FORCE PROTECTION CONDUCTED JOINTLY BY CENJOWS AND IMR 09 MAY 2023 MANEKSHAW CENTRE, NEW DELHI

Complied by
Aditya Acharya, Research Intern
Shreya Mamgain, Research Intern
CENJOWS

SESSION 1 - INAUGRAL SESSION (0930 - 1030 HRS)

Welcome Address - Lt Gen Sunil Srivastava, Director, CENJOWS

Key Takeaways

- He outlined that *those who protect us, the armed forces, need to be protected* which has been a pertinent issue since the times of ancient thinkers like Chanakya due to threats emanating from various domains ranging from land, sea, air, and other emerging threats like cyber, space, and information warfare.
- *Managing the risk* - risk being brought down to acceptable levels through mitigation.
- *Ensuring force protection* while *guaranteeing freedom of action of forces* and looking after that these do not inhibit the maneuverability.
- Force protection is *not just about physical protection but policies, plans, training, organization, strategies*, etc.
- Force Protection is a *dynamic continuum of the cycle of threat prediction, detection, deterrence, and resilience*.
- In the changing threat landscape, there are *no fronts and no rear*. There is a large amount of open source information, OSINT, GEOINT, AI, and unmanned systems which enhance the threats, which are *not well-defined and hybrid.*
- *Our current focus is 'perimeter and manpower centric.' We need to integrate cutting-edge and emerging technology* in our goal of protecting the forces and its assets. This calls for close cooperation of all the stakeholders and leveraging commercial off-the-shelf technology by integrating the efforts of users (armed forces and CAPFs), the scientific community of DRDO, DPSUs, and the industry.

SEMINAR REPORT ON FORCE PROTECTION CONDUCTED JOINTLY BY CENJOWS AND IMR 09 MAY 2023 MANEKSHAW CENTRE, NEW DELHI

Inaugural Address - Shri G Satheesh Reddy, SA to RM

Key Takeaways

- Force protection is a very 'wide subject' and covers everything except the offensive part of the war. To understand the topic at hand better, he *limited his ideation of force protection to border surveillance, mines, intrusion, explosives, IEDs, protection perimeters, and personnel protection.*
- He then threw light on aspects of *intrusion detection, and tunnel detection used primarily for smuggling and infiltration*. He underlined the use of *heat imaging, radars, cameras of high resolution, etc*. He also spoke about the limitations of such technologies regarding depth, range, and quality (resolution) and how AI can be integrated into these systems.
- He then shifted the discussion to the issue of perimeter protection of the army and naval bases and airforce stations. He outlined the *need for standoff scanning of persons and explosives* and again here highlighted the challenges with range, chemical detection of explosives, suicide bombers, and mines (in naxal areas).

How to handle these challenges? (Shri Reddy, SA to RM)

- Develop sensors that have 360-degree scanning to check for weapons and explosives.
- For tunnels and mines - Ground Penetrating Radars with over 10 meters capability and miniaturization of radars mounted on robots with increased accuracy.
- Improve devices to capture hyperspectral images of high resolution and SAR images.
- He underlined the need for the use of drones, motion sensors, integration of AI, and ML for better friend-or-foe identification for an effective perimeter protection system.
- Elaborating on drones, he explained the challenges posed by swarm drones and the use of Anti-Drone Detection systems.

- In Personnel Protection Systems, he threw light on recent developments and upgrades in BPJs, Ballistic helmets, goggles, and high-altitude clothing systems and pressed on the need for rapid indigenization in these domains.

Towards the end of his remarks, he highlighted the need for increased debates, and discussions among the users (i.e., armed forces, CAPFs), R&D teams of DRDO, and its various labs and industry (for better commercialization) to come up with specific requirements and solutions for increased force protection and overall protection of sovereignty and territorial integrity of Bharat.

Lt Gen Arvind Walia - Engineer-in-Chief, Army HQ

Key Takeaways

- Force Protection is a very contemporary topic, warfare today is shaped by grey-zone tactics, and the prolonged Russia -Ukrainian conflict has proved force protection has become more important than ever.
- We need a whole-of-nation approach to multiply our efforts towards force protection, with Army, Navy, and Airforce as well as CAPF and civilian setups coming together and working towards the goal of force protection.
- He brought to light the efforts of the Engineers Corps in the ongoing Eastern Ladakh Crisis:
    1. Additional habitat for forces done in record time which are fast, modular, and relocatable.
    2. Construction of field trenches, operations rooms, underground storage for ammunition in record time, and digging borewells for freshwater supply.
    3. Construction of an Anti-Infiltration Obstacle System (AIOS) along LoC and integration of AI, ML, and facial recognition) for more accurate surveillance.
    4. Counter Mine and counter IEDs and counter CBRN ops.
    5. Camouflage Protection - Hide your vulnerability, you are inherently protected.

    6. 3-D printed bunkers for shelters for overhead protection.

But he flagged that these are not comprehensive and enough, given developments seen in the Russia-Ukraine war.

Col KV Kuber - Director of Defence and Aerospace, EY

Key Takeaways

- Col. KV Kuber presented the industry perspective. He started with an episode of Arjuna Vishad-yoga and explained that the Kurukshetra war was more about who possessed better quality and quantity of information and relative strength. So force protection is more about the information of inimical circumstances and enemies within and without.
- He posed some serious questions regarding force protection and related aspects:

  1. How many casualties will we face due to enemy suicide attacks or convoy attacks?

  2. How to handle psychological force protection? (Example - Honeytraps)

  3. Who will talk about the brunt being faced by forces due to failures of diplomacy?

  4. Should we have collectors or high-ranking officers in civilian offices from the armed forces in 'disturbed regions?

He then went on to explain the need to specifically earmark "force protection vertical" in the defense budget. He outlined the importance of 'information' in today's war times and the need for a 'whole-of-government' approach to approach the issue of force protection in a better manner.

SESSION 2 - PERIMETER PROTECTION AND INFILTRATION DETECTION (1100 - 1215 HRS)

Chairperson - Brig Gurpal Singh, Brig Infantry-B, Dte Gen of Infantry, Army HQ - Introduction of Speakers and Opening Remarks

Key Takeaways

- Each border has with its unique challenges and threats due to varied characteristics. So different borders require different border management protocols and force protection methods.
- Urbanization poses a challenge in perimeter protection as has been highlighted by recent attacks on IA bases. Most naval bases are surrounded by urban agglomerations, which poses a unique set of challenges to the protection of these assets.
- The use of emerging technology with support from R&D branches and industry is the need of the hour.

Shri Asif Jalal, - IG (IT), BSF HQ, - Challenges in Countering Infiltration Across Borders

Key Takeaways

- BSF guards very diverse borders ranging from jungles, creeks, and deserts as well as snow-clad mountains. Hence border sanitization and protection is a difficult task.
- Challenges are Extreme weather conditions (Rainfall, dense fogs, riverine gullies which often shift their course), Infiltration Smuggling of arms & ammunition as well as narcotics. Emerging threats are Drone/UAV activities and extensive tunneling activities for the purpose of smuggling.
- Counter-Measure Activities - Border Flood Lights, Night Boat Nakas, IR walls, management of gaps through QRTs, and coordination with local police, IA and IAF.
- The industry is making good efforts in providing updated technologies to BSF but it must focus on developing low-cost solutions as BSF faces a budget problem.
- Also, the industry must try to make systems more accurate as they at times raise false alarms due to which scarce resources are diverted.

  Demands from Industry - More efficient Anti-Tunnel Tech, Anti-fog HHTIS, SONARs, and Sarkanda clearance technology

Air Cmde S Kannan, VSM, Provost Marshall, Air HQ - "Protection of IAF Bases"

Key Takeaways

- Talked at length about the Integrated Perimeter Security System (IPSS) which was developed in the wake of Pathankot attacks, which is virtually impregnable in deterring, detecting, and locating the threats and providing early warnings.
- Advantages - Early warning, increased situational awareness, real-time monitoring, and quick decision-making. The open architecture of technology allows the integration of emerging updations like ML and gesture analysis.
- Demands from Industry - Need to make better radars (due to vegetation, it does not work properly), improvements in resolution of images captured by the IPSS, integration of Anti-drone technology in the IPSS-Phase 2, and solution to issue of false alarms.

Mr. Manoj Purohit - Instruments Research and Development Assistance

Key Takeaways

- Gave a detailed presentation on Border Surveillance System, and lessons learned in a journey from concept to induction.
- Characteristics of the system - 27x7 observation (all weather), unmanned installation, remote operations, captive power (hybrid power source with fuel cells) with advanced video analytics (image enhancement, motion detection, and tracking) with networkable dissemination of information and recording and retrieval of data.
- Challenges Remaining - Issues in operation in very low temperatures, security, deicing and de-fogging, and harnessing low-temperature operation and lack of image intelligence.

SESSION 3 - PERSONNEL PROTECTION TECHNOLOGIES (1220-1330 HRS)

Chairperson: Brig Ravi Yadav, Brig Tech Resource Center, Army Design Bureau, Army HQ - Introduction and Opening Remarks by Chairman

Key Takeaways

- The soldier must remain at the center of initiatives of force protection. Problems must be discussed at the personnel level and solutions must be executed at that level.
- Army Design Bureau has in-house innovations which have yielded the development of systems like Sarvatra, Kavach, and Shakti. D&D efforts led to the development of the iDEX project and ballistic helmets and goggles.
- The challenges that remain are - reducing the weight of NIJ4 level BPJs as well as helmets with improved modularity and integrity for higher absorption capacity and integration of sensors.
- What the future holds?

    1. Focus on the material - lightweight and modular

    2. Integration of nano-tech solutions
    3. Integration with advanced projectile detection system, combat gear, and sensors.

Col Praveen Raghuvanshi, Col INF-8 - Protecting the Soldier, Requirements, and Challenges

Key Takeaways

- Though modern wars will be more ‘information-centric’ in cyber, space, and information domains, then too, the soldier remains as important as ever.
- The equipment of focus should be Modular Integrated Load Carrying Eqpt (MILE), BPJs, Exo-Skeleton, Multi-Spectral Camouflage Suit, Anti-Mine Boots,

Ballistic Helmet and Goggles along with gloves and knee pads, and ballistic shields.

- The expectations from the industry are a reduced gestation period between innovation and commercial production, indigenization of raw materials, development of lighter equipment, and development of a mechanism of Ballistic Test Reports to verify claims of firms - NFSU & TBRL along with the development of feedback loop.

Shri Ajitendra Parihar, DMSRDE, DRDO

Key Takeaways

- No linear approach to the problem will provide the desired protection. In addition to the immediate body protection a need exists to remain mobile, agile and flexible for effective operation in the battlefield.
- The aspects considered for “Design & Development” of PPE include injury patterns from the type of threat envisaged, specifics of threat manifestations & agility/flexibility of the person and effective use of personal weapons.
- Mobility also to include operational endurance while wearing the PPE.
- R&D and testing for in-house innovations and indigenization of materials.

Various types of protection equipment made of ballistic resistant material like NIJ III & IV +BIS5/6, modular lightweight B4 Ballistic Helmets, Ballistic Goggles were discussed.

Dr N K Chaudhury,ScG,INMAS

Key Takeaways

- Ability to predict the type of CBRN threats and an assessment of hazards.
- Assessing the capability of the force to operate in CBRN environments - need for verifiable data and models.
-

- The fields of R&D in CBRN being undertaken by our adversaries and counter measures to be developed.
- Need to develop human resources-chemical scientists, virologists, microbiologists.
- Better ways of detection to be explored- drone and vehicle-based detectors, autonomous systems exploiting evolving sensor and communication technology.

SESSION 4: IEDs, FIRE AND CBRN (1430- 1545HRS)

The **Chairman Brig Amod Chadha** before inviting the panelists emphasized on the importance of remaining current on all aspects in "Asymmetric Domain" especially the employment of IEDs.

Key Takeaways

- IEDs have graduated from the traditional crude bombs operated by manual switch or a simple remote control to sophisticated use of 5-7 digit activation codes. The technology for pre-initiators and jammers need to keep pace with the changes in IED construction and employment.
- The CBRN threat is critical and has a unique nature which may be less likely to occur but it's consequences will be catastrophic.
- Additionally, the presence of tactical nuclear weapons in the South Asian neighborhood needs to be factored into the counter CBRN strategy.
- Fire can have devastating effects on the Command & Control nodes as also the Ammunition Depots/ Logistics Support System and therefore needs to be protected against.
- While preventive measures in place need to be strengthened, we must move on from old and obsolete fire-fighting mechanisms to modern sensor-based systems and exploit all available technologies.
-

- Both uniformed and civilian personnel need to be trained and equipped to counter the threats from IEDs, CBRN weapons and Fire which could be used as a weapon of sabotage.

Lt Col Ashish Tandon, SI EDD, CME

Lt. Col Tandon while expounding on the subject of "Concept of Application of Counter IED Strategy" brought out the point that the IEDs are a weapon of choice for terrorists, insurgents and criminals. In order to counter this threat, concerted and coordinated strategy involving all state organs like the military, paramilitary, police forces, NSG and disaster management machinery is a must.

Key Takeaways

- While countering the threat is largely limited to physical neutralization or the disposal of the IED, a comprehensive strategy calls for an understanding of the organisation behind the perpetrators of attack, motivation and funding of the terrorists / insurgents.
- The type of IED threat will also vary depending on the operational area. In the Indian IED scenario these templates relate to J&K, LWE affected areas, NE and other parts of India.
- The IED threat network thrives on availability of funds, radicalized elements for recruitment, availability and procurement of material, construction of the device and its triggering mechanism, identifying targets and deployment of device and finally showcasing the event on social media after triggering the blast.
- Counter IED operations and strategy are based on a proactive policy to mitigate the effects and protection through analysis and neutralisation of IED network.
- Post blast investigation of the site provides maximum threat intelligence, dissemination of information for protection of forces and civilian population, uniform training, exposing the network and use of latest technology.

- Uniform training must concentrate on developing tactics, procedures and SOPs before induction of forces in an operational area.
- Thorough forensic research/ investigation provides identification of material, it's likely source, history of similar construction, planting and planning methods, development of new techniques and technologies.
- Counter IED Strategy has three lines of operations- Attack the network, Defeat the device and Train the forces.

Col Salim Ajaz, Strategic Planning Directorate, Army HQ

Key Takeaways

- The perceived threat, the protection policy and the role of the industry to enhance the efficacy.
- The COVID-19 pandemic brought to light numerous global inadequacies.
- The weaponisation of virus can be easily done with plausible deniability and with very little or no attributability. Threats can manifest as pandemics in no time. The threat landscape has now expanded to the civilian populace, which must be protected as well.
- With proliferation of Bio Safety Lab worldwide, the likelihood of non-state actors accessing and employing bio-weapons has become a distinct possibility. The "microbes vs missiles" logic will embolden non-state actors.
- The Bio-Technological threshold of India's neighborhood is high, with involvement of 70 - 80 BSL Level 4 laboratories doing R&D.
- The use of chemical agents in the Second World War, the Iran-Iraq Conflict, the Balkans, Japan (the Tokyo Sarin Sub way attack) and as recently as 2022 allegedly in Russia-Ukraine war, provide evidence of chemical attacks.
- Chemical attacks have also been used in targeted assassinations.
- While the number of casualties has decreased but the level of toxicity has intensified.

- The Organization for Prohibition of Chemical Weapons (OPCW) under the provisions of CWC 1997 has claimed to have destroyed 99.3 % of verifiable stocks of chemical weapons, and aims to destroy the remaining by 2023.
- It is not possible to identify, inspect and neutralize every chemical production facility. A useful chemical/ medicine developed during the R&D can potentially be a precursor to numerous lethal by products.
- Easy availability of ingredients to manufacture Chemical Weapons with internet providing the knowledge on processes involved rules out the possibility of complete eradication of this threat.
- The threat posed by nuclear weapons remains relevant. This has become more so with the possibility of use having increased with the Ukraine conflict and North Korea testing nuclear enabled weapons unabated and India flanked by nuclear capable neighbors.
- Though no nuclear weapons tests have taken place since 1998, the current availability is adequate to keep nuclear threat alive. Besides external threat, internal elements are also capable to add to the threat especially when the leakage can be through the research labs involved in using radioactive reagents, indiscriminate disposal of radioactive waste etc.
- The current CBRN strategy in place is based on "Doctrine of No First Use" and "Maintenance of Credible Minimum Deterrence" with the operational philosophy consisting of 3 elements. These include-Prevent CBRN attack at all costs, in case of an attack withstand the same and finally remain battle worthy to operate through a contaminated environment and continue to fight.
- At the strategic level a deterrence-based policy is adopted but at the operational and tactical level the policy of Contamination Avoidance (Active/ Passive), Contamination Protection (Individual/ Collective) and Decontamination (Restoration of Combat Effectiveness & Reduction of Casualties) is in place.
- These new and emerging threats can only be dealt with concerted and coordinated efforts of all stakeholders.

- While the focus on Conventional and Counter Insurgency Operation will remain, the support from industry will need to cater to development of sensors and detection infrastructure, adequate protection facilities in terms of shelters and sanitizing equipment for decontamination and individual protection.
- The pharma industry will need to gear up to provide backup to counter ill effects of the CRBN attacks. Hence the indigenisation of relevant R&D and end products to counter the CBRN would be the expected aim of the national industrial base.

Col Harsimran Singh Gill, Col OS 20, Directorate General of Ordnance Services

Key Takeaways

- While speaking on "Modernization of Fire Protection Infrastructure at Ammunition Depots", Col. Gill highlighted that depots are usually spread over vast areas with wild vegetation and undergrowth which pose great fire risk.
- The pilot project to modernise the infrastructure was taken up at 3 depots initially and included both Security and Fire Fighting Systems.
- Later this project was expanded to 16 Ammunition Depots spread over 20 locations. The fire-fighting infrastructure has following three main components:
    - ❖ Fire Detection System for both Smoke & Flames.
    - ❖ Fire Fighting System with Remote Control Monitors (both water and foam application) connected to the water storage tanks.
    - ❖ Central Control Center that receives inputs on a single platform from all areas (Thermal Cameras, Intrusion Defectors, Fire Alarms and communication systems) which are collated and analysed for producing integrated depot level information and response.
- The aim of the project is first to prevent a fire incident, provide early warning and finally to ensure that the fire is put down in its nascent/ initial stage.

SESSION 5 - PROTECTION OF NAVAL ASSETS & SPECIAL CONDITIONS (1550 - 1700 HRS)

Chairperson - Cmde Gaurav Mehta, Cmde (Personnel Services) & Provost Marshall Navy - Introduction of Speakers and Opening Remarks by Chairman

Key Takeaways

- Our 'seascape' is at crossroads of important SLOCs where vagaries are unique not due to diversified terrain (as in land boundaries) but due to problems of 'visibility' and technology being limited only to SONARs
- The threats to naval bases are unique as they are mainly surrounded by urban agglomerations and dangers also of mines. Integrated Underwater Harbor Defense & Surveillance systems have been installed to enhance IN's capability and situational awareness and increase the capability of responding to threats.

Capt KP Sreesan, Capt (Staff Requirements) Anti-Submarine Warfare, Naval HQ. - Protection Against Mines & Underwater Threats

Key Takeaways

- Explained at length about underwater threats i.e., clandestine attacks, sea mines, and torpedoes as well as clandestine attacks i.e. underwater sabotage threats which makes harbor protection immensely important with the installation of physical barriers, portable diver detection SONARs as well as boat patrols.
- Also spoke on Mines and its countermeasures as they pose a very big threat to naval ships. He explained MCMs (both offensive as well as defensive) and unmanned solutions like UUVs. In Anti-Torpedo Defence systems. He explained the 'towed array', 'towed decoy', and 'expendable decoy' systems.
- In conclusion, he said, underwater sea operations are 'low-risk, high return' in nature. Sea-borne trade is very important for the economic well-being of our country, so naval force protection becomes very important.

Dr Amreek Singh, Addl Director & Head Avalanche Forecasting Div, Defence GeoInformatics Research Establishment, DRDO - "Protection Against Avalanches and Recovery

Key Takeaways

- Explained what avalanches are and shared data regarding them, like the most dangerous weather situation is 'clear day after cessation of the storm' and the most dangerous month is 'March'. He at length also explained the socio-economic, environmental, and psychological impact of avalanches on the general public and forces.
- He also gave a presentation on 'Avalanche Hazard Mitigation' elucidating active (artificial triggering, detection radars & afforestation) and passive measures (mapping, forecasting, and capacity building)
- He also explained how (for civil users) Avalanche Warning Bulletins are released with 'color coding') as per threat perception and how they have been integrated with the SACHET Alert system prepared by NDMA.