Centre for Aerospace Power and Strategic Studies

Report on

CAPSS-IMR Seminar and Exhibition on

'C4I2 and Network-Centric Warfare'

11 November 2025

SESSION I

INAUGURAL SESSION

Welcome Address

Air Vice Marshal Anil Golani (Retd), Director General, Centre for Air Power Studies

Air Vice Marshal Anil Golani highlighted that the nature of warfare is undergoing a rapid transformation, with network-centric warfare now being key to operational success in modern conflicts. He emphasized that real-time data, resilient networks, and the ability to make fast, precise decisions are what define victory today. He further highlighted India's capacity to respond to diverse operational theatres, from high-altitude challenges to maritime competition, and pointed to recent Ladakh operations as proof of the effectiveness of integrated surveillance and secure communications. He discussed advances in secure digital networks, multi-sensor fusion, SATCOM resilience, and the foundational role of cyber and space operations. AVM Golani also noted emerging vulnerabilities, especially in cyberspace and electromagnetic domains, which require resilience and robust security designs. He stressed that despite technological advancements, doctrines, leadership, and the capabilities of trained operators remain central to defence success and that the seminar should yield actionable recommendations for India's military preparedness.

Special Address

Air Marshal Ashutosh Dixit AVSM VM VSM, Chief of Integrated Defence Staff

Air Marshal Ashutosh Dixit said that network-centric warfare, with its emphasis on indigenous innovation and integrated warfighting, has fundamentally transformed India's approach to military operations. Reflecting on a coordinated tri-service campaign, Air Marshal Dixit described how real-time ISR data, AI-enabled munitions, and system integration allowed precise targeting deep inside adversary territory, all without broad escalation or collateral risk. He highlighted the role of the Integrated Air Command and Control System (ICCS), electronic warfare successes, and the seamless operation between air, land, and naval assets. The speaker credited India's industry for resilient communication and indigenous defence systems and noted the growing role of artificial intelligence including the promise and challenges of possible artificial general intelligence. He concluded by affirming that technological sovereignty, operational adaptability, and cognitive dominance are vital, but ethical stewardship and human judgment must remain at the forefront as the country transitions to more advanced warfighting capabilities.

Keynote Address

Mr Manoj Kumar Dhaka, DS & DG DEAL, DRDO

Dr Manoj Kumar Dhaka mentioned that while India has made notable achievements in network-centric warfare, further progress is needed in the areas of interoperability, integration of diverse legacy and new systems, and doctrinal development. He described the challenges of integrating equipment with varied standards, especially those from foreign suppliers, and emphasized the need for indigenous solutions to ensure control and security. The speaker discussed the fast-paced evolution of information and communication technology, the looming challenge of data overload from expanded sensor deployments, and the requirement for automated data filtration. He also spoke about developing joint operational standards, enhancing cyber resilience, and the ongoing work on new projects—such as military IoT, 5G communications near borders, and intelligent radios capable of adaptive anti-jamming. He concluded that continuous local innovation, robust industry-academia cooperation, and comprehensive system standardization are essential for maintaining India's technological edge in defence.

Inaugural Address

Air Marshal Narmdeshwar Tiwari SYSM PVSM AVSM VM, Vice Chief of Air Staff

Air Marshal Narmdeshwar Tiwari said that network-centric capabilities are profoundly beneficial for the Indian Air Force, describing the historic trajectory from fragmented sensor coverage to the development of an integrated national air defence network. He emphasized how multi-decade efforts in integrating diverse radar technologies and building the ICCS platform have enabled comprehensive situational awareness and more efficient resource allocation. Air Marshal Tiwari reflected on the importance of continuous development, noting that integrating new weapon and sensor systems is an ongoing process, much like the evolution of the internet—it is never truly complete. He cautioned that protecting the network from both external and internal vulnerabilities is paramount, and industry must provide solutions that are both technically sound and secure. The address highlighted the need for ongoing vigilance and adaptability in both technology and doctrine to maintain readiness for current and future threats.

Industry Perspective

Col KV Kuber (Retd), Director Defence & Aerospace, Ernst & Young

Col KV Kuber mentioned that advancements in C4I2 systems have revolutionized military doctrine and operations across all domains. He pointed out that India's private sector contributes significantly by delivering modular, interoperable platforms and robust communications. Col Kuber stressed that procurement must shift from purely platform-centric approaches to partnerships focused on adaptive solutions and continuous support. He noted the importance of upgradeable, standardized, and export-ready technologies as India aims to become a central hub in global defence innovation and manufacturing.

The session concluded with book release titled 'India's Aerospace Power: The Central Asian Dynamics' by Gp Capt (Dr) Rajneesh, Senior Fellow, CAPSS. IMR also launched a knowledge paper in collaboration with EY titled 'Surveillance and Electro--optic Devices'.

SESSION II

BACKBONE OF MODERN WARFARE – INNOVATIONS IN C4I2 SYSTEMS

Chair: Air Vice Marshal Rahul Bhasin, VSM

Opening Remarks by the Chair

Air Vice Marshal Rahul Bhasin, VSM, set the tone for the session with introductory remarks emphasising the enduring nature of warfare, though its conduct has evolved significantly in the modern era. He highlighted the important role of **Command, Control, Communication, Computers, Intelligence and Information (C4I^2)** systems in modern warfare. He noted that innovation in C4I2 systems is the hallmark of modern warfare and introduced the distinguished panel of experts comprising serving officers, retired officers, representatives from DRDO laboratories, and international industry leaders.

Panel Presentations & Key Discussions

Rear Adm Mohit Gupta (Retd), VSM, Cyber Sec Consultant

Rear Admiral Mohit Gupta (Retd), VSM, Cyber Security Consultant, delivered an insightful presentation on *“Net-Centric Operations in the Indian Navy.”* He provided a comprehensive overview of the Navy’s evolution into a network-centric, multidimensional maritime force operating across vast ranges with over 180 ships and submarines. Tracing the journey toward self-reliance under the *Atmanirbhar Bharat* initiative, he highlighted key indigenous developments driven by the Weapons and Electronics Systems Engineering Establishment (WESEE), the Naval Communication Network (NCN) systems, the DRDO-developed Trigun System, and customised encryption protocols. He elaborated on the integration challenges of fusing multi-sensor underwater data into combat management and communication systems, and noted the replacement of the Rukmani Satellite with GSAT-7R to enhance connectivity. Rear Admiral Gupta underscored the importance of data accuracy, latency, and real-time targeting, particularly in missile operations. He was also drawing attention to emerging vulnerabilities such as supply chain attacks and the risk of breaches even in air-gapped networks. He emphasised the need for resilience and bandwidth diversification to secure naval communications and cited the role of the Information Fusion Centre–Indian Ocean Region (IFC-IOR) in facilitating data sharing through bilateral arrangements. Addressing the growing threat of GPS spoofing, he pointed to the reliance on NAVIC and sophisticated algorithms to maintain signal integrity. Concluding his address, he asserted that interoperability among the three services is both technologically feasible and strategically imperative, reaffirming that indigenisation and self-reliance must remain the guiding principles of India's defence modernisation

Wg Cdr Deepak Prasad, Chief Devp Officer AI, UDAAN Dte, Air HQ:

Wing Commander Deepak Prasad, Chief Development Officer (AI) at the UDAAN Directorate, Air Headquarters, delivered an engaging presentation on *"Integrating AI with C4I2 Systems for Faster and More Accurate Command Decisions."* He addressed the growing challenge of information overload in modern command systems, where vast amounts of sensor data often surpass the capacity of human operators to process and respond effectively. Emphasising the pivotal role of Artificial Intelligence (AI), he described it as the *"adrenal"* to C4I2, energising and accelerating decision making to achieve faster, more accurate, and autonomous operations. He elaborated on the AI-enhanced OODA Loop, which enables detection-to-decision processes in under a minute through automated data fusion, predictive analytics, and coordinated response mechanisms. Highlighting key AI components such as Natural Language Processing for instant operational summaries, Reinforcement Learning for tactical simulations, Computer Vision for intelligence, surveillance, and reconnaissance (ISR), and Predictive Analytics for threat forecasting, he underscored their growing operational relevance. He further outlined critical implementation imperatives, including data standardisation, establishment of joint AI cells, embedding AI doctrines within command frameworks, and ensuring sustainability through continuous retraining and refinement of models. Drawing global parallels, he cited the U.S. JADC2 and Project Maven initiatives, where more than 60% of efforts focused on data standardisation to enable AI integration. For

India, he proposed a domain-led, collaborative approach involving joint development across services, deployment of AI fusion nodes, adoption of edge computing, and creation of secure, air-gapped defence clouds. Concluding his address, Wg Cdr Prasad asserted that AI-driven C4I2 systems would fundamentally transform decision cycles, enhance situational awareness, and ensure mission effectiveness across strategic, tactical, and logistical domains.

Smt Anireddy Bhavani, Sc G, DLRL, DRDO:

Smt. Anireddy Bhavani, Scientist 'G' at the Defence Electronics Research Laboratory (DLRL), DRDO, delivered an insightful presentation on *"DLRL's Contributions to AI/ML-Driven C4I Platforms."* She traced the evolution of DLRL since its establishment in 1961 into India's premier R&D organisation for Electronic Warfare (EW) systems, highlighting its integration of Artificial Intelligence (AI) and Machine Learning (ML) technologies across communication, radar, and command domains. She described the transition of EW systems from conventional to cognitive electronic warfare, enabling autonomous decision-making with response times measured in milliseconds. DLRL's application of deep learning, supervised and unsupervised ML, natural language processing (NLP), federated learning, and transfer learning was shown to significantly optimise limited EW resources and operational efficiency. Among notable use cases, she cited AI-based radar mode detection for air platforms, counter-drone systems using spectrogram-based classification, and smart sensing with predictive emitter identification. She also highlighted the integration of multi-sensor data fusion combining RF, EO/IR, and radar inputs to enhance situational awareness and decision support. Additionally, Smt. Bhavani detailed the development of AI-enabled control entities for mission planning and real-time data analysis using Spark-based architectures, alongside DLRL's collaborative initiatives with academia for model development and system enhancement. She concluded by emphasising that the integration of AI and ML is vital to achieving cognitive adaptability and maintaining electromagnetic spectrum dominance in the evolving landscape of modern warfare.

Mr. Zvika Zuckerman & Gp Capt Amit Sharma (Retd) Rafael Advanced Defense Systems:

Mr. Zvika Zuckerman and Gp Capt Amit Sharma (Retd) from Rafael Advanced Defence Systems jointly delivered a presentation on *"Combat Cloud Solutions in the Battlefield for Communication and Sensing."* Mr. Zuckerman introduced the Rafael Combat Cloud, describing it as a comprehensive network-centric warfare solution that enables real-time information sharing, situational assessment, and coordinated multi-domain operations. He elaborated on how the system supports GPS-independent targeting, multi-sensor AI-driven data fusion, and real-time Intelligence, Surveillance, Target Acquisition, and Reconnaissance (ISTAR) capabilities, thereby enhancing operational freedom and decision-making in contested environments. Building on this, Gp Capt Amit Sharma (Retd) highlighted the Make in India collaboration between Rafael and Astra Microwave, emphasising the development of Software Defined Radios (SDR) and the BNet communication systems designed to ensure interoperability, resilience, and self-sufficiency in networked operations. Together, they underscored that such integrated combat cloud solutions represent the future of multi-domain connectivity, providing a unified, secure, and adaptive digital backbone for modern warfare.

Gp Capt Ritu Raj Tyagi (Retd) – SAAB India Technologies

Group Captain Ritu Raj Tyagi (Retd) from **SAAB India Technologies** delivered an engaging presentation on *"Software-Defined, AI-Powered Combat Systems."* He highlighted Saab's longstanding legacy of innovation in network-centric and AI-enabled defence technologies spanning the air, naval, and land domains. Elaborating on Saab's unique design philosophy, he explained how a unified AI software core can be seamlessly integrated across multiple platforms, ensuring rapid adaptability, scalability, and sustained operational relevance. Emphasising Saab's agile research and development culture, he noted the company's capacity to translate technological innovation into operational capability at remarkable speed. Gp Capt Tyagi concluded by asserting that software-defined architectures and AI-driven adaptability will be the cornerstone of future combat readiness, enabling forces to stay ahead in an era of rapid technological evolution and dynamic operational challenges.

Mr. Roberto Simonetti Spallotta – Chief Rep Officer India, ELT Group

Mr. Roberto Simonetti Spallotta from ELT Group delivered a detailed presentation on *"Advanced Electronic Defence and EMSO-C2 Systems."* He highlighted ELT Group's global expertise in Electronic Defence and Electromagnetic Spectrum Operations (EMSO), noting the company's extensive operational footprint with over 3,000 systems deployed worldwide. Emphasising the importance of collaborative integration and scalable multi-sensor architectures, he described how ELT leverages artificial intelligence and deep learning to achieve electromagnetic dominance across modern battle spaces. Mr. Spallotta outlined the company's key contributions, including advanced EMSO Command and Control (C2) solutions, big data management frameworks, unmanned threat assessment systems, and simulation-based operator training tools designed to enhance situational awareness and mission effectiveness. He concluded by underscoring that ELT's integrated approach—combining cutting-edge technology with operational experience—enables seamless coordination within joint operations frameworks, strengthening electromagnetic superiority in complex, multi-domain warfare environments.

Question and Answer Session:

The Q&A session brought out appreciation of the critical role of AI, networking, and edge-based systems in shaping future warfare capabilities. Participants enquired about the importance of industry–start up collaborations to strengthen the national defence innovation ecosystem. The recent roll-out of IRSA (Indian Regional Security Architecture) as an example of integrated technological synergy was brought out by panellists and they also emphasised the need for global interoperability through coordinated frameworks such as SAAR overlays.

SESSION III

CONNECTING THE BATTLESPACE FOR OPERATIONAL SUPERIORITY

Chair: Commodore SS Dhody, Addl DG, Wpns & Electronics Sys Engg Estab, NHQ

Opening Remarks by the Chair

The third session focused on the theme of connecting the battlespace to achieve operational superiority. In his opening remarks, Commodore SS Dhody described C4I2 as the nervous system of connected warfare. He emphasised that it serves as the vital framework enabling modern forces to coordinate and act effectively. He observed that the concept is not new but gained momentum as the United States shifted its approach in the 1990s.

He traced the evolution of warfare systems from platform-centric models to network-centric and now to data-centric operations. According to him, this ongoing transformation marks the third revolution in modern warfare, driven by the power of data and digital connectivity.

He outlined four pillars of modern warfare: sensor-based capabilities, information structure, command centre and TERA (Threat Evolution and Resource Allocation). He stated that these four pillars collectively represent a modern iteration of the OODA loop (Observe, Orient, Decide, Act), adapted to the dynamic data environment of contemporary battlefields.

Panel Presentations & Key Discussions

Group Captain SS Walasang, Gp Capt IACCS (Plg & Proj), Air HQ

Group Captain SS Walasang spoke on the “Integrated Air Command and Control System (IACCS)” and its role in network-centric warfare. He focused on how artificial intelligence supports data management, situational awareness, and threat assessment. He explained that IACCS enables real-time communication and collaboration across the operational network. It serves as the backbone of net-centric operations, linking sensors, decision-makers, and weapon systems through seamless data exchange.

He highlighted the growing use of AI in the OODA Loop, noting that it allows faster, data-driven decision-making. AI tools enhance every phase of the process, from observation to action, by improving accuracy and speed of response. He outlined several areas of AI employability. These include hyper-personalisation, pattern recognition, predictive analysis, goal-driven systems, autonomous functions, and advanced pattern analysis. He added that AI also strengthens decision-support tools and network monitoring systems. He emphasised cybersecurity as an essential component of network-centric warfare. He also called for the development of scientific systems such as AI-based testbeds to refine operational capabilities.

The speaker identified data quality and availability as significant challenges. He concluded by emphasising that India must invest continuously in AI-enabled systems to maintain operational readiness in the evolving digital battlespace.

Capt Kunal Tiwari, Naval HQ

Capt Tiwari delivered an insightful presentation on “AI-Enhanced Combat Management System (CMS). He began with tracing the historical development of home-grown C4ISR capabilities within the Indian Navy. He highlighted the development from EMCCA to the CMS to show the evolution of combat management.

He explained that the modern CMS ensures greater operational transparency through predictive modelling, detection, classification, and continuous tracking of targets. With advanced sensor fusion, the system combines inputs from multiple sensors and platforms to create a unified, real-time operational picture. The system enhances threat classification and situational awareness, enabling commanders to interpret data and make informed, timely decisions quickly. Its AI components enable automated analysis and prediction, thereby reducing the workload for humans during complex missions.

The speaker highlighted key challenges, including electronic jamming and cybersecurity vulnerabilities. He underlined the need for robust protection against interference and data breaches. He concluded that AI integration must extend across all domains of warfare, air, land, sea, space, and cyber, to create a fully connected and responsive combat environment for future operations.

Brig (Dr) Vivek Verma (Retd) Sr Research Fellow, USI

Brigadier (Dr) Vivek Verma spoke on “Integration of Artificial Intelligence in Surveillance and Target Acquisition”. He explained that the traditional kill chain is being redefined through technologies such as computer vision, machine learning, pattern recognition, and predictive analysis. He highlighted that in modern warfare, intelligence, surveillance, and reconnaissance (ISR) operations are increasingly driven by algorithms and data rather than raw firepower. Victory, he noted, will belong not to those who fire first but to those who see first.

Brigadier Verma observed that the battlefield of today has compressed—from engagements lasting days to decisions made in seconds, and from localised zones to a global operational space. He pointed to rapid growth in the global AI defence market, where developments in automation and real-time analytics are transforming decision cycles.

He illustrated these points through examples such as the Russia–Ukraine conflict, describing it as the first large-scale real-time AI-enabled war. He noted Russia’s constraints due to a lack of advanced processors, contrasting this with industrial-scale AI-targeting seen in conflicts involving Israel, Gaza, and Iran.

He discussed key challenges, particularly the architectural difficulty of integrating AI systems with legacy platforms. He also drew attention to the significant advancements made by the PLA in AI-enabled warfare, warning that any delay in adaptation would be dangerous. He concluded with a remark that delay equals defeat, noting that each year of inaction widens the technological gap exponentially.

Question and Answer Session:

The Q&A session brought out several important reflections on the theme of AI-enabled connected warfare. Participants emphasised that humans must always remain in the decision loop. A primary concern raised was the persistence of data silos, which limit information sharing and reduce the effectiveness of AI across integrated domains. It was also noted that AI technology is dual-use and equally accessible to adversaries. Hence, the same systems designed to provide an operational edge could be exploited by opponents to develop countermeasures.

SESSION IV

CYBERSECURITY AND RESILIENCE IN C4I2 SYSTEMS

Chair: Rear Admiral Sanjay Sachdeva, NM, DG Defence Cyber Agency

Opening Remarks by the Chair

Rear Admiral Sanjay Sachdeva, the session chair, opened the discussion by establishing the foundational concept that C4I2 systems function as the nervous system of military operations. Joshi emphasised several critical points about the operational environment:

Multi Domain Operations: Modern military operations are no longer confined to single domains. Civil and military infrastructure must be integrated, and all forces must work together seamlessly. This integration extends across land, sea, air, cyber, and space domains, creating a complex ecosystem where actions in one domain can have cascading effects in others.

Joint Cyberspace Doctrine: The release of the joint cyberspace doctrine represents an important step in addressing cyber operations as a strategic concern. The decision to unclassify cyber doctrine reflects a recognition that the effects of cyber operations can be felt within minutes, making this domain as operationally significant as traditional military domains.

Technological Maturity and Collaboration: While technology continues to advance, Joshi noted that full technological maturity has not yet been achieved. The solution lies in collaboration between technologists and military strategists, between different services, and between civilian and military experts. This requires developing synergy between cyber discipline and trained minds across organisations.

Security Across All Systems: The integration of civil and military infrastructure means that security must be consistently applied across all systems. This consistency is often challenging because civil infrastructure was not originally designed for military-grade security, and retrofitting creates complications.

In the cyber domain, the distinction between peacetime and wartime operations has become unclear. Cyber-attacks can occur at any time, and the threshold for what constitutes an act of war remains a subject of debate internationally. Networks that can be attacked must be assumed to be under threat constantly.

Panel Presentations & Key Discussions

Navin Chawla, Poly Business Leader, BizAnekdotes

Navin Chawla through his talk on 'HP and Pexip's Intelligent Collaboration Solutions' presented technological solutions for ensuring security and reliability in modern communication systems, particularly for hybrid meetings and remote operations.

Communication Infrastructure: HP offers a comprehensive portfolio of solutions including all-in-one video bars, USB video bars, Windows-based modular systems, and Android-based solutions. These are designed to provide premium video and audio quality, which is essential for command and control operations where clear communication is critical.

Smart Camera Technology: The smart camera technology Chawla discussed employs automatic framing modes that enhance the user experience. In operational environments, this technology helps ensure that key participants are always visible and communication flows smoothly without technical interruptions.

Security Features for Private Meetings:

Several security measures are built into the HP system:

- **Custom Layouts and Participant Control:** The system allows for custom layouts where specific participants can be pinned, and breakout rooms can be created for compartmentalised discussions.
- **Dual Authentication:** A dual-authentication method ensures that only authorised personnel can access meetings. This is critical in military communications where access control is non-negotiable.

- **Direct Communication Channels:** The web scheduler, message overlay, and direct chat functions provide multiple communication channels that can be used depending on classification levels and security requirements.
- **Private AI Platform:** The private AI platform requires no connectivity to the public internet or the cloud. This is a critical security feature because it prevents potential interception or data exfiltration through public networks.
- **Full User Control:** Users maintain complete control over the infrastructure, layout, and participation, ensuring that military organizations can enforce their own security protocols.

AI-Powered Features: HP's system is the first to introduce AI-powered auto framing and intelligent layout capabilities for any meeting participant. This reduces the need for technical staff to manage meetings and allows military personnel to focus on content and decisions rather than technical details

Gp Capt Thomson George, Gp Capt Ops IW, Air HQ

Gp Capt Thomson George gave talk on ‘Addressing Vulnerabilities in C4I2 Systems to Ensure Mission Success’. His presentation focused on understanding the evolving threat landscape and developing comprehensive approaches to vulnerability management.

Evolution of the Threat Landscape:

The nature of threats to C4I2 systems has changed significantly:

- **Threat Actors:** Traditional state actors remain a concern, but the threat landscape now includes growing private sector mafias, criminal organisations, and non-state actors. These actors have varying motivations and capabilities, requiring different defensive strategies.
- **Threat Scenarios:** Modern threats are characterized by attempts to disrupt information flow, degrade digital situation awareness, and conduct more persistent, targeted, and coordinated attacks. The sophistication of coordinated attacks has increased substantially.

Four Categories of Vulnerabilities:

George identified four main categories of vulnerabilities in C4I systems:

1. **Hardware and Software Cluster:** Physical components and the software running on them can be compromised through supply chain attacks, manufacturing flaws, or software vulnerabilities. Both must be secured.
2. **Network and Communication:** The systems that connect different nodes of the C4I network can be intercepted, jammed, or degraded. Network security and redundancy are essential.
3. **Human and Operational:** People operating the systems represent a vulnerability through mistakes, inadequate training, or malicious insider action. Operational procedures must take into account human factors.
4. **Intelligent Systems:** Artificial intelligence and automated decision-making systems can be manipulated, poisoned with false data, or exploited through their algorithmic weaknesses.

He summarised his talk by giving solutions:

1. **Robust Incident Response and Recovery Capabilities:** Organisations must prepare for the reality that attacks will occur. Having well-developed incident response procedures and recovery capabilities minimises damage.
2. **Binding Process Through Governance, Audits, and Oversight:** Governance structures, regular audits, and oversight mechanisms ensure that security policies are actually implemented and maintained over time.

Col Deepak Joshi, Retd, CISO, Hewlett Packard Enterprise

Col Joshi through his talk on ‘Emerging Threats to Net-centric Infrastructure’ identified sensors as a major component of NCW that is vulnerable to attack. Sensors are the input to the C4I2 system, providing the information on which all decisions are based. If sensors are compromised or if false data is fed into the system, the entire operational picture becomes unreliable.

Cross-Cutting Themes and Implications

Several themes emerge across all four presentations:

Security is Multifaceted- No single technological solution solves the security problem. Security requires attention to hardware, software, networks, human factors, and institutional structures. The HP solutions presented address one aspect - secure communication - but this must be part of a broader security framework.

Resilience - Rather than trying to achieve perfect security, military organisations must accept that breaches will occur and build systems that can function despite compromises. This requires redundancy, backup systems, training, and institutional support. In the cyber domain, effects can be felt within minutes. Organisations must have the capability to detect, respond to, and recover from attacks with similar speed. This requires trained personnel, pre-planned procedures, and often automation.

Integration Creates Vulnerability- While the integration of civil and military systems, multiple domains, and various services creates operational advantages, it also introduces vulnerabilities. Any weakness in any component can potentially affect the entire system. This requires comprehensive security approaches rather than point solutions.

Institutional Preparedness is as Important as Technology; Technology Alone Cannot Solve Security Problems. Organisations must have governance structures, trained personnel, clear procedures, cultural commitment to security, and regular exercises to test their readiness. These institutional factors are often the limiting factor in actual security.

Constant Evolution is Required - The threat landscape is constantly evolving. New threat actors emerge, attack methods become more sophisticated, and new vulnerabilities are discovered. Security approaches must evolve continuously through regular assessment, learning from incidents, and adaptation.

Closing Address

Air Vice Marshal Anil Golani (Retd), Director General, CAPSS

DG CAPSS conclusively brought out that the fundamental message across all presentations is that mission success in the modern security environment requires comprehensive, coordinated, and continuous effort across technical, operational, and institutional domains. No single actor or technology can solve the problem on its own. Success requires synergy between cyber experts and trained military minds, between civilian and military organisations, between different services and agencies, and between technical specialists and policy makers.

As militaries continue to depend more heavily on C4I2 systems and net-centric operations, the importance of addressing these vulnerabilities and building comprehensive security and resilience approaches will only increase. The experts in this session have identified the critical challenges and outlined pathways forward; however, implementing these approaches remains an ongoing challenge for military organisations worldwide.