ENGINE AS A WEAPON XI

26 – 27 NOVEMBER 2025

SECURITY CONSIDERATIONS FOR DESIGN, DEPLOYMENT AND MAINTENANCE OF FUTURE WIRELESS TECHNOLOGY NETWORKS IN THE NAVY

Captain (Dr) Nitin Agarwala

Indian Navy

Center for Joint Warfare Studies

Commodore (Dr) R K Rana

Indian Navy Veteran

PhD (IIT-M), MSc-Marine Engg(UK), BSc-Mech Engg (DU)
ME†, CEng (UK), FIMarE (I), FIMarEST (UK), MASNE (USA)

INTRODUCTIONS
CAPTAIN (DR) NITIN AGARWALA

- PhD (Cochin University of Science and Technology), Mtech (OE&NA) (IIT, Kharagpur), Dip IIT (Naval Construction) (IIT, Delhi), BTech (NA&SB) (Cochin University and Science and Technology)
- A **Naval Architect by profession**. Has experienced various facets of a warship as a user, designer, inspector, maintainer, a policymaker, a teacher and a researcher.
- Is a serving naval officer
- Has **authored** over 80 articles, papers, book chapters and two books entitled "*Deep Seabed Mining in the Indian Ocean: Economic and Strategic Dimensions*" and "*Rise of China as a World Leader in Commercial Shipbuilding*".
- **Research interests** include Shipbuilding and associated technologies, Decarbonisation in the maritime sector, Deep Seabed Natural Resource, Submarine Cables, Blue Economy, Artificial Intelligence, Marine Pollution, Climate Change in the maritime domain, Blue Economy, and 'Maritime technological issues' with their linkages to International Relations and Public Policy.
- Was a **Research Fellow** at the National Maritime Foundation from 2017-2019 and a **Senior Fellow** at the Centre for Joint Warfare Studies (CENJOWS) from 2023-2025.
- **Presently** a Visiting Faculty at the Naval War College, Goa and the Centre for Maritime Studies at the University of Mumbai with **two doctoral students** working under him.

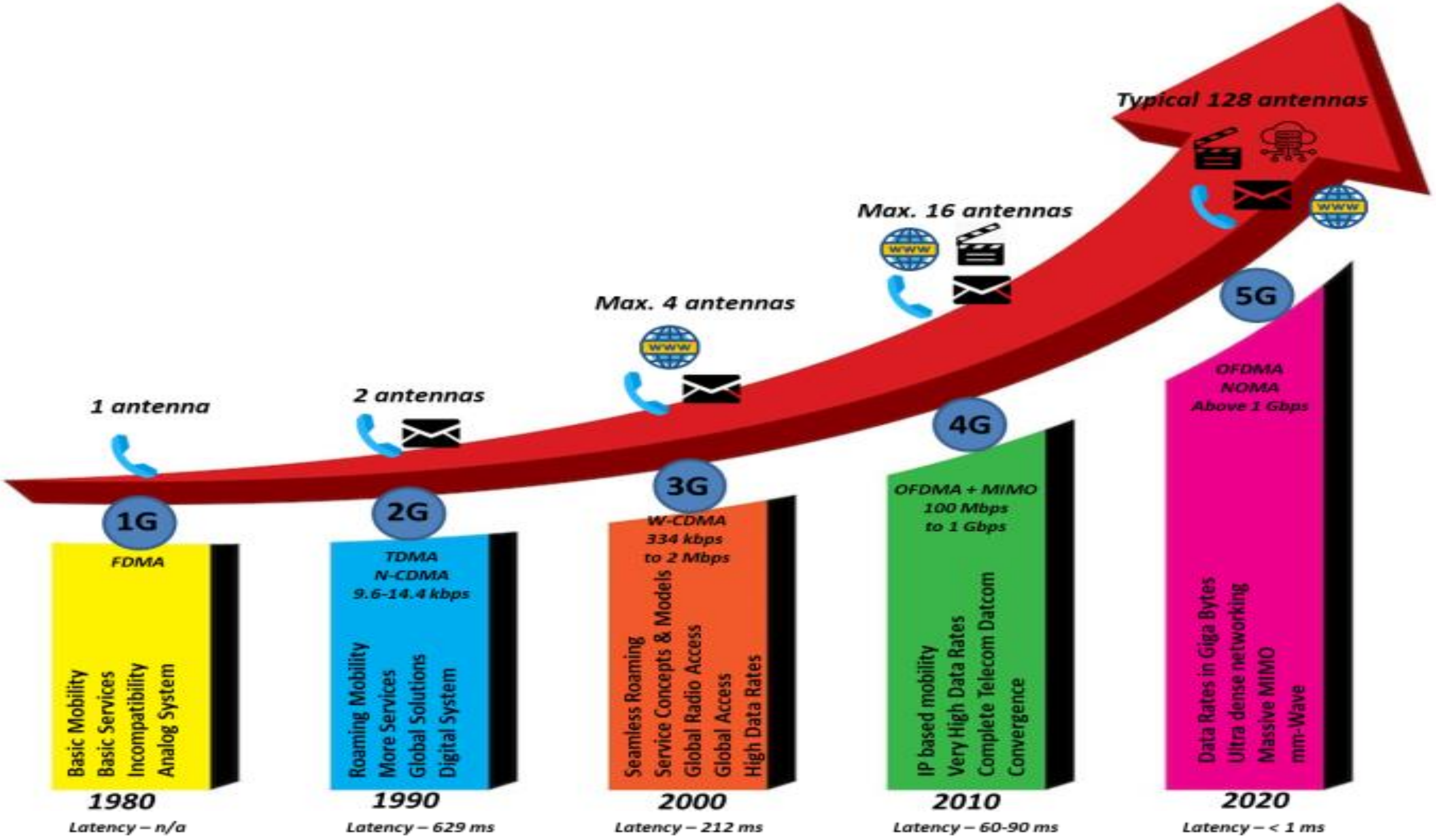
INTRODUCTIONS
COMMODORE (DR) R K RANA

- **Ph D** from IIT Madras, **M Sc** (Marine Engineering, UK), **B Sc** (Mechanical Engineering, DU).
- Served for more than **33 years** in the **Indian Navy** before premature retirement on 31 Oct 12.
- Served on board variety of warships, and wide spectrum of shore jobs – naval dockyards, training, research and development, warship design, indigenous product development.
- Part of the design team designing **Indigenous Aircraft Carrier** **(commissioned in Sep 22)** and **Corvettes** (**all 4 sailing now**)
- **Lloyd's Register** - Dec 2012 to Jun 2016.
- Special Invitee in the Planning Board of Delhi Technological University (Formerly Delhi College of Engineering),Delhi – **At present**
- Startup Strategy Advisor at DTU – Innovation and Incubation Foundation. – **At present**
- Adjunct Faculty at Bharti School of Telecommunication Technology of IIT Delhi - **At present**
- **Member** of American Society of Naval Engineers, USA.
- **Fellow** of the Institute of Marine Engineering, Science and Technology (IMAREST), London, UK
- **Technical Advisory Committee member** for the International Naval Engineering Conference (INEC) and Engine As A Weapon (EAAW) conferences / Symposium organized by IMAREST, UK.
- Former member of the Apex Advisory Committee (R&D) of Tehri Hydropower Development Corporation India Limited, Rishikesh, India.
- More than **72** publications/presentations.

SCHEME OF PRESENTATION

- Introduction
- Use Areas of 5G in the Navy
- Commercial Vs Military 5G
- Challenges to address Data Security
  - In general
  - Naval Environment
- Ensuring Data Security
  - Design
  - Operation
  - Maintenance
- Efforts of the Indian Navy
- Use of AI and ML
- Closing Remarks

INTRODUCTION - WIRELESS TECHNOLOGY OVER THE YEARS



1 antenna

1G

FDMA

Basic Mobility
Basic Services
Incompatibility
Analog System

1980

Latency – n/a

2 antennas

2G

TDMA
N-CDMA
9.6-14.4 kbps

Roaming Mobility
More Services
Global Solutions
Digital System

1990

Latency – 629 ms

Max. 4 antennas

3G

W-CDMA
334 kbps
to 2 Mbps

Seamless Roaming
Service Concepts & Models
Global Radio Access
Global Access
High Data Rates

2000

Latency – 212 ms

Max. 16 antennas

4G

OFDMA + MIMO
100 Mbps
to 1 Gbps

IP based mobility
Very High Data Rates
Complete Telecom Datcom
Convergence

2010

Latency – 60-90 ms

Typical 128 antennas

5G

OFDMA
NOMA
Above 1 Gbps

Data Rates in Giga Bytes
Ultra dense networking
Massive MIMO
mm-Wave

2020

Latency – < 1 ms

Source: Authors

INTRODUCTION – FIFTH GENERATION WIRELESS TECHNOLOGY

- Based on the third Generation Partnership Project (3GPP) standard.
  - Transforming how information can be exchanged and threats addressed
  - By using higher throughput, higher connection capacity, higher user density, and lower latency for improved capabilities
- Services - space to the battlefield edge
- Facilitating the seamless integration of Artificial Intelligence (AI) and Machine Learning (ML)
- Operating between 24 and 300 GHz, 5G allows -
  - Control of swarm unmanned vehicles,
  - Assist simulation and training using Augmented Reality (AR) and Virtual Reality (VR),
  - Permit intelligence, surveillance, and reconnaissance (ISR),
  - Distributed control,
  - Smart warehousing and logistics,
  - Use of dynamic radio frequency (RF) spectrum
  - Minimizing vulnerabilities like electronic warfare (EW) jamming - essentially required by the military in this age of cyber warfare

INTRODUCTION – MARITIME & SECURITY

- **Maritime sector**
  - Traditionally slow to adopt new technologies
  - Disruptive innovations like 5G – Effectively utilized in Commercial Shipping, Ports, Shipbuilding, and logistics to name a few.
- **Security concerns during military use**
  - Available commercially-off-the-shelf (COTS) equipment require modifications
  - Use of open-source software,
  - Use of edge-computing for latency reduction,
  - Shift from software logic to management network operations,
  - Increased cost and complexity,
  - Proprietary effectiveness,
  - Leading to a measured pace of 5G adoption in the military globally.

INTRODUCTION – NAVY

- **Only Navy discussed**
  - Connectivity and Data Security at sea - Linking up at sea and using existing terrestrial networks when alongside.
  - Significant complication for ships - need to integrate wide range of
  - Internet of Things (IoT) devices & sensors,
  - Integrated Bridge Systems (IBS),
  - Integrated Platform Management Systems (IPMS),
  - Drones operating in all the three domains
  - Global variations in spectrum usage
  - Uses 28 GHz
  - Rest the world uses 24.5 GHz
  - LEO satellites by Starlink uses 26.5 - 40 GHz

SCHEME OF PRESENTATION

- Introduction
- Use Areas of 5G in the Navy
- Commercial Vs Military 5G
- Challenges to address Data Security
  - In general
  - Naval Environment
- Ensuring Data Security
  - Design
  - Operation
  - Maintenance
- Efforts of the Indian Navy
- Use of AI and ML
- Closing Remarks

USE AREAS OF 5G IN THE NAVY (1/5)

- **Enhanced Shipboard Connectivity and Internal Networks –**
  - High-Speed Data Transfer; Improved Crew Welfare; Real-time Monitoring & Diagnostics; Seamless Integration of Onboard systems.
- **Smart Repair Yards and Naval Bases –**
  - Automated Logistics & Asset Tracking; Smart Warehousing; Enhanced Security & Surveillance; Optimized Resource Management; Connected Maintenance & Repair.
- **Augmented and Virtual Reality (AR/VR) for Training and Mission Planning –**
  - Immersive Training Simulation; Collaborative Mission Planning; Remote Guidance & Assistance.
- **Enhanced Situational Awareness and Intelligence Gathering –**
  - Real-time Sensor Data Fusion; Edge Computing for Data Analysis; Improved Information Sharing.
- **Support for Autonomous and Unmanned Systems –**
  - Reliable Command & Control; High-Bandwidth Data Streaming from Autonomous Platforms; Coordinated Swarm Operations.

USE AREAS OF 5G IN THE NAVY (2/5)

- **Tactical Communications and Network Modernization –**
  - Secure & Resilient Tactical Networks; Dynamic Spectrum Utilization; Mobile Ad-Hoc Networks (MANETs); Integration with Satellite.
- **Cybersecurity Enhancements –**
  - Enhanced Security Protocols; Network Slicing for Security; Real-time Threat Detection and Response
- **Remote health care –**
  - Advise onboard doctors by those stationed ashore; Monitoring health of individuals in difficult environments.

Technology **still in developmental stages** for the maritime domain.

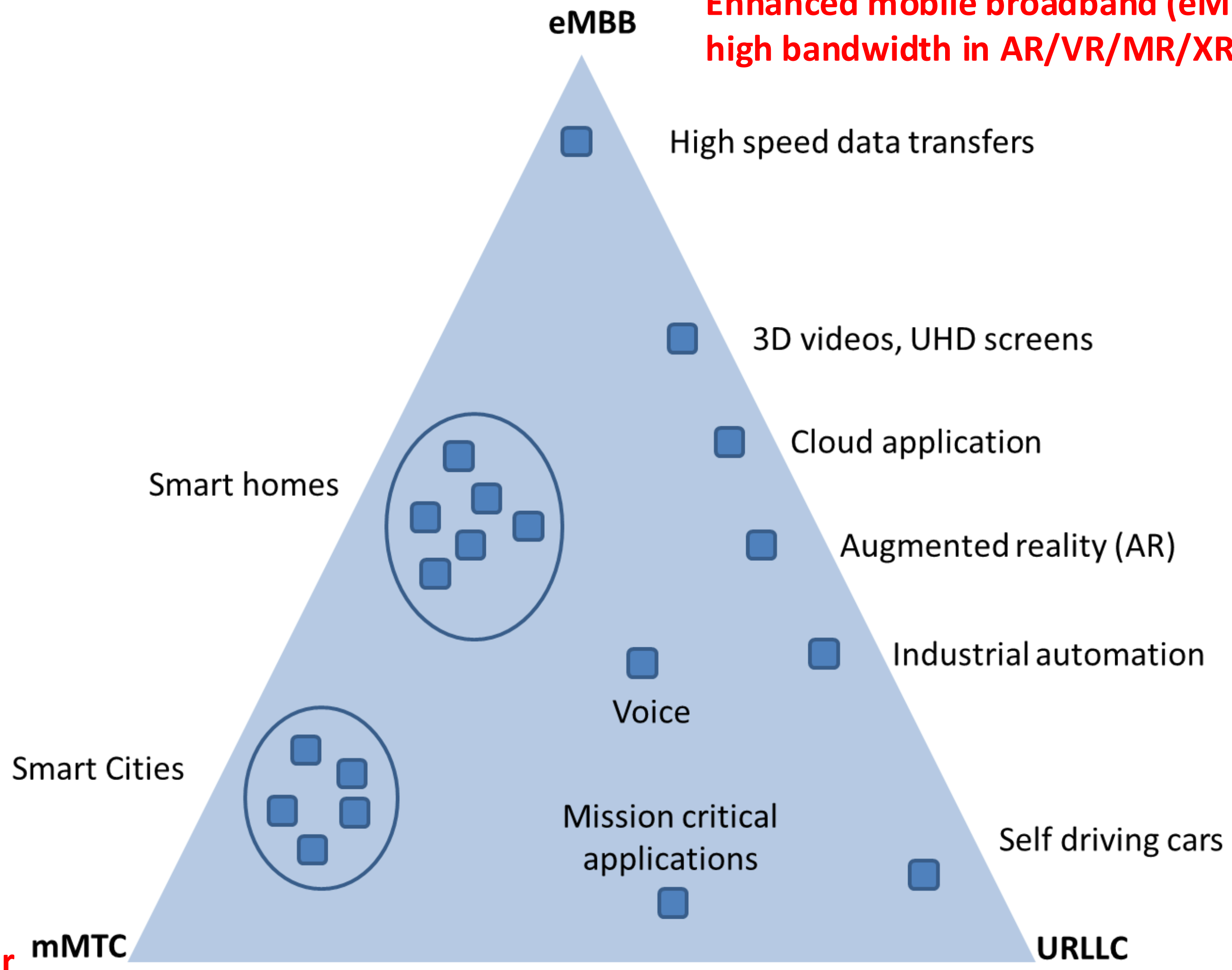
Has been experimented with for **numerous** activities.

USE AREAS OF 5G IN THE NAVY (3/5)

- **Continued evolution** will expand utility of 5G in the maritime domain.
- Lessons learnt & infrastructure established crucial for **transition to 6G**.
- 5G serves as **a pathway** to numerous **other innovations**.
- Due to **high data transfer speeds** marine & naval operations will be revolutionised at every level.

USE AREAS OF 5G IN THE NAVY (4/5)

Enhanced mobile broadband (eMBB) – for use of high bandwidth in AR/VR/MR/XR technologies



Ultra-reliable & low latency communications (URLLC) – where guaranteed connection & low latency is required especially in mission-critical applications

Massive machine type communications (mMTC) – when number of devices are more

USE AREAS OF 5G IN THE NAVY (5/5)

Three scenarios feasible to use 5G - Feasible only if Line-of-sight available

- ***Ship-to-ship communication*.**
  - Each ship has a 5G base station in sub-6-GHz (mid and low) freq. bands (gNB)
  - Form a meshed LOS network.
- ***Ship-to-shore communications*.**
  - Base station on ship and shore.
    - If range is more, communication through multiple hops.
  - Shore base station - public or private.
    - If public station, network slicing would be needed.
  - Complements / dispenses need for satellite communications.
- ***Ship-to-amphibious communication*.**
  - Relevant during amphibious warfare.
  - Uses a sub-1-GHz freq. on amphibious ship & LOS communication with mobile unit
  - For connectivity to HQ - sidelink-enabled 5G arrangement used.

SCHEME OF PRESENTATION

- Introduction
- Use Areas of 5G in the Navy
- Commercial Vs Military 5G
- Challenges to address Data Security
  - In general
  - Naval Environment
- Ensuring Data Security
  - Design
  - Operation
  - Maintenance
- Efforts of the Indian Navy
- Use of AI and ML
- Closing Remarks

5G IN COMMERCIAL AND MILITARY SECTORS

Feature / Aspect	Commercial Sector	Military Sector
Primary Objectives	Economic growth.	Operational effectiveness.
Performance Requirements	Broad coverage.	High reliability.
Security Requirements	Data protection.	Highly stringent.
Standardization Processes	Driven by international bodies / industry.	Uses military standards or modified commercial standards.
Deployment Environments	Terrestrial infrastructure.	Diverse domains.
Spectrum Usage	Unlicensed/ shared spectrum.	Dedicated spectrum.
Adoption Timelines	Usually rapid adoption.	Slow due to security concerns.
Focus for 6G	New economic models.	Multi-domain operations.

SCHEME OF PRESENTATION

- ➢ Introduction
- ➢ Use Areas of 5G in the Navy
- ➢ Commercial Vs Military 5G
- ➢ Challenges to address Data Security
  - In general
  - Naval Environment
- ➢ Ensuring Data Security
  - Design
  - Operation
  - Maintenance
- ➢ Efforts of the Indian Navy
- ➢ Use of AI and ML
- ➢ Closing Remarks

DATA SECURITY VS CYBER SECURITY

	Data Security	Cybersecurity
Focus	**Protecting data** throughout lifecycle	**Protect all components** of a computer system & network - hardware, software, infrastructure, and data.
Goal	**Ensures** confidentiality, integrity, and availability of **data**.	**Wider range of threats** – unauthorised access, data breach, malware attack etc.
Scope	**Concentrates on safeguarding data**, regardless of where it resides / processed /transmitted.	**Concentrates on** preventing, detecting, and responding to **cyber threats**
Examples	• Encryption (at rest and in transit) • Access controls (user permissions, role-based access) • Data masking and anonymisation • Data loss prevention (DLP) tools • Data backup & recovery procedures • Data classification and labelling • Data retention and disposal policies • Integrity checks and hashing	In addition to data security measures • Firewalls & intrusion detection/ prevention systems • Anti-malware software • Network security protocols • Security awareness training for users • Incident response planning and execution • Vulnerability management and patching • Security audits and penetration testing • Physical security of IT infrastructure

Our focus in this discussion is limited to Data Security

CHALLENGES – ENSURING DATA SECURITY (1/3)

- 5G network architecture - **provides greater attack area**.
  - Hence exposed to greater cyber threats.
- Being **commercially developed**, they need
  - Data protection & encryption when used for military applications.
- New Radio (NR) or IMT-2020 is a **civilian 5G standard**.
  - Cannot be used by military for fear of jamming & interference.
  - But, advantages offered have forced military to use civilian standards.
- 3GPP defined 5G network **susceptible to**
  - Fake & rouge base stations.
  - IMSI (International Mobile Subscriber Identity) catcher.
- Items **manufactured to civilian standards**
  - Subject to cyber threats
  - Manufacture military standards difficult - limited demand & hence cost.

CHALLENGES – ENSURING DATA SECURITY (2/3)

- **Trust Infrastructure.**
  - 5G uses a Public Key Infrastructure (PKI) system to establish identity.
    - Private key known only to system + Public key distributed to users.
    - If key compromised, can be reissued by changing user SIM.
      - Not feasible – due to high number of users in 5G.
        - Makes system vulnerable to spoofing & message alteration.
  - **If system unable to authenticate key**
    - Will deny services & system becomes unavailable.
- **Interconnection of Devices.**
  - IoT systems in 5G space vulnerable to
    - Eavesdropping, potential denial of service (DoS) attacks, & data collection devices.
  - For security & untested systems, manufacturer provides security updates.
    - Makes system and associated people vulnerable to cyber-attacks.

CHALLENGES – ENSURING DATA SECURITY (3/3)

Way Ahead

- To meet reliability and effectiveness
  - Resort to use of military proven components that are building blocks of 5G.

- Some such building blocks are
  - Self-organising networks (SON)
  - Software-defined networking (SDN)
  - Network function visualisation (NFV)
  - Multi access edge computing (MEC)
  - Multiple-input and multiple-output (MIMO)
  - Millimetre-wave (mmWave)
  - Device-to-device (D2D)
  - Integrated access and backhaul (IAB) and beamforming

CHALLENGES – NAVAL ENVIRONMENT

Data Security near maritime borders:

- Wireless signals from vessels near borders can be accessed by neighbours.

Need for interoperability:

- Wireless technology required along with existing legacy system.
  - Wireless networks need to operate seamlessly with diverse technologies in various ships.

Mobility and Dynamic Environment:

- Requires robust & secure wireless connectivity.

Electromagnetic Interference:

- Can affect wireless signal reliability & security.
- Needs to be addressed.

Supply Chain Security:

- Security of entire supply chain (hardware & software) critical to prevent introduction of compromised components.

SCHEME OF PRESENTATION

- Introduction
- Use Areas of 5G in the Navy
- Commercial Vs Military 5G
- Challenges to address Data Security
  - In general
  - Naval Environment
- **Ensuring Data Security**
  - **Design**
  - **Operation**
  - **Maintenance**
- **Efforts of the Indian Navy**
- **Use of AI and ML**
- **Closing Remarks**

ENSURING DATA SECURITY – DESIGN STAGE (1/2)

- **Threat modelling -** Identify potential vulnerabilities & attack vectors.
  - Include state-sponsored actors, cybercriminals, & insiders.
- **Security by design -** Introduce security at design stage.
  - Better than addressing security measures later.
- **Network Segmentation -** Prevent movement of attackers.
  - Separate networks for various activities be established
- **Encryption –** Strong encryption protocols (e.g., WPA3-Enterprise).
  - Enhances security even on open networks.

ENSURING DATA SECURITY – DESIGN STAGE (2/2)

- **Authentication -** Multi-factor authentication, to verify identity.
- **Authorisation -** Role-based access control.
- **Redundancy & Resilience –** Ensure operation under attack.
  - Use Geo-redundant hubs & multi-beam satellite capabilities.
- **Physical Security -** Protect network against man-in-the-middle attacks.
- **Choice of Equipment –** Avoid compromised components/ systems.
  - Select trusted vendors.
  - Prioritize devices that offer timely security patches.

ENSURING DATA SECURITY – DEPLOYMENT STAGE (1/2)

- **Secure Configuration -** for all devices, access points, routers, & switches.
  - Change default passwords immediately.
  - Disable unnecessary services and ports.
- **SSID Management –**
  - Avoid using easily identifiable SSIDs (Service Set Identifiers).
  - Disable SSID broadcasting to make network less visible to casual attackers.
- **MAC Address filtering –** For additional security
  - To restrict network access to only authorized devices.
  - Be aware that MAC addresses can be spoofed.

ENSURING DATA SECURITY – DEPLOYMENT STAGE (2/2)

- **Intrusion Detection and Prevention Systems (IDPS) –**
  - To monitor network traffic for malicious activity.
  - Automatically block or prevent potential threats in real-time.
- **Firewall deployment –**
  - To control network traffic.
  - Prevent unauthorized access between different network segments.
- **Guest Network Implementation –** Create guest network for visitors
  - To prevent unauthorized access to Navy's internal network.
- **Security Audits and Penetration Testing –**
  - Conduct before and after deployment.
  - To identify and address any vulnerabilities.

ENSURING DATA SECURITY – MAINTENANCE STAGE

- Regular Firmware and Software Updates
- Password management
- Security Monitoring & Analysis
- Incident Response Planning
- Security Awareness Training
- Vulnerability Management – Continuously scan for threats & take corrective action if found
- Performance Monitoring
- Auditing & Logging
- Secure Disposal of Equipment – Prevent loss of sensitive information

SCHEME OF PRESENTATION

- Introduction
- Use Areas of 5G in the Navy
- Commercial Vs Military 5G
- Challenges to address Data Security
  - In general
  - Naval Environment
- Ensuring Data Security
  - Design
  - Operation
  - Maintenance
- **Efforts of the Indian Navy**
- **Use of AI and ML**
- **Closing Remarks**

EFFORTS OF THE INDIAN NAVY (1/3)

- ***Human Resource Development*****:** Established wireless technology laboratories in over 20 academic institutions.
  - **Creating awareness and developing human resources for 5G and 6G**
- ***Dedicated Military Spectrum*****:** Defining a spectrum exclusively for military use
  - **To ensure secure communication**.
- ***Trusted Source Procurement*****:** Implementing 5G equipment 'trusted source' guideline
  - **To eliminate backdoor vulnerabilities**.
- ***Network for Spectrum (NFS):*** Establishing a secure, fibre-based backbone for defence communications.
  - To integrate optic fibre, satellite, and network systems **to enhance overall security and resilience of military networks**, including future 5G deployments.

EFFORTS OF THE INDIAN NAVY (2/3)

- ***Advanced Security Features***: Leveraging 5G security features such as adaptive frequency hopping, beam-forming, and AI-driven intrusion detection systems to counter EW threats and cyber-attacks.
  - **Will impede intercepting or jamming communications**.
- ***Active Involvement in 5G Standards***: Actively involved in evolving 5G standards for security and IoT.
  - **To address defence requirements in next-gen wireless ecosystem**.
- ***Defence Innovation Organisation (DIO) Initiatives***: Projects on wireless technologies nurtured & developed.
  - Encourages home-grown technology & strengthen Indian research.
  - Led to **development of wireless machine-to-machine communication infrastructure using 5G NR for IN ships**.
    - 5G NR can be used for data access & analysing data using AI/ML.

EFFORTS OF THE INDIAN NAVY (3/3)

- ***Software Defined Radios (SDRs):*** WESEE of *IN* involved in indigenous development and design of SDRs.
  - **Enhance** communication capabilities and security
  - **Support** network-centric operations.
- ***Indigenous 5G Infrastructure*:** DRDO, BEL, and C-DOT developing indigenous 5G infrastructure for defence.
  - **Create** a secure, encryption-protected, & EW-resilient 5G network
  - **Minimise** dependency on foreign technology while bolstering cyber security.
- ***NISHAR (Network for Information SHARing):*** *IN* & industry developed a tactical communication link to use between domestic & friendly nations.
  - Provides a unified Common Operating Picture (COP)
  - Equipped with powerful tools for streamlined operations, target tracking, incident reporting etc. for complete MDA.

SCHEME OF PRESENTATION

- Introduction
- Use Areas of 5G in the Navy
- Commercial Vs Military 5G
- Challenges to address Data Security
  - In general
  - Naval Environment
- Ensuring Data Security
  - Design
  - Operation
  - Maintenance
- Efforts of the Indian Navy
- **Use of AI and ML**
- **Closing Remarks**

USES OF AI AND ML

- AI can
  - Analyse vast amounts of data, identify patterns, make predictions in real-time.
  - Ensures sophisticated cyber threats are countered.
    - Hence, no study considered complete without discussing AI & ML.

- While considered a potent tool, to implement, **challenges** exist.

CHALLENGES IN USE OF AI AND ML

- ***Data Quality & Bias***: AI/ML rely on quality of training data
  - Clean data is essential for improved results.
- ***Explainability & Trust***: Understanding decision process of AI/ML important to build trust & ensuring accountability.
  - ‘Black box’ models can be a challenge.
- ***Adversarial AI***: Attackers can evade detection by using AI.
  - Continuous research is essential to maintain the edge.
- ***Integration with Existing Systems***: Integrating AI/ML security solutions with existing IT & OT infrastructure complex
  - Requires careful planning.

AI AND ML IN DATA SECURITY (1/2)

- Enhanced Threat Detection and Anomaly Detection
  - By analysing network traffic in real-time & identifying anomalies & deviations.
- Proactive Vulnerability Management
  - Can assess risk associated with user access attempts
- Intelligent Access Control and Authorization
  - Can assess risk associated with user access attempts
- Automated Incident Response and Remediation
  - Can automatically identify and isolate infected devices

AI AND ML IN DATA SECURITY (2/2)

- Enhanced Cyber security in Autonomous Systems
  - Monitor vessel behaviour, detect deviations & possible cyber attack

- Deception Technology and Cyber Threat Intelligence
  - Create realistic & dynamic deception environment to analyse attackers

- Specific Benefits for the Naval Domain
  - Countering Sophisticated EW and Cyber-attacks
  - Securing Distributed and Mobile Assets
  - Protecting Critical Operational Technology (OT) Systems
  - Insider Threat Detection in High-Security Environments

SCHEME OF PRESENTATION

- Introduction
- Use Areas of 5G in the Navy
- Commercial Vs Military 5G
- Challenges to address Data Security
  - In general
  - Naval Environment
- Ensuring Data Security
  - Design
  - Operation
  - Maintenance
- Efforts of the Indian Navy
- Use of AI and ML
- **Closing Remarks**

CLOSING REMARKS (1/3)

- Increasing sensors have exponentially increased data collected.
- For data to be useful, needs to be analysed & acted upon on near-real-time basis.
  - Demands higher data transfer rate which can be provided by 5G.
- With 5G - Drones & EW can create an “Anti Access/Anti Denial (A2/AD) perimeter.
- 5G development - currently commercial & needs hardening for military.
- Hardening possible during design, deployment or maintenance phase.

CLOSING REMARKS (2/3)

BENEFITS OF 5G OVER TRADITIONAL UHF

Features	Improvements
Data Rate Improvements	• Current naval UHF: 19.2 kbps maximum • Naval 5G (sub-6GHz): Up to 100 Mbps • Naval 5G (mmWave): Up to 1+ Gbps
Latency Reduction	• Current SATCOM systems: 500-600ms round-trip • Naval UHF networks: 50-100ms • Naval 5G URLLC: <1ms for critical applications • Tactical advantage: Real-time coordination of swarm drone operations, instantaneous threat data sharing
Network Capacity	• Current systems support 10-50 simultaneous users per ship • Naval 5G can support 1,000+ IoT devices and sensors per vessel • Enables comprehensive ship monitoring and autonomous damage control systems

CLOSING REMARKS (3/3)

- While new technology is imbibed, legacy systems continue.
  - Hence, suitable hand shake is needed.
- 5G not a standalone technology. A gateway for future technologies
  - Shying away from 5G will disallow easy absorption of future upgrades.
- Today commercial sector leading technological innovations
  - If military does not keep pace, procurement and sustenance of equipment would become a herculean task.
- Since 5G technology for the military is under-development and closely guarded secret
  - Innovations and advances available in open domain discussed.
- **Need of the hour** is to ensure that
  - Innovations are propelled by adequate military support & guidance

Will facilitate seamless integration with more advanced technologies like 6G when available

Thank You