Security Considerations for Design, Deployment and Maintenance of future Wireless Technology networks in the Navy

Captain (Dr) Nitin Agarwala*, Indian Navy, BTech (NA&SB), DIIT (NC), MTech (OE&NA), PhD
Commodore (Dr) R K Rana**, Veteran, PhD (IIT-M), MSc-Marine Engg (UK), BSc-Mech Engg (DU), ME†, CEng (UK), FIMarE (I), FIMarEST (UK), MASNE (USA)

*Senior Fellow, Centre for Joint Warfare Studies, New Delhi, India, nitindu@yahoo.com
**Adjunct Faculty, Indian Institute of Technology, New Delhi, India, rkrana14@gmail.com

* Corresponding author. Email id: nitindu@yahoo.com

Synopsis

The fifth-generation (5G) wireless technology which is based on the third Generation Partnership Project (3GPP) standard is expected to enable a quantum leap in the performance of wireless communication by providing higher throughput, higher capacity of connections, lower latency, higher user density, and improved capabilities and services. This thus makes 5G and their subsequent iterations, such as the 6G technology, as potent candidates for adoption in the military. However, military use of 5G and its subsequent iterations will require certain modifications to address the security concerns arising from commercially-off-the-shelf (COTS) equipment, shift from software logic to management network operations, use of open source software, and use of edge computing to realise latency reduction. This requires a need to address these security issues to ensure safety of sensitive data and availability of secure communication especially when working in a contested environment. However, such solutions are subject to cost and complexity and require the military to deploy their own networks to be effective.

It is to address these issues that the paper aims to discuss technological innovations and functional changes required to ensure security, self-provisioning, and management of the new-era wireless technology networks, such as 5G and their subsequent iterations, in the military. In doing so, the paper will look at how research work of such advanced technologies can be adopted or translated into military applications. To explain the efforts involved, endeavours of the navies across the world in general and India in particular will be discussed.

Keywords: 5G; Data Security; Navy; Military; Data Security

Author's Biography

Captain (Dr) Nitin Agarwala, a serving naval officer, has experienced various facets of a warship as a user, designer, inspector, maintainer, a policymaker, a teacher and a researcher. He has authored over 80 articles, papers, book chapters and two books. He was a Research Fellow at the National Maritime Foundation from 2017- 2019 and is presently a Senior Fellow at the Centre for Joint Warfare Studies and a Visiting Faculty at the Naval War College, Goa and the Centre for Maritime Studies at the University of Mumbai.

Commodore (Dr) R K Rana, an Indian Navy veteran with 33 years of illustrious career on board warships, dockyards, training, research, staff, design and indigenous product development organisation. He was part of the design team designing the first Indigenous Aircraft Carrier and Corvettes in the Indian Navy. A four year stint with the world's oldest and renowned Classification Society, Lloyd's Register, has provided him a global experience. He is presently, an Honorary Senior Advisor at the Foundation for Innovation and Technology Transfer of IIT Delhi, where he helps startups and faculty to connect with the Military. He is also a distinguished member of the Apex Advisory Committee (R&D) of Tehri Hydropower Development Company India Limited, India

1. Introduction

The fifth-generation (5G) wireless technology which is based on the third Generation Partnership Project (3GPP) standard is 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 and services in domains ranging from space to the battlefield edge while facilitating the seamless integration of Artificial Intelligence (AI) and Machine Learning (ML). Wireless technology has seen continuous growth since its inception in the 1970s, with a new generation typically released every 10 years as seen in **Fig. 1**. Although the maritime sector has traditionally been slow to adopt new technologies (Agarwala, 2022), disruptive innovations like 5G have been effectively utilized in the maritime sector by commercial shipping (Agarwala and Guduru, 2021), ports (Wang et al., 2022), shipbuilding (Zhao et al., 2020), and logistics (Kartakoullis et al., 2023) to name a few.

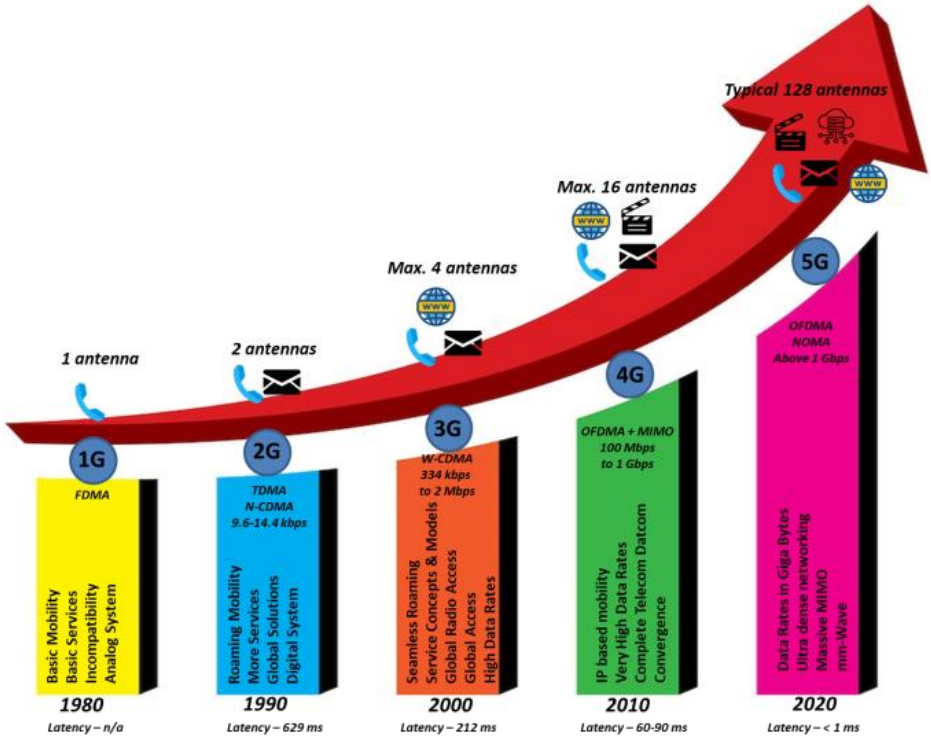

Figure 1: Evolution of wireless technology over the years (Source: Authors)

When 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, and use of dynamic radio frequency (RF) spectrum while minimizing vulnerabilities like electronic warfare (EW) jamming all of which are essentially required by the military in this age of cyber warfare. However, to address security concerns during military use, available commercially-off-the-shelf (COTS) equipment require modifications necessitated by use of open-source software, use of edge-computing for latency reduction, and shift from software logic to management network operations, among other factors. Such solutions increase cost and complexity, and require proprietary networks for effectiveness, leading to a measured pace of 5G adoption in the military globally. Since the three military domains viz. land, sea, and air have their own unique operating environment and hence concerns, it is not feasible to discuss 5G usage, application and security concerns for all the three services in a single document. Accordingly, the discussion is limited to the Navy by looking at how ships at sea can maintain their connectivity and data security when linking up at sea and using existing terrestrial networks when alongside. A significant complication for ships is the need to integrate wide range of Internet of Things (IoT) devices, sensors, Supervisory Control and Data Acquisition (SCADA) systems, Integrated Bridge Systems (IBS), Integrated Platform Management Systems (IPMS), and drones operating in all the three

domains. This complexity is further compounded by the global variations in spectrum usage (e.g. the US uses 28 GHz while the rest of the world uses 24.5 GHz) (Keller, 2025) and the differing frequencies used by LEO satellites (Starlink uses 26.5 - 40 GHz).

The paper thus aims to discuss technological innovations achieved to-date, and functional changes required to ensure security, self-provisioning, and management of 5G in navies globally. With a particular focus on India.. Accordingly, the paper begins by outlining existing challenges to data security when using 5G, followed by an analysis of efforts undertaken by navies to address these challenges. Subsequent sections will discuss the Indian Navy's efforts toward data security using existing wireless technology networks and potential future directions to meet future requirements. A general discussion will precede the conclusion for completeness

2. Use areas of 5G in the Navy

Before discussing the challenges towards data security when using 5G, it is important to discuss in brief areas where 5G can be employed in the naval domain. One realises that since the technology is still in developmental stages for use in the maritime domain, specifics of only a few applications are available. This notwithstanding, broad areas where this technology is under experimentation, pilot programme, and early deployment by navies worldwide is seen in Table 1. It is believed that continued evolution of 5G technology, and development of specialised naval applications will further expand utility of 5G in the maritime domain. The lessons learnt and infrastructure established through 5G implementation will be crucial for eventual transition and further exploitation of 6G technologies in the future.

It is important to recognize that 5G serves as a pathway to numerous other innovations. Since it can provide data transfer at 100 times the speed achieved by 4G, the response time is nearly instantaneous. With such data transfer rates marine and naval operations will be revolutionised at every level (Moseley, 2024). Currently, the International Telecommunication Union (ITU-R, 2015) has identified three main areas of use. By combining these three areas, multiple applications can be configured for use as depicted in Figure 2 (Bastos et al., 2020).

(a) Enhanced mobile broadband (eMBB) – for use of high bandwidth in AR/VR/MR/XR technologies;
(b) Ultra-reliable and low latency communications (URLLC) – for use where guaranteed connection and low latency is required especially in mission-critical applications;
(c) Massive machine type communications (mMTC) – for use when number of devices are more.

Use Area	Features / Advantages
Enhanced Shipboard Connectivity and Internal Networks	• High-Speed Data Transfer • Improved Crew Welfare • Real-time Monitoring and Diagnostics • Seamless Integration of Onboard Systems.
Smart Repair Yards and Naval Bases	• Automated Logistics and Asset Tracking • Smart Warehousing • Enhanced Security and Surveillance • Optimized Resource Management • Connected Maintenance and Repair
Augmented and Virtual Reality (AR/VR) for Training and Mission Planning	• Immersive Training Simulations • Collaborative Mission Planning • Remote Guidance and 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 and Control • High-Bandwidth Data Streaming from Autonomous Platforms • Coordinated Swarm Operations
Tactical Communications and Network Modernization	• Secure and Resilient Tactical Networks • Dynamic Spectrum Utilization • Mobile Ad-Hoc Networks (MANETs) • Integration with Satellite Communications
Cybersecurity Enhancements	• Enhanced Security Protocols • Network Slicing for Security • Real-time Threat Detection and Response
Remote health care	• Advise onboard doctors, in the event of any emergency, by specialists stationed ashore • Monitoring health of individuals in difficult environments

Table 1: Experimental, pilot programmes and early development areas for 5G technology by navies worldwide (Source: Compilation by authors from various studies)

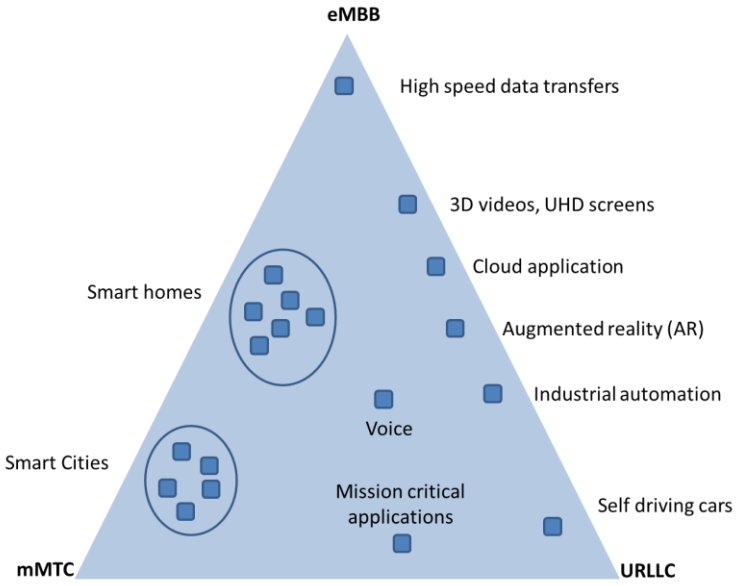

Figure 2: Main areas of 5G use (Source: Author from ITU-R, 2015)

Based on the experience gained, three different marine and naval scenarios are feasible that allow 5G to be used.

(a) *Ship-to-ship communication*. Such communication is feasible if ships are in line-of-sight (LOS). A 5G base station using an integrated access and backhaul (IAB) technology is required on each ship to maintain this communication. These base stations need to be in the sub-6-GHz (mid and low) frequency bands (gNB) which will form a meshed LOS network and provide high throughput and low latency communications.

(b) *Ship-to-shore communications*. This communication also uses a LOS communication between 5G base stations on ship and shore. The shore based base station could be public or private. This would allow complementing or even offloading need for satellite communications. When using a public 5G station, network slicing would need to be used. Communication to ship could be established directly or using other ships (called sidelink process) for multiple hops.

(c) *Ship-to-amphibious communication*. This communication is relevant during amphibious warfare and uses a sub-1-GHz 5G cell on the amphibious ship and LOS communication with mobile amphibious unit to provide high data rate connectivity. If connectivity to HQ is required, a sidelink-enabled 5G arrangement can be used.

3. Challenges towards Data Security using 5G

Like any digital infrastructure, 5G presents inherent challenges towards data security that must be thoroughly understood before the technology can be exploited effectively by the military. Before discussing these challenges it is important to clarify that data security and cyber security may sound similar but are not and should not be confused. Similarly, just because 5G has been adopted for commercial use, it does not mean that the technology is ready for use in the military. To elaborate, the differences between data security and cyber security, and the distinct requirements for commercial versus military applications, are discussed in greater detail below, prior to addressing the challenges faced by 5G in ensuring data security and those encountered by the Navy in utilizing 5G.

3.1 *Data Security versus Cyber Security*

Data security and cyber security are terms often used interchangeably, necessitating a clear understanding of their differences to address appropriate risk mitigating measures within an organization's digital domain. When looking at the differences (see Table 2), one realises that though both data security and

cyber security are closely related and often work in tandem. Cyber security is an overarching field within which the critical data security exists. To achieve cyber security, data and hence information of assets needs to be protected.

3.2 *Differences between Commercial and Military requirements for 5G*

Post-Cold War technologies have mostly been industry driven unlike those in the Cold War that were primarily driven by the requirements of the military. This shift has brought about technology to be developed keeping in mind cost and utility of the industry as the primary objective.. If a technology can also be used by the military, it is termed a dual-use technology. Such technologies require modification to ensure their components can withstand the rigorous demands of military environments and are not easily overwhelmed by adversaries during conflict, thus ensuring their availability when needed.. Given the rapid advancements in futuristic wireless technologies (5G, with 6G on the horizon) within the commercial sector, and the recognized advantages of these technologies for military applications, armed forces worldwide are working to leverage this commercial technology. However, since requirements of the commercial sector and the military are very different (see Table 3) the transition is not easy to achieve.

	Data Security	Cybersecurity
Focus	Primarily concerned with protecting data itself throughout its lifecycle – from creation and storage to processing, transmission, and destruction	A much broader discipline that encompasses the protection of all components of a computer system and network, including hardware, software, infrastructure, and the data residing on them.
Goal	To ensure the confidentiality, integrity, and availability (CIA triad) of data. This means: • Confidentiality: Preventing unauthorized access to data. • Integrity: Ensuring data is accurate, complete, and hasn't been tampered with. • Availability: Ensuring authorized users can access data when they need it	To protect against a wider range of threats in the cyber domain, including: • Unauthorized access • Data breaches • Malware attacks (viruses, worms, ransomware) • Phishing and social engineering • Denial-of-service (DoS) attacks • Insider threats • Cyber espionage • Cyber warfare
Scope	Concentrates on the controls and measures implemented to safeguard data, regardless of where it resides (e.g., databases, file systems, cloud storage, physical documents) or how it's being processed or transmitted.	Deals with the overall security posture of an organization's digital environment, including networks, devices, applications, and the human element. It involves preventing, detecting, and responding to cyber threats
Examples	• Encryption (at rest and in transit) • Access controls (user permissions, role-based access) • Data masking and anonymization • Data loss prevention (DLP) tools • Data backup and recovery procedures • Data classification and labeling • Data retention and disposal policies • Integrity checks and hashing	In addition to data security measures • Firewalls and intrusion detection/prevention systems (IDPS) • 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

Table 2: Data Security Vs Cyber Security (Source: Compilation by authors from various studies)

Feature / Aspect	Commercial Standards / Adoption	Military Standards / Adoption
Primary Objectives	Economic growth, user experience, enabling new consumer/business services, increasing revenue.	Operational effectiveness, security, resilience, enhancing warfighting capabilities.
Performance Requirements	High peak data rates, good average throughput, low latency for mass users, broad coverage.	High reliability, resilience, guaranteed QoS for critical applications, performance under extreme conditions, LPI/LPD, robustness against interference/jamming.
Security Requirements	User data protection, fraud prevention, network integrity (industry best practices, regulations).	Highly stringent; resistance to advanced cyberattacks (state-sponsored, APTs), secure authentication/authorization, end-to-end encryption, supply chain security, TEMPEST compliance.
Standardization Processes	Primarily driven by international bodies (3GPP) with industry influence, focused on global interoperability and economies of scale.	Often involves specific military standards or modifications of commercial standards, driven by national/multinational defense agencies (e.g., DoD, NATO), prioritizing security and operational needs over commercial interoperability.
Deployment Environments	Terrestrial infrastructure (urban, suburban, rural areas).	Diverse: Shipboard, airborne, tactical ground, potentially underwater; requiring ruggedized equipment and adaptable networks.
Spectrum Usage	Relies on licensed spectrum allocated by regulators, increasing interest in unlicensed/shared spectrum.	Dedicated spectrum allocations for defense, but also requires spectrum sharing and coexistence with commercial and allied systems.
Timelines for Adoption	Driven by market demand and technological advancements, typically leading to relatively rapid and widespread rollouts.	Longer due to complex requirements, rigorous testing/evaluation, and emphasis on secure, reliable solutions; security often prioritized over speed of adoption.
Focus for 6G	Enabling immersive experiences (holographic communication), ubiquitous AI/IoT, new economic models.	Enhanced multi-domain operations, ultra-reliable/low-latency for autonomous systems, secure high-bandwidth data transfer, military ISAC applications, quantum-resistant security.

Table 3: Varying 5G requirements of Commercial and Military sectors (Source: Compilation by authors from various studies)

3.3 *Challenges faced by 5G in ensuring data security*

A 5G network due to its architecture for cloud computing, volume of connected devices and reliance on new technologies like software-defined networks (SDN), network slicing, etc. provides a greater attack surface and hence exposed to greater cyber threats (Humayun et al., 2021). Being commercially developed, they need advanced data protection and encryption when used for military applications. The recently developed 5G standard called New Radio (NR) or IMT-2020 is a civilian standard that cannot be used directly in the military for fear of jamming and intentional interference disallowing transmission of sensitive information and not being available when required due to possible jamming. Furthermore, even while the 3GPP defined 5G network uses authentication, encryption, integration protection, access control and firewalls for security, it is susceptible to fake and rouge base stations (Michaelides et al., 2025) or IMSI (International Mobile Subscriber Identity) catcher. However, the advantages offered by 5G have forced use of these civilian standards by the military with parallel studies being done by various organisations [The European Defence Agency (EDA), NATO Communications and Information Agency (NCIA), Allied Command Transformation (ACT), and NATO Science and Technology Organization (STO)] with the research task group on '5G Technologies Application to NATO Operations' working dedicatedly on developing military specific standards for 5G (Zmysłowski et al., 2023).

While demand for military standards and military specific equipment is considered justified from the users point of view, the same cannot be manufactured due to limited demand and expense involved in developing military grade specific equipment when compared to commercial equipment (Heckmann, 2024).

Though implementation of a 5G network in the military looks simple, it has its own challenges some of which may not cause harm but can lead to performance degradation if left unattended. These threats include:

(a) *Trust Infrastructure*. 5G architecture uses a Public Key Infrastructure (PKI) system to establish identity. The private key is known only to the system and the public key is distributed to users. If a key is compromised it can be reissued only by changing the user SIM. However, with high number of users in 5G space, doing this may not be feasible. This makes the system vulnerable to spoofing and message alterative (messages that have been modified) resulting in loss of integrity of data. At times when the system is unable to authenticate the key, it may deny services and hence unavailability of system.

(b) *Interconnection of Devices*. IoT systems introduced in the 5G space are vulnerable to eavesdropping, potential denial of service (DoS) attacks, and data collection devices. Sometimes the IoT device may not be fully tested thereby disallowing manufacturer to provide security updates. This makes these systems and associated people vulnerable to cyber-attacks and hence loss of confidentiality and integrity of data.

Since military specifications need to be met so that reliability and effective use in the battlefield can be ensured, one can resort to use of military proven components that are considered 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). Likewise by using millimetre-wave (mmWave), device-to-device (D2D), integrated access and backhaul (IAB) and beamforming, reduction of radio emissions and covertness can be achieved.

3.4 *Challenges in the Naval Environment*

The challenges discussed so far were generic to 5G technology when employed for the military. If one were to look at the naval environment in particular one observes that there are some unique challenges that need to be proactively addressed during design, deployment and maintenance phases of 5G implementation. It is only when this is done, will navies be able to build future wireless technology networks that are resilient, secure and capable of supporting critical naval operations. Some of the unique challenges faced by the navies are:

(a) *Data Security near maritime borders*: Being a wireless signal, signals from vessels operating close to border areas can easily cross national boundaries, potentially allowing unauthorised access to these wireless signals by that country.

(b) *Need for interoperability*: Since use of wireless technology would be required along with the existing legacy system, future wireless networks will need to evolve such that they are able to operate seamlessly with diverse communication technologies used across various ships of the fleet.

(c) *Mobility and Dynamic Environment*: Naval vessels operate in dynamic environments, thereby requiring robust and secure wireless connectivity that can adapt to changing conditions while being reliable.

(d) *Electromagnetic Interference*: The maritime environment can be subject to electromagnetic interference from various sources, which can affect wireless signal reliability and security which need to be addressed to ensure reliability and availability.

(e) *Supply Chain Security*: Ensuring security of the entire supply chain for network hardware and software is critical to prevent introduction of compromised components.

4. Efforts of Navies to ensure Data Security

The increasing digital transformation within navies, spurred by the advantages of futuristic wireless technologies, has significantly expanded the attack surface area. It is therefore imperative to build data security considerations early in the process of building a robust futuristic wireless technologies solution. This proactive approach will prevent unforeseen issues during the system's deployment and maintenance phases throughout its

lifecycle Security considerations during the design phase, deployment phase, and maintenance phase are summarized in Table 4, 5 and 6 respectively.

Activity	Details
Threat Modeling	Conduct thorough threat modelling to identify potential vulnerabilities and attack vectors specific to naval wireless networks. This includes considering threats from state-sponsored actors, cybercriminals, and insider threats.
Security by Design	Integrate security controls and mechanisms from the initial design phase. This proactive approach is more effective than bolting on security measures later.
Network Segmentation	Implement robust network segmentation to isolate critical systems and data. This limits the impact of a security breach by preventing lateral movement of attackers. For instance, separate networks for operational technology (OT), information technology (IT), and guest access should be established.
Encryption	Employ strong encryption protocols (e.g., WPA3-Enterprise) for all wireless communications to protect the confidentiality and integrity of data transmitted over the air. Individualized data encryption enhances security even on open networks.
Authentication and Authorization	Implement strong authentication mechanisms, such as multi-factor authentication (MFA), to verify the identity [1] of users and devices. Role-based access control (RBAC) should be used to ensure that users only have access to the resources they need to perform their duties.
Redundancy and Resilience	Design networks with redundancy and failover mechanisms to ensure continuous operation even in the event of a cyberattack or system failure. Geo-redundant hubs and multi-beam satellite capabilities can enhance resilience.
Physical Security	Consider the physical security of network infrastructure, especially in geographically dispersed naval units. Protecting network lines against man-in-the-middle attacks is complex but crucial.
Choice of Equipment	Select wireless equipment from trusted vendors with a track record of providing secure and regularly updated devices. Prioritize devices that offer timely security patches.

Table 4: Security considerations during design phase (Source: Compilation by authors from various studies)

Activity	Details
Secure Configuration	Implement secure configurations for all network devices, including access points, routers, and switches. Change default passwords immediately and disable unnecessary services and ports.
SSID Management	Avoid using easily identifiable SSIDs (Service Set Identifiers) and consider disabling SSID broadcasting to make the network less visible to casual attackers.
MAC Address Filtering	Implement MAC address filtering as an additional layer of security to restrict network access to only authorized devices. However, be aware that MAC addresses can be spoofed.
Intrusion Detection and Prevention Systems (IDPS):	Deploy IDPS to monitor network traffic for malicious activity and automatically block or prevent potential threats in real-time.
Firewall Deployment	Strategically deploy firewalls to control network traffic and prevent unauthorized access between different network segments.
Guest Network Implementation	Create a separate and isolated guest network for visitors to prevent unauthorized access to the Navy's internal network.
Security Audits and Penetration Testing	Conduct thorough security audits and penetration testing before and after deployment to identify and address any vulnerabilities.

Table 5: Security considerations during deployment phase (Source: Compilation by authors from various studies)

Activity	Details
Regular Firmware and Software Updates	Establish a rigorous process for applying firmware and software updates to all network devices and security systems promptly. These updates often include critical security patches
Password Management	Enforce strong password policies and encourage regular password changes. Consider implementing a password management system.
Security Monitoring and Analysis	Continuously monitor network traffic and security logs for suspicious activity. Employ security information and event management (SIEM) systems for centralized monitoring and analysis.
Incident Response Planning	Develop and regularly update an incident response plan to effectively handle security breaches and minimize their impact. This plan should include procedures for detection, containment, eradication, recovery, and lessons learned.
Security Awareness Training	Conduct regular security awareness training for all personnel who use the wireless network to educate them about potential threats, social engineering tactics, and best security practices.
Vulnerability Management	Implement a vulnerability management program to continuously scan for and remediate security vulnerabilities in the network infrastructure and connected devices.
Performance Monitoring	Monitor network performance to detect anomalies that could indicate a security incident or a denial-of-service (DoS) attack.
Auditing and Logging	Maintain comprehensive audit logs of network activity, user access, and security events for forensic analysis and compliance purposes.
Secure Disposal of Equipment	Establish secure procedures for the disposal of old or replaced network equipment to prevent sensitive information from falling into the wrong hands.

Table 6: Security considerations during maintenance phase (Source: Compilation by authors from various studies)

5. Initiatives by the Indian Navy in Enhancing Data Security

The Government of India has taken many initiatives in different aspects of developing 5G wireless technology and beyond at the national level from where many Indian entities are likely to benefit, including the Indian Navy (Abbas, 2021). Towards this goal, the government is focusing on the following.

(a) ***Human Resource Development*:** Creating awareness and developing human resources for 5G and 6G by establishing wireless technology laboratories in over 20 academic institutions.

(b) ***Dedicated Military Spectrum*:** Defining a spectrum exclusively for military use to ensure secure communication.

(c) ***Trusted Source Procurement*:** Implementing a 'trusted source' guideline, overseen by the National Cyber Security Coordinator, for the procurement of 5G equipment to eliminate backdoor vulnerabilities.

(d) ***Network for Spectrum (NFS):*** Establishing a secure, fibre-based backbone for defence communications. This infrastructure aims to integrate optic fibre, satellite, and network systems to enhance the overall security and resilience of military networks, including future 5G deployments.

(e) ***Indigenous 5G Infrastructure*:** Developing indigenous 5G infrastructure for defence through organizations like the Defence Research and Development Organisation (DRDO), Bharat Electronics Limited (BEL), and the Centre for Development of Telematics (C-DOT). The goal is to create a secure, encryption-protected, and electronic warfare-resilient 5G network to minimize dependency on foreign technology while bolstering cyber security (Mann, 2025).

(f) ***Advanced Security Features*:** The Indian Navy is expected to leverage advanced 5G security features such as adaptive frequency hopping, beamforming, and AI-driven intrusion detection systems to counter EW threats and cyber-attacks (Mann, 2025). These technologies will impede adversaries from intercepting or jamming communications, ensuring high resilience and operational security.

(g) ***Active Involvement in 5G Standards*:** The Indian Armed Forces, including the Indian Navy, are actively involved in evolving 5G standards, particularly concerning security and IoT. By participating in global standard-setting, the Navy ensures its unique defence requirements are addressed in the next-generation wireless ecosystem (Bedi, 2022).

(h) ***Software Defined Radios (SDRs):*** The Weapon and Electronics System Engineering Establishment (WESEE) of the Indian Navy have been deeply involved in the indigenous development and design of SDRs for naval applications (PIB, 2019; PIB, 2021). These SDRs are progressively being deployed on naval warships to enhance communication capabilities, security, and support network-centric operations, significantly contributing to India's self-reliance in critical defence technologies. Indigenous SDRs are equipped with secure, military-grade waveforms and protocols, improving information assurance and resistance to electronic warfare (Banerjee, 2023; DW Bureau, 2023).

(j) ***Defence Innovation Organisation (DIO) Initiatives*:** In an effort to encourage home-grown technology and strengthen the Indian research ecosystem at a fundamental level, numerous innovation projects have been started by the Government of India through the DIO. Accordingly, projects on wireless technologies, through Defence India Startup Challenges (DISC) under their Innovation for Defence Excellence (IDEX), have been nurtured and developed. This has led to the development of a wireless machine-to-machine communication infrastructure using 5G NR technology for Indian Navy ships. In the future, this 5G NR technology could be used for data access and analysing sensor data using AI/ML (Srinivasiah and Faheem; 2022).

(k) ***NISHAR (Network for Information SHARing):*** This is a classic case of the Indian Navy partnering with the industry to develop a tactical communication link. This link can be used between domestic and friendly foreign countries (X.com, 2023). NISHAR provides a unified Common Operating Picture (COP) equipped with powerful tools for streamlined operations, target tracking, incident reporting etc. for complete Maritime Domain Awareness. Operating over a highly secure network infrastructure, it employs AES 256 encryption and quantum keys to guarantee unparalleled data security, safeguarding sensitive information from unauthorized access.

6. Use of Artificial Intelligence and Machine Learning

In today's context, no study is considered complete without discussing the strengths of AI and ML. As previously mentioned, the volume of data being handled is exponentially increasing, and given the nature of warfare, AI and ML tools have become essential. Both these tools have demonstrated their power in numerous domains and are now poised to significantly enhance data security in emerging wireless technologies within the naval domain. Their ability to analyse vast amounts of data, identify patterns, and make predictions in real-time ensures that sophisticated cyber threats are countered while improving overall security posture. Some such areas where AI and ML can contribute have been summarised in the Table 7.

AI and ML are not merely beneficial but increasingly essential for bolstering data security in an ever evolving landscape of wireless technologies within the naval domain. Navies that strategically invest in and integrate AI/ML into their cyber security strategies will be better positioned to defend their networks and data in the future. However, it is crucial to remember that every new technology has some challenges that must be factored in to realise the true benefit of AI and ML. Some of these challenges and their possible way ahead are discussed.

(a) *Data Quality and Bias*: Since AI/ML models rely heavily on quality of training data it is essential that clean data from naval environments is used for improved results (Kartal, 2022).

(b) *Explainability and Trust*: Understanding why an AI/ML model makes a particular security decision is important for building trust and ensuring accountability. 'Black box' models can be a challenge for high-stake naval applications.

(c) *Adversarial AI*: Since attackers can develop AI-powered tools to evade detection by AI-based security systems continuous research is essential to maintain the edge.

(d) *Integration with Existing Systems*: Integrating AI/ML security solutions with existing naval IT and OT infrastructure can be complex and require careful planning.

Category of Contribution	Specific Benefits	Contribution of AI/ML
Enhanced Threat Detection and Anomaly Detection	Real-time Analysis of Network Traffic	AI/ML algorithms can analyse network traffic patterns in real-time, to identify anomalies and deviations from normal behaviour that might indicate a cyber-attack, insider threat, or malfunctioning equipment. This is far more efficient and accurate than traditional signature-based detection systems.
	Detection of Novel and Zero-Day Attacks	ML models can be trained on historical data to recognise subtle indicators of malicious activity, even for previously unknown ("zero-day") attacks that have not been codified in security signatures.
	Identification of Advanced Persistent Threats (APTs)	AI can help detect long-term, low-and-slow activities characteristic of APTs by correlating seemingly innocuous events over time.
	Behavioral Biometrics for User Authentication	AI can analyse user behaviour patterns (e.g., typing speed, mouse movements) to create biometric profiles, adding an extra layer of authentication and detecting compromised accounts.
Proactive Vulnerability Management	Automated Vulnerability Scanning and Prioritisation	AI can assist in automating vulnerability scanning processes and, more importantly, prioritise vulnerabilities based on their potential impact and exploitability within the specific naval environment.
	Predictive Vulnerability Analysis	ML models can analyse historical vulnerability data, patch information, and threat intelligence to predict potential future vulnerabilities and recommend proactive security measures.
Intelligent Access Control and Authorization	Dynamic Risk-Based Access Control	AI can continuously assess the risk associated with user access attempts based on factors like location, time of day, device posture, and user behaviour. This allows for dynamic adjustments to access privileges, granting access only when and where it is deemed safe.
	Anomaly Detection in User Access Patterns	AI can identify unusual login attempts or access patterns that deviate from a user's normal behaviour, potentially indicating a compromised account.
Automated Incident Response and Remediation	Faster Threat Containment	AI-powered systems can automatically identify and isolate infected devices or compromised network segments, significantly reducing spread of an attack.
	Automated Remediation Actions	Based on predefined security policies and learned patterns, AI can initiate automated remediation actions, such as quarantining files, blocking malicious IP addresses, or terminating suspicious processes.
	Intelligent Security Orchestration and Automation (SOAR)	AI can enhance SOAR platforms by providing intelligent insights and recommendations for incident response workflows, streamlining the process and reducing human intervention.
Enhanced Cyber security in Autonomous Systems	Anomaly Detection in Autonomous Vehicle Behavior	AI can monitor behaviour of autonomous naval vessels and drones, detecting deviations from their expected operational patterns that might indicate a cyber intrusion or manipulation.
	Adaptive Security Measures	AI can enable autonomous systems to dynamically adjust their security posture based on the perceived threat environment.
Deception Technology and Cyber Threat Intelligence	AI-Powered Deception Environments	AI can create realistic and dynamic deception environments (honeypots, decoy systems) to lure and analyse attackers, providing valuable intelligence on their tactics, techniques, and procedures (TTPs).
	Intelligent Threat Intelligence Analysis	AI can process vast amounts of cyber threat intelligence data from various sources, identifying relevant threats and providing actionable insights for proactive defence.
Specific Benefits for the Naval Domain	Countering Sophisticated EW and Cyber-attacks	AI/ML can help analyse complex EW signals and cyber intrusions, enabling faster identification of threats and development of countermeasures.
	Securing Distributed and Mobile Assets	AI driven security solutions can adapt to the dynamic nature of naval deployments, providing consistent protection for vessels and personnel operating in diverse and remote locations.
	Protecting Critical Operational Technology (OT) Systems	AI can be trained to understand specific operational patterns of naval OT systems (e.g., weapon control, navigation), enabling detection of subtle anomalies that could indicate a cyber-attack targeting these critical functions.
	Insider Threat Detection in High-Security Environments	AI can analyse user behaviour and access patterns to identify potential insider threats, which are a significant concern in the naval domain.

Table 7: Contribution of AI and ML in data security (Source: Compilation by authors from various studies)

7. Discussion

The increasing number of sensors used for information collection has led to an exponential increase in the volume of data being gathered. For this data to be relevant, it needs to be transferred, analysed and acted upon on a near-real-time basis. This demands that higher data transfer rate mechanisms are employed of which 5G is considered a possible and viable option. Furthermore, the need for agility after attacking an adversary to avoid retaliatory fire is critical in an 'anti-access, area denial' (A2/AD) regime for survival. To achieve this, fixed platforms have to quickly relocate and reorganise themselves for a fresh offensive. As a counter, using 5G, drones, and EW can be effective to create an A2/AD perimeter. This demands that 5G technology needs to be employed in the military for greater control of the battle space. However, current development of 5G is

commercial sector based and needs to be hardened to meet military requirements which have been discussed here. This hardening may be looked at during the design, deployment or maintenance phase.

One may wonder why 5G is required to be introduced for naval platforms and why the traditional UHF type of communication cannot be used in place. This is primarily because, in light of exponential increase in the data that will be required to be handled, there are quantified benefits of introducing 5G and beyond, as is brought out in Table 8. While UHF signals can travel long distances and penetrate structures relatively well, the high-band signals of 5G are best suited for dense environments and short-range, high-capacity applications. Furthermore, 5G is designed to support a heterogeneous network combining licensed and unlicensed wireless technologies, unlike traditional UHF communications which are typically confined to specific licensed bands. The 5G New Radio (5G NR) standard also introduces advanced features like massive MIMO, enabling multiple data streams to be transmitted simultaneously, which is not a standard feature in conventional UHF-based systems.

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

Table 8: Quantified benefits of 5G and beyond over traditional UHF communications in the Navy (Source: Compilation by authors from various studies)

One needs to be weary of the fact that while new technology is imbibed, many legacy systems may not be upgraded or have an equivalent. Hence, to have suitable hand shake between technologies of two eras, appropriate mechanisms will need to be developed. Since 5G is not a standalone technology but a gateway for future technologies, shying away from 5G will not help but will only disallow easy absorption of future upgrades. This becomes even more critical as today commercial sector is leading technological innovations and if the military does not keep pace with them, procurement and sustenance of onboard equipment for platforms would become a herculean task.

This said it is important to highlight that the discussion here is not entirely complete as the technology and our understanding of the strengths and weaknesses of 5G are evolving and development of hardware is hence limited and slow. Limitations such as LOS operability, use of integrated access and backhaul (IBH) technology for connectivity to shore, quantifying benefits of 5G over current UHF networks used by the military, use of different frequencies and hence limitations of connectivity when in different geographical regions, and use of AI and Ml for use in networks are some areas that remain a topic of discussion and further scholarship. What has been discussed in this paper is limited to open source information be it for the world navies or for the Indian Navy as most of the work worldwide remains in the classified domain.

8. Way Ahead

Since the end of the Cold War, technological innovations have been primarily industry driven, as shift from the military led developments during the Cold War. This shift of innovation ecosystem has forced the

military to align itself to the technology of the day. While there is no doubt that the commercial technology needs to be hardened and ruggedized before its use in the military to make them safe for conduct of military operations, a concerted effort to shortlist and understand new technologies by the military is imperative.

The need to use 5G onboard ships for operations is one such advanced technology that is being studied extensively by the military to garner benefits of high speed and low latency of data such that wartime decisions can be made faster and more accurate thereby ensuring minimum casualty during wartime. Like for most recent technological developments, the leaders in breaking ground remains to be the US and now China which is also the case for 5G technology for naval applications.

One realises that in order to ensure safety of sensitive data and availability of secure communications when working in a contested environment numerous technological innovations and functional changes have been developed and incorporated to ensure safety, self-provisioning, and management of the new-era wireless technology networks. Since the 5G technology for the military is still under-development and in most cases a closely guarded secret, a few innovations and advances that are available in the open domain both globally and in India have been discussed here.

The need of the hour is to ensure that such innovations are propelled by adequate military support and guidance of the military as they will facilitate seamless integration with more advanced technologies like 6G when they become available.

9. Conclusion

Wireless technology has undergone multiple innovations since it was first introduced for voice-only in the 1970s. From voice-only to video streaming, this technology has evolved significantly over the past 50 years. The fifth generation of this technology also called 5G has enabled real-time and high speed video and data transfers thereby facilitating developments in automation and Artificial Intelligence. As new innovations that emerge in the commercial sector are not military ready, they need to be hardened and ruggedized to ensure that they can be safely used in a conflict zone. Accordingly, advances made globally and in India in particular for their Navy have been discussed here. What remains relevant is that such advances and efforts need to be continued duly supported by the government to ensure that the military does not lag excessively behind the commercial sector in technology, thereby avoiding a situation of obsolescence of legacy equipment where upgrades would be costly and potentially jeopardise national security.

Disclaimer

Views expressed are those of the authors and do not reflect those of the Government of India or the Indian Navy.

Nomenclature

3GPP	Third Generation Partnership Project
5G	Fifth generation
6G	Sixth generation
A2/AD	Anti-access, area denial
ACT	Allied Command Transformation
AI	Artificial Intelligence
APT	Advanced Persistent Threat
AR	Augmented Reality
BEL	Bharat Electronics Limited
C-DOT	Centre for Development of Telematics
CDMA	Code-Division Multiple Access
COP	Common Operating Picture
COTS	Commercially-off-the-shelf
D2D	Device-to-device
DoS	Denial of service
DIO	Defence Innovation Organisation

DISC	Defence India Startup Challenges
DRDO	Defence Research and Development Organisation
eMBB	Enhanced mobile broadband
EDA	The European Defence Agency
EW	Electronic Warfare
FDMA	Frequency Division Multiple Access
gNB	gNodeB
IoT	Internet of Things
IAB	Integrated access and backhaul
IBS	Integrated Bridge Systems
IDEX	Innovation for Defence Excellence
IDPS	Intrusion Detection and Prevention System
IP	Internet Protocol
IPMS	Integrated Platform Management Systems
ISR	Intelligence, surveillance, and reconnaissance
IT	Information Technology
LOS	Line-of-sight
mMTC	Massive machine type communications
mmWave	millimetre-wave
MAC	Media Access Control
MEC	Multi access edge computing
MIMO	Multiple-input and multiple-output
ML	Machine Learning
MR	Mixed Reality
N-CDMA	Narrowband CDMA
NCIA	NATO Communications and Information Agency
NOMA	Non-Orthogonal Multiple Access
NISHAR	Network for Information SHARing
NR	New Radio or IMT-2020
NFS	Network for Spectrum
NFV	Network function visualisation
OFDMA	Orthogonal Frequency Division Multiple Access
OT	Operational Technology
PKI	Public Key Infrastructure
RBAC	Role-based Access control
RF	Radio frequency
SCADA	Supervisory Control and Data Acquisition
SDN	Software-defined networks
SIEM	Security Information and Event Management
SOAR	Security Orchestration and Automation
SON	Self-organising networks
SSIDs	Service Set Identifiers
STO	NATO Science and Technology Organization
TDMA	Time Division Multiple Access
TTP	Tactics, Techniques and Procedures
URLLC	Ultra-reliable and low latency communications
VR	Virtual Reality
WESEE	Weapon and Electronics System Engineering Establishment
WPA3	Wi-Fi Protected Access 3
W-CDMA	Wideband CDMA
XR	Extended Reality

References

Abbas, M., (2021, April 15), Armed forces to deploy 5G network for AI, unmanned vehicles, The Hindu, https://telecom.economictimes.indiatimes.com/news/armed-forces-to-deploy-5g-network-for-ai-unmanned-vehicles/82080734

Agarwala, N., (2022), Role of policy framework for disruptive technologies in the maritime domain, Australian Journal of Maritime & Ocean Affairs, 14:1, 1-20, https://doi.org/10.1080/18366503.2021.1904602

Agarwala, N. and Guduru, SSK, (2021), The potential of 5G in commercial shipping, Maritime Technology and Research, 3(3): 254-267, https://doi.org/10.33175/mtr.2021.248995

Bastos, L., Capela, G., and Koprulu, A., (2020), Potential of 5G technologies for military application, NATO Communications and Information Agency (NCIA), Hague, the Netherlands, Working paper NCIA/2020/NCB014792/03, Sep. 2020.

Banerjee, A., (2023, July 30), WESEE: Celebrating A Vibrant Technology legacy, Indian Aerospace and Defence Bulletin, https://www.iadb.in/2023/07/30/wesee-celebrating-a-vibrant-technological-legacy/

Bedi, NS., (2022), 5G, IoT and its relevance for the Armed forces, Monograph, CENJOWS, https://cenjows.in/wp-content/uploads/2022/02/5G_layout.pdf

DW Bureau, (2023, July 24), Indian Navy equipping warships with 'Made in India' tech, Defence Watch, https://www.defencewatch.in/defence-news/latest-defence-news/indian-navy-equipping-warships-with-made-in-india-tech

Heckmann, L., (2024, July 08), Military struggles to make inroads with 5G commercial Wireless Tech, https://www.nationaldefensemagazine.org/articles/2024/8/5/military-struggles-to-make-inroads-with-5g-commercial-wireless-tech

Humayun, M., Hamid, B., Jhanjhi, NZ., Suseendran, G., and Talib, M.N., (2021), 5G Network Security Issues, Challenges, Opportunities and Future Directions: A Survey, Journal of Physics: Conference Series, Vol. 1979, International Conference on Recent Trends in Computing (ICRTCE-2021) 20-22 May 2021, Maharashtra, India, DOI: 10.1088/1742-6596/1979/1/012037

ITU-R, (2015), Recommendation ITU-R M.2083-0: IMT vision – Framework and overall objectives of the future development of IMT for 2020 and beyond, International Telecommunication Union (ITU), Geneva, Switzerland, Rec. ITU-R M.2083-0, Sep. 2015.

Kartakoullis, A., Slamnik-Kriještorac, N., Carlan, V., Vulpe, A., Suciu, G., Iordache, M., Brenes, J., Landi, G., Trichias, K., (2023), VITAL-5G: a novel 5G-enabled platform for vertical innovations in transport and logistics, Transportation Research Procedia, 72, 4303-4310, https://doi.org/10.1016/j.trpro.2023.11.341

Kartal, E., (2022), A Comprehensive Study on Bias in Artificial Intelligence Systems: Biased or Unbiased AI, That's the Question!. International Journal of Intelligent Information Technologies (IJIIT), 18(1), 1-23. https://doi.org/10.4018/IJIIT.309582

Keller, J., (2025, January 02), 5G takes its place leading-edge military communications systems, *Military-Aerospace Electronics*, https://www.militaryaerospace.com/communications/article/55244347/5g-military-communications-opens-plethora-of-new-applications

Mann, A., (2025, February 27), The 5G Revolution: Transforming Battlefield Communications for the Indian Army, OneIndia, https://www.oneindia.com/india/the-5g-revolution-transforming-battlefield-communications-for-the-indian-army-4081891.html

Michaelides, S., Lenz, S., Vogt, T., Henze, M., (2025), Secure integration of 5G in industrial networks: State of the art, challenges and opportunities, Future Generation Computer Systems, Volume 166, 107645, https://doi.org/10.1016/j.future.2024.107645

Moseley, B., (2024, October 17), The impact of 5G on the Maritime Industry: Steering towards smarter Boats, https://seaitapp.com/the-impact-of-5g-on-the-marine-industry-steering-towards-smarter-boats/#:~:text=With%20data%20transfer%20speeds%20up,marine%20operations%20at%20every%20level

PIB, (2019, June 26), Software Defined Radios, Ministry of Defence, https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=1576037

PIB, (2021, February 08), MoD and BEL sign contract for procurement of Software Defined Radio (Tactical) worth over Rs. 1,000 crore, Ministry of Defence, https://www.pib.gov.in/PressReleasePage.aspx?PRID=1696177

Srinivasiah, R and Faheem, M (2022), Wireless Sensor Network for Enabling Private Cloud on Board Naval Ships, Conference Proceedings of INEC, https://doi.org/10.24868/10686

Wang, Y., Potter, A., Naim, M., Vafeas, A., Mavromatis, A. and Simeonidou, D., (2022), 5G Enabled Freeports: A Conceptual Framework, in *IEEE Access*, vol. 10, pp. 91871-91887, doi: 10.1109/ACCESS.2022.3201889

X.com, (2023, October 05), News IADN, https://x.com/NewsIADN/status/1709943242769490322

Zhou, J., Xu, R. and Zhu, J., (2020), Research on typical application of intelligent shipbuilding based on 5G communication technology, *2020 IEEE International Conference on Artificial Intelligence and Computer Applications (ICAICA)*, Dalian, China, 2020, pp. 230-234, doi: 10.1109/ICAICA50127.2020.9182624

Zmysłowski D., Skokowski P., Malon K., Maślanka K., Kelner J.M., (2023), Naval Use Cases of 5G Technology, TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation, Vol. 17, No. 3, pp. 595-603, doi:10.12716/1001.17.03.11