CST هيئة الاتصالات والفضاء والتقنية
Communications, Space & Technology Commission

Defence & Security Spectrum Outlook

cst.gov.sa

Content

01

Glossary

Glossary

3GPP	3rd Generation Partnership Project
BVLOS	Beyond Visual Line of Sight
FSS	Fixed-Satellite Service
GACA	General Authority of Civil Aviation of Saudi Arabia
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSO	Geostationary Orbit
HF	High Frequency
ICAO	International Civil Aviation Organization
IMT	International Mobile Telecommunications
IoT	Internet of Things
ITU	International Telecommunication Union
LEO	Low Earth Orbit (satellite)
LoRa	Long Range
MIFR	ITU Master International Frequency Register
MNO	Mobile Network Operator
MSS	Mobile Satellite Service
NB-IoT	Narrow Band-Internet of Things
NGSO	Non-Geostationary Orbit

UHF	Ultra-High Frequency
VHF	Very-High Frequency
VLOS	Visual Line of Sight
WRC-27	World Radiocommunication Conference 2027
NFR	National Frequency Registry

02

Introduction

Introduction

As part of the ongoing national efforts to enhance national security and advance digital transformation within military and security entities, this document presents CST's plans with the support and contributions of the defence and security entities, the implementation of the Defence and Security Spectrum Outlook, developed in 2025 In alignment with international standards and the International Telecommunication Union (ITU) to ensure consistency with global best practices.

Defence and security applications rely heavily on the use of spectrum, and the usage volume in the kingdom accounts for the majority of the total licenses recorded in the NFR, reflecting the critical role it plays in national defence and security. These frequencies are essential for secure communications, radar operations, navigation, and advanced weapon systems, ensuring the effectiveness and coordination of military operations.

The allocation of appropriate spectrum to defence and security users is essential to enable and/or enhance defence and security operations. In the KSA National Frequency Allocation Table, spectrum is identified for either Civil use, Government use or shared Civil and Government use.

The spectrum requirements for defence and security users are expected to increase in order to support new technologies and adapt to new techniques in spectrum management.

With the first Defence & Security Spectrum Outlook and this associated plan, the aim is to establish an approach that will enable dialogue between defence and security users and ourselves on access to specified bands for civil and governmental users to meet the needs of current and new emerging defence technologies. It is impractical to review all the frequency bands in a single exercise due to the number of bands and wide range of services involved so the Defence & Security Spectrum Outlook is based on work undertaken on a number of priority bands where there are several key development opportunities to consider, including:

- **Migration of legacy assignments.**
- **Enabling new technologies.**
- **Maximizing and enhancing the efficiency of spectrum utilization.**

In the Defence & Security Spectrum Outlook, each priority band has been analysed separately, and a number of options has been identified for its future use and any necessary further analysis. The objectives are to increase the efficiency of spectrum use, facilitate sharing where feasible and ensure both governmental and civil users have access to necessary spectrum. Additionally, considerations for improving the governance of government spectrum are provided.[1]

It is anticipated that the Defence & Security Spectrum Outlook will become a regular initiative and will aligning with the Spectrum Outlook for Commercial and Innovative use and the relevant strategies. This approach reflects internationally recognized best practices.

The following sections provide a summary of

- **Defence and security radio spectrum use cases.**
- **The governance of defence and security spectrum access.**
- **Approaches for enabling developing defence and security technologies in KSA.**
- **The defence and security spectrum priorities.**
- **Future issues and areas that may need to be monitored and addressed in future outlooks.**

[1] It is important to note that Governance refers to the processes of spectrum management (which is the combination of administrative and technical procedures necessary to ensure the efficient utilization of the radio frequency spectrum) as well as the structures and systems for direction control and accountability. It involves the policies, monitoring of their implementation, and mechanisms for decision-making and oversight, ensuring the organization operates in a legal, ethical, and effective manner, aligning with its goals and the interests of its stakeholders.

03

Defence and security technologies radio spectrum use cases

Defence and security technologies radio spectrum use cases

Defence and security systems require access to radio spectrum to enable / enhance defence and security operations or hinder the potential adversary's ability to do the same. The military use of spectrum ranges from using very low frequencies to communicate with submarines underwater to microwaves for data links to connect weapons systems (e.g., aircraft, satellites, ground forces and ships); a wide range of capabilities to determine and exploit information derived from spectrum sensing including location; and to counter an adversary's use, such as jamming.

Precision navigation

Global navigation satellite system use to provide highly accurate positional information for precision targeting information for weapons delivery

Situational awareness

Use of radars to support many operational roles including surveillance, navigation, target acquisition, tracking and meteorology

Communications

Transmitting secure and encrypted messages, orders, and reports by means of terrestrial (including maritime), aeronautical and satellite systems

Signature management

Manipulation of radio spectrum to reduce their electromagnetic signature for example by reducing radar returns, creating narrow radio beams to reduce the probability of detection or intercept, and minimising radio emissions

Signals intelligence

Interception and analysis of electronic signals and systems used by targets such as terrestrial and satellite communications networks and radars

Electronic warfare

Military activities that use radio spectrum for threat detection, suppression and neutralisation using a range of jamming techniques

C6ISR

Command, Control, Communications, Computers, Cyber-defence, Combat systems (C6), Intelligence, Surveillance and Reconnaissance (ISR) where spectrum is exploited in various forms to undertake operational tasks

04

Defence and security radio spectrum governance

Defence and security radio spectrum governance

The recent development of defence and security technologies focuses on the importance of reliable access to spectrum for defence and security services. On the other hand, radio use by civil applications is growing and there is still a need for further spectrum access to support civil radio services. National administrations have been looking at ways to enhance spectrum allocated for governmental use and are exploring potential solutions for efficient use where both civil and government stakeholders have interests.

The governance of defence and security radio spectrum has therefore become a critical issue. The following key topics will be considered in the context of governance.

Principles
of defence and security spectrum governance.

The current
adopted governance approach.

Plans
to enhance current governance methods.

4.1 Governance Principles

In determining governance principles, it is important to take account of the following.

1

Spectrum is a strategic asset and a key enabler for the range of government defence, security and policy objectives.

2

Spectrum management should promote innovation and investment alongside meeting security and operational requirements.

3

The governance should ensure efficient and optimum use and be linked to actual usage requirements[2] with appropriate users empowered to make decisions where appropriate.

4

The actual spectrum management process itself should take advantage of innovation to ensure efficient spectrum management as well as supporting innovation in the applications which use spectrum.

In this context, the governance structure should follow the principles of:

1

Ensuring continuing availability for existing, developing and new uses which deliver improved, innovative and new defence and security capabilities.

2

Prioritizing spectrum efficiency while recognizing the specific defence and security requirements and constraints to protect operational integrity.

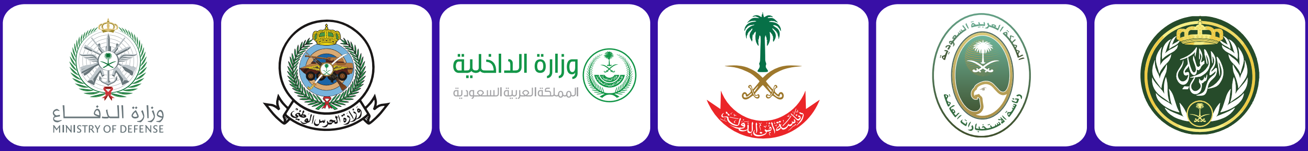
3

Maintaining a continuing focus on identifying and making available spectrum no longer required for specific defence or security requirements to enable opportunities for other services.

[2] Note that actual use is not confined to active emissions.

4.2 Current governance approach

Key stakeholders of defence and security spectrum in KSA are.



The National Spectrum Coordination Committee (NSCC) for Frequency Spectrum, chaired by CST, is the main body where representatives from defence and security entities alongside other key national users of the frequency spectrum are involved. This committee is established to strengthen national coordination and collaboration in the implementation of the spectrum strategy. It also supports CST in both local and international spectrum coordination efforts, with the overarching goal of ensuring the efficient and optimal use of the radio spectrum. Furthermore, the committee plays a key role in promoting the adoption of advanced and effective radio technologies to maximize the utilization of available frequencies.

The committee includes a sub-committee named 'Military and Security Frequency Management Committee' which is the key organization in the management of defence and security spectrum issues. This committee is attended by the defence and security entities listed above. It is aimed to expediting frequency licensing processes, enabling defence and security uses and developing national expertise in the field of spectrum management. The committee is also responsible for spectrum licensing, spectrum sharing considerations and coordination between different entities.

The following provides an overview of the Committee primary responsibilities.

▶ Undertake the necessary regulatory procedures to evaluate and process frequency licensing requests submitted by defence and security entities.

- Verify compliance with national spectrum policies – Ensure requested frequencies align with the national frequency allocation table, defence and security priorities, and any special restrictions.
- Coordinate with relevant entities – Consult with relevant entities to confirm operational requirements and prevent harmful interference.
- Follow up on operational deployment – Monitor actual use of the assigned frequencies to ensure spectrum efficiency.

▶ Review and assess spectrum plans and reallocation proposals for defence and security entities.

- Consider future spectrum needs – Consider long-term defence and security operational requirements and emerging technologies.
- Evaluate impact on existing services – Assess the potential for harmful interference with current users in the same or adjacent bands.
- Examine proposed spectrum usage – Analyze technical specifications, operational requirements, and justifications for the requested allocation or reallocation.

▶ Enhance the participation of defence and security entities in local and international workshops and conferences.

- Support international engagement – Foster connections with foreign counterparts, regulatory bodies, and international organizations (e.g., ITU, regional groups).

▶ Evaluate requests for frequency-sharing among defence and security entities.

- Review technical details of requests – Assess frequency bands, bandwidth requirements, emission characteristics, and proposed operational areas.
- Prepare formal agreements – Document the frequency-sharing arrangement, including technical conditions and responsibilities.

▶ Consider any other matters within the committee's tasks and responsibilities.

The 'Military and Security Frequency Management Committee' since its establishment in 2020 has streamlined the spectrum management processes for government users to a certain extent. Nevertheless, some key topics with the current governance require attention and improvement such as:

- Areas for improvement in cooperation and coordination.
- Lack of regular spectrum audits to understand spectrum utilization.
- Lack of an evidence-based approach for sharing and release opportunities.
- Improved key stakeholder engagement.

4.3 Plans to enhance current governance methods

Regarding the use of spectrum by defence and security entities in KSA, It is worth noting that there are ongoing efforts to establish Frequency Spectrum Management Offices in different governmental entities and these should help to facilitate the coordination required amongst these to achieve efficient governance of spectrum.

Following coordination with military and security entities, there may also be a requirement for a trusted third party, for example from academia with the necessary credentials to provide support to the activities undertaken by the relevant entities.

In the process of implementation, it is important to identify which entities are responsible, consulted and informed for each activity, ensuring transparency and clarity of roles.

The governance will be reviewed and monitored periodically to ensure the issues raised above are addressed. This will include the issuance of regular status reports to track progress, highlight precautionary considerations or areas for improvement, and propose corrective actions. Timely adjustments will be made where necessary to maintain alignment with the plan's objectives, and all relevant stakeholders will be kept informed to support coordinated decision-making and smooth execution.

05

Defence and Security Spectrum Priorities

Defence and Security Spectrum Priorities

During the Defence and Security Spectrum Outlook cycle covered by this plan, different approaches that could be facilitated for optimizing defence and security spectrum use will be considered, for example, spectrum sharing and refarming options that can address the needs of developing technologies. The efforts will concentrate on existing governmental use to several priority bands with a view to leveraging development opportunities including migration of legacy assignments and increasing band utilization to enable defence and security applications.

In the context of the possibility of sharing and refarming in the KSA, it is important to note the following points.

1

Current use of spectrum bands should be carefully monitored before making any decisions.

2

Spectrum fees should be considered to promote efficient spectrum use by all users.

3

Release of a spectrum band may take a considerable time in particular if it depends on decisions relating to other bands. Transition planning may need to be developed.

4

Future demand for spectrum bands should be considered in any decisions – in particular the likely developments of new security and defence solutions / applications.

5

There needs to be a well-defined approach, to identify spectrum for release (or sharing) and the necessary tools needed to evaluate potential for interference in place. An evidence-based approach should be used to determine technical protection and operational constraints.

5.1 Spectrum sharing

Spectrum sharing can enhance the efficiency of spectrum use either between governmental and civil organizations for the same service or between different services. Spectrum sharing methods can encourage innovation and expand the supply of spectrum to enable two or more radio systems to safely operate in the same frequency band[3] under given rules and conditions and this can allow multiple service providers to coexist in the same spectrum band and so provide the means to increase the spectrum supply and use the spectrum more extensively. Sharing rules should incentivize coordination and planning in both the government and civil sector.

The most appropriate sharing will depend on a number of factors including:

1. The potential for harmful interference between the different uses / services.

2. The quality of service / quality of experience required.

3. The duration of sharing.

5.1.1 Types of spectrum sharing

Spectrum sharing typically requires that the spectrum access rights among the different wireless systems involved are clearly defined. It is achieved by management of harmful interference through the application of appropriate sharing techniques to fulfil the agreed sharing criteria.

Spectrum sharing can either be on the basis of:

1. More than one service / system having equal access to the spectrum and provided the same level of protection from interference.

2. Multiple services share spectrum with different access rights. The higher tiers of services are guaranteed a higher level of protection over the lower tier(s).

In practice, spectrum sharing means making frequencies available for users:

1. At specific times.

2. In specific geographies.

3. In specific frequencies.

4. At specific power levels.

5. Under specific technical constraints.

[3] It is important to note that other techniques like MORAN (Multiple Operator Radio Access Network) which permits operators to share infrastructure at sites except the radio carriers, and MOCN (Multi Operator Core Networks), which permits two or more operators to share the same radio access network (RAN), differ from spectrum sharing as they are forms of infrastructure sharing.

5.1.2 Sharing mechanisms under consideration

The following approaches have been considered in the analysis of priority bands:

- **Frequency segmentation by service:** There may be the potential to sub-divide a frequency band such that services are allocated their own tranche of frequencies with, as necessary, a suitable guard band between the different services to avoid the potential for interference. In the case of duplex services such as fixed links and PMR, it will be necessary to segment the band such there is sufficient duplex spacing between the uplink and downlink which makes the implementation of such an approach more difficult. Also fixed links will generally conform to an ITU-R channel plan which defines the duplex and channel spacings and the transmit / receive frequencies.
- **Frequency segmentation by user:** Another option may be to sub-divide the frequencies allocated for a service between governmental and civil users if there is demand from both.
- **Geographic sharing – defined transmitter locations:** In the case that the transmitter locations of a service can be clearly defined, such as individual fixed link transmitters, there is the potential to define a coordination and / or exclusion zone around the site within which another service cannot be deployed. This is an easily implemented sharing approach but not suitable if there is a significant number of transmitter locations as deployment of the other services may be limited.
- **Geographic sharing – area coverage:** There may be limited opportunities for geographic sharing where a service is deployed in well-defined limited geographic area.
- **Dynamic sharing:** The use of databases to enable sharing between different users and different services is already being introduced in some frequency bands and could potentially facilitate sharing. The use of sensing technologies such as listening before talking in WLAN technology and frequency hopping in radar systems can also facilitate dynamic sharing. The implementation of such sharing requires accurate and up to date licensing data and the development of agreed sharing criteria and analysis approach.

The National Telecommunications and Information Administration (NTIA), in coordination with the Federal Communications Commission (FCC) and the Federal agencies, established a Spectrum Sharing Innovation Testbed pilot program to examine the feasibility of increased sharing between federal and non-federal users. This pilot program is an opportunity for the federal agencies to work cooperatively with industry, researchers, and academia to objectively examine new technologies that can improve management of radio frequencies.[4] There have also been other initiatives such as Nokia and Hill Air Force Base partnership in a Dynamic Spectrum Sharing (DSS) testbed in Dallas to mitigate radar interference with 5G networks.[5] There are similar initiatives in Europe including a joint initiative between the European Commission and CEPT.[6] It is expected that the outcome of these testbeds will inform the viability of different dynamic sharing options.

[4] Spectrum Sharing Innovation Test-Bed | National Telecommunications and Information Administration (ntia.gov)

[5] Nokia partners with Hill Air Force Base on testbed for radar interference management with Open RAN architecture | Nokia

[6] Microsoft PowerPoint - EuCNC21_EU testbeds for Spectrum Sharing (cept.org)

5.2 Spectrum refarming

Government spectrum may, over time, be considered for reallocation to support other applications. The methodology for evaluating this potential aligns closely with the approach used for assessing spectrum sharing opportunities. To facilitate informed decision-making regarding the possible release of spectrum, it is important to ensure clarity in the following aspects:

1 Current demand for access to specific frequency bands.

2 Potential future demand for access to specific frequency bands.

3 Availability of alternative spectrum to meet the governmental use requirements.

4 Harmonized frequency bands and equipment availability.

5 Assessment of potential for services to share spectrum.

6 Frequency bands and approaches adopted in other countries.

7 Identification of critical spectrum requirements which are key to supporting the defence and security core tasks.

Possible approaches for refarming include the following.

- **Migration undertaken by incumbent:** The incumbent may decide to migrate to a new more efficient technology and as a result release some spectrum for other uses and users. The use of spectrum fees may act as an incentive to release spectrum.
- **Migration at end of equipment life:** This is possibly the simplest approach, but governmental equipment can have long life cycles (in excess of 15 years) so it is not suitable for newer equipment.
- **Planned migration:** In this approach, the user will need to migrate from their spectrum by a defined date that will be set based on a transition plan. The transition plan will need to take into account where the existing use will be migrated (for example the new frequency band), the availability of any new equipment and any other constraints such as other users needing to be migrated first or agreements needed on how to implement spectrum sharing. It may also be necessary to put in place a payment scheme to recompense the incumbent for the costs of migration – the process for deciding who should contribute the costs and determining what they should be will need to be made clear for all involved parties.

Proposed targets for release of spectrum need to be realistic and based on the feasibility analysis of the different bands. It is difficult to compare targets between countries as the spectrum access approach differs (for example, who manages spectrum, how sharing is managed) as well as the spectrum allocations and uses between ITU Regions 1, 2 and 3.

5.3 Priority bands for increasing spectrum utilization

Several bands have been identified as important for further analysis in the context of sharing and refarming opportunities. These are in different parts of the radio spectrum including UHF, S-band and X-band. Key issues associated with these bands include:

1. Spectrum congestion.
2. Coexistence with high demand applications.
3. Increasing band utilization where a limited number of assignments exist.
4. Extending band use, for example from civil only to civil and government use.
5. Exploring potential for improved governance.
6. Migrating legacy use to ensure compliance with the KSA NFAT allocations.
7. Developing technology deployment.

The Defence and Security Spectrum Outlook considers sharing and refarming opportunities associated with priority bands as well as potential for deployment of developing technologies.

06

Developing Defence Technologies

Developing Defence Technologies

There are several key areas of developing technologies which are driving the demand for access to more spectrum. These are:

- The use of IMT technologies in defence and security applications.
- Progress in unmanned systems.
- Increasing satellite use in defence and security use cases.
- Rapidly evolving sensor technologies.
- Improvements in defence and security radar applications.

These technologies have the potential for widespread deployment in land, sea, air and space operational environments as shown in the following figure.

Figure 2: Devaloping Defence and Security technologies

Unmanned systems

- Ability to enhance surveillance and intelligence gathering.
- Extend communications range and deploy weapons delivery.
- Autonomous operational capabilities.

Radars

- Support operations including surveillance, navigation, targeting.
- Enhanced performance: better antennas, lower power, wider coverage.
- Key trends: 3D & passive radars, AESA, tech integration (GPS, IMT).

IMT

- Offers wide bandwidth and low latency.
- Enhanced situational awareness through AR/VR.
- Cost effective equipment availability.
- Defined standards and specification .

Space networks

- Software defined platforms with fully reprogrammable payload.
- Constellations of small satellites in LEO for low latency communication.
- Hybrid constellations that combine benefits of different orbit types.

Sensors

- Collecting critical data for awareness and support decisions.
- Base security and equipment maintenance.
- Defense inventory and fleet management
- Health surveillance with sensors in military uniforms.

6.1 Spectrum for Developing Defence Technologies

Spectrum requirements associated with the implementation of each technology will be determined by several factors including.

1

The demand/need of key stakeholders.

2

Availability of targeted frequency bands.

3

Impact on incumbent use in targeted frequency bands.

4

Cost and availability of equipment.

The following sections address these in more detail.

6.1.1 Unmanned systems

Unmanned systems use the radio spectrum for:

Command and control
remotely controlling the unmanned system.

Payload and data links
gathering data through sensors or radars on-board and downloading payload data to the ground.

These uses can be combined to provide additional features such as tracking, navigation and additional resilience. In the case of unmanned aeronautical systems, there is commonality with conventional aeronautical systems to support interoperability and integration into air traffic management. However, actual use is determined in relation to role and size.

Unmanned defence systems make use of a range of bands from HF to satellite Ku- and Ka-bands under licensed and/or license-exempt authorization regimes. Primarily uses are within mobile and satellite service allocations. Any interference concerns associated with deployment in any of potential bands should be addressed on an ad-hoc basis by considering band-specific technical and regulatory requirements.

International developments

Aeronautical unmanned system applications have grown significantly in recent years. This has resulted in several bands targeted for command-and-control links. For example, ITU-R identified 5030 – 5091 MHz frequency band for unmanned aircraft command and control. National regulators are developing appropriate frameworks for the use of this band. In the US, there are proposed band plans, spectrum access methods (based on dynamic frequency management system administrator) and licensing rules.[7]

In addition, there are international obligations to be met in terms of compatibility and interoperability as set out by ICAO. The complexity of issues and disparate civil, military and security requirements across air, land and maritime surface and sub-surface environments have a significant impact on spectrum. As a result, there is a need for a coordinated strategy with supporting policy and regulation to satisfy national infrastructure requirements.

Current situation

There is continuing development in the unmanned defence sector and spectrum requirements are in the process of gradually attaining readiness in line with operational requirements. There is a regulatory and operational overlap between civil, military and security requirements with shared spectrum implications from a command-and-control perspective.

▶ **Key considerations for Command-and-Control use are:**

- Whether operating within Visual Line of Sight (VLOS) or Beyond Visual Line of Sight (BVLOS).
- Lower bands are more favorable for command-and-control links typically VHF/UHF.
- Higher bandwidth provided by UHF and above preferable for data links.
- SATCOM for extended links.
- GNSS is typically used for navigation, tracking and guidance.

▶ **Payload which is determined by the operational role and specific payload requirements such as:**

- Reconnaissance.
- Intelligence gathering including electronic intelligence.
- Logistics support.

[7] https://docs.fcc.gov/public/attachments/FCC-22-101A1.pdf

The direction

To meet the increasing demand for unmanned system defence use, the following approaches will be considered.

1

Exclusive band assignment
for example, assign geographically unconstrained beyond visual line of sight and mission critical unmanned aircraft vehicle defence and security use in an exclusive sub-band.

2

Refarming of incumbents
moving existing band users to alternative bands. Appropriate transition plans will need to be developed.

3

Reviewing the legacy assignments
assessing existing allocations to ensure they align with current operational and technical requirements and updating them where necessary to improve efficiency.

4

Dynamic spectrum sharing
encourage development of dynamic spectrum sharing between different entities operating in a band allocated for unmanned system deployments.

5

International obligations
ensure consistency with international obligations such as ICAO requirements in relation to unmanned aircraft systems in conjunction with GACA.

The governance and spectrum-sharing frameworks described in this outlook will guide the implementation of these measures, ensuring transparent decision-making, coordinated .planning, and efficient spectrum use for unmanned system deployments

6.1.2 Radars

Defence and security stakeholders deploy radars for a diverse range of applications including land, sea and air surveillance; earth imaging; and air traffic control. Radar technology advancements have led to a significantly reduced transmitted power necessary to achieve improved range and target discrimination performance resulting in better coverage, target detection and tracking capabilities. Developments in pulse form, beam forming, antenna design and receiver design have improved spectrum efficiency and potential for co-existence.

Defence and security radars operate over wide frequency range. Examples are shown below.

Figure 4: Key Defensive and Security Applications of Radar Use

HF, VHF, UHF

- Early warning
- long range over the horizon
- weather observation
- coastal

UHF, L&S Band

- Air, land and sea surveillance
- air traffic control
- long range weather
- maritime coastal

Q, V, W Bands

- Short range and high accuracy airfield surveillance
- high resolution meteorological observation
- imaging

X, Ku, Ka Bands

- Airborne and missile control
- ground tracking and surveillance
- precision landing
- ship and coastal navigation
- terrain mapping
- weather monitoring
- UAV detect-and-avoid

C Band

- Short and medium range mobile military battlefield (quick installation and high precision for weapon control)
- weather
- maritime shipborne
- airborne weather

International developments

There are several potential aspects, which are the subject of further development, likely to impact on the management of radar spectrum in the future. These include passive radars (capable of exploiting transmissions from communications and navigation systems), diverse waveforms (leading to optimization of waveforms based on mission requirements), and cognitive approaches (enabling autonomous decision making). These advancements are shaping future radar spectrum management strategies worldwide.

Current situation

Defence and security radars currently operate across a wide frequency range (see figure 4 illustrating main defence and security radar uses). However, growing demand for radar spectrum requires the establishment of procedures in terms of balancing operational requirements with efficient spectrum utilization. Emerging technologies such as passive and cognitive radars introduce new possibilities but also create additional complexity in frequency management. The challenge is to enable diverse radar systems to coexist without harmful interference while ensuring readiness for both military and civil users.

The direction

In order to facilitate an effective spectrum use of bands where radar demand is high, the following points will be considered.

1

Improved planning
increase band use by enabling more government and civil radar assignments through better planning achieved by, for example, developing appropriate sharing criteria and deploying spectrally efficient equipment that incorporate improved antennas and receivers.

2

Reviewing the legacy assignments
assessing existing allocations to determine where adjustments are required to improve spectrum efficiency and facilitate sharing.

3

Refarming of incumbents
move existing users to alternative bands. Appropriate transition plans will need to be developed.

4

Dynamic spectrum sharing
encourage for the development of efficient sharing procedures among civil and government radar use. This could involve, for example, the introduction of database based dynamic sharing primarily to address potential use by mobile and transportable radars.

The governance and spectrum-sharing frameworks described in this document will guide the implementation of these measures, ensuring transparent oversight, coordinated planning, and secure spectrum access for defence radar operations.

6.1.3 Sensors

Sensors support a wide range of functions, including.

Earth observation

License exempt operations

Data collection from unmanned systems

Spectrum sensing for more efficient use of shared bands.

Sensor deployment scenarios can impact spectrum use by indirectly increasing the demand for spectrum, for example increasing data collection and the need to distribute it over wireless links; or by mitigating the demand through enabling dynamic resource allocation.

International developments

Globally, sensors make use of a wide spectrum range, from sub-1 GHz license-exempt bands to Earth Exploration Satellite Service (EESS) bands approaching 100 GHz. Their regulation depends on application type: some require international satellite filings, while others fall under national license-exempt rules. Several terrestrial IoT technologies are in use, such as NB-IoT and LoRa, often below 6 GHz. In addition, new opportunities are being explored in higher bands such as 24 GHz for defence and security applications requiring very high data throughput. For space-based sensing, satellite bands are being complemented by growing use of Ku- and Ka-bands to handle larger payload data volumes.

Current situation

Within defence and security operations, sensors are already integrated into terrestrial IoT platforms and space-based systems. Established satellite bands are relied upon for data relay, while terrestrial deployments primarily occupy 2.4 GHz and sub-1 GHz ranges, with some trials in mmWave. However, increasing demand for high-capacity applications – such as augmented reality– is putting pressure on available spectrum. Another challenge is the need to incorporate security-specific requirements into authorization schemes for 3GPP technologies, and to adapt regulations to cover defence and security-oriented sensing missions.

The direction

The way forward will involve.

1

Regulatory requirements
strengthening coordination of spectrum assignments for sensor systems, ensuring that defence and security requirements are embedded in authorization frameworks, and preparing for the progressive adoption of higher frequency bands to serve data-intensive applications.

2

Spectrum sharing
governance and spectrum-sharing mechanisms described in this document will support these actions, providing transparent oversight and efficient allocation of spectrum resources for sensor deployments.

6.1.4 Space networks

Defence satellite networks are deployed in well-established frequency bands allocated to satellite services according to ITU RR Article 5, for example L-band for global positioning, X-band for strategic and tactical communications, Ku- and Ka-band for broadband use and Q/V-band for future systems. Developing technologies, e.g. small satellite technologies and hybrid constellations, will also make use of these bands.

International developments

Globally, two main scenarios exist for defence satellite network implementation:

Defence-developed networks incorporating new technologies
for example, the U.S. Defence Advanced Research Projects Agency's (DARPA) Blackjack program aims to develop LEO small satellite capabilities that would benefit national security users. The program provided funds to a wide range of specialists to develop capabilities related to communications, targeting, missile warning, and navigation.[8]

Use of commercial satellite network capacity with new technologies
for example, the US Defence Department's plans to add more than 100 of SpaceX's Star shield satellites to its future satellite communications architecture, satellites will be owned and controlled by the US government.[9]

[8] https://spacenews.com/parsons-to-develop-prototype-ground-operations-center-for-darpas-blackjack-satellites/

[9] Pentagon embracing SpaceX's Starshield for future military satcom - SpaceNews

For both scenarios, access to satellite spectrum is governed by international regulations established within ITU. Although Article 48 of the ITU Constitution (titled Installations for National Defence Services) recognizes the member states freedom with regard to military radio installations it also encourages them to observe statutory provisions and comply with the administrative regulatory provisions.

Current situation

Once defence and security entities aim to develop a satellite network with developing technologies, it will be targeting one of the well-established satellite bands to take advantage of economies of scale and will comply with the ITU's international regulatory provisions. The network can also be registered in the ITU MIFR database to gain international recognition and be protected from harmful interference. The coordination of frequency use by ground elements (such as user terminals and gateways) within KSA will be handled in the Military and Security Frequency Management Committee by recognizing the potential use of the target frequency bands by other civil and/or governmental radio services.

In the case of the use of commercial satellite network capacity by KSA defence and security entities, the frequency use will need to be in compliance with the authorization conditions associated with the target commercial satellite network. It is worth noting that the use of commercial systems may pose precautionary considerations if they are not as resilient to operational requirements for military systems.

The direction

Defence and Security Spectrum Outlook will seek to:

1

Secure access to suitable and sufficient satellite spectrum in established ITU-allocated bands to support current and future operational requirements.

2

Enable the development of owned satellite networks leveraging emerging technologies while complying with ITU provisions and securing ITU MIFR registration.

3

Develop regulatory provisions and security requirements for the use of commercial satellite networks to ensure operational resilience.

The governance and spectrum-sharing frameworks outlined in this document will guide decision-making, coordination, and implementation for defence and security satellite network development and use, ensuring transparency, spectrum efficiency, and alignment with both national security priorities and international obligations.

6.1.5 IMT

IMT systems are standardized systems with well-defined technical specifications. They operate in 3GPP frequency bands. Defence and security IMT developments will need to be in the harmonized 3GPP band plans to provide the necessary economies of scale for the equipment. We anticipate that there will be a need for both coverage and capacity to support the defence and security mobile broadband needs. Also, there will be a minimum bandwidth that needs to be identified depending on the applications that need to be supported.

International developments

Internationally, defence and security entities have explored different approaches to delivering IMT services. For example, during the naval exercise at the Norwegian Navy's main base in Bergen in August 2023 where Telia Norway and the Norwegian Defence Materiel Agency demonstrated how network slicing is used to create a private network for the Norwegian Armed Forces.[10] Telia has set up a new unit called Telia Tactical Networks to manage a 5G slice for the Norwegian armed forces and providing service guarantees.

Current situation

There are two options to support the provision of IMT services for defence and security.

1

Use of network slicing over commercial mobile operator networks.

2

Access to spectrum identified by 3GPP to build dedicated network(s) which could be facilitated by refarming of spectrum, trading of MNO spectrum, award of new spectrum for national coverage, or licensing for limited geographic coverage.

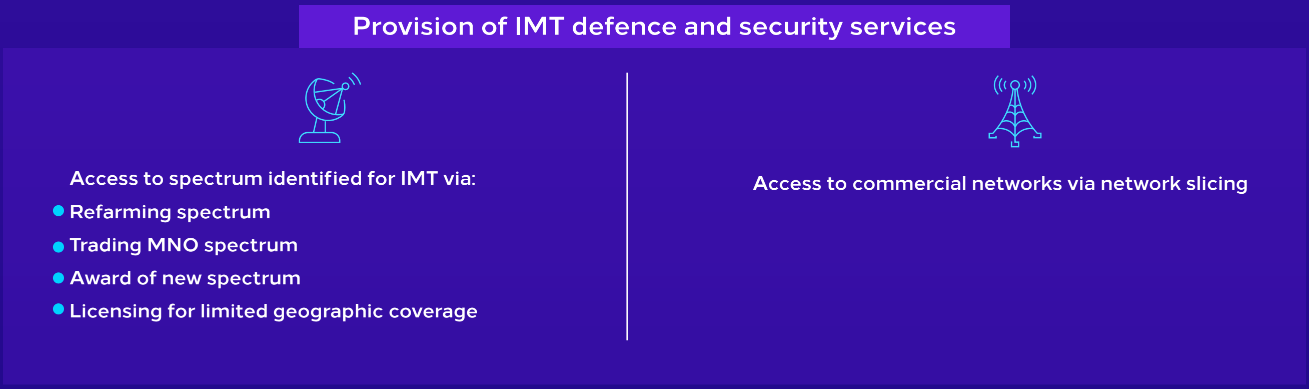
[10] https://www.teliacompany.com/en/news-articles/telia-norway-demonstrates-5g-network-slicing-for-the-norwegian-armed-forces

However, operational requirements for military and security users remain. Ensuring network security and being able to meet the quality of service and coverage needed for governmental organizations may be difficult to satisfy using commercial networks.

There might be a need for deployable technologies such as cell-on-wheels, gateway stations and air-to-ground communication. It may therefore be necessary to access sufficient and suitable spectrum (i.e. IMT bands, to meet coverage and capacity needs) to support one or more networks specifically for governmental use.

Options for the provision of IMT services are illustrated below.

Figure 3: Access Mechanisms for International Mobile Telecommunications (IMT) Services



Provision of IMT defence and security services

Access to spectrum identified for IMT via:

- Refarming spectrum
- Trading MNO spectrum
- Award of new spectrum
- Licensing for limited geographic coverage

Access to commercial networks via network slicing

The direction

To meet these needs, defence and security entities must secure access to an adequate spectrum in harmonized IMT bands, either through dedicated networks or through guaranteed, secure network slices.

The approach will emphasize in

1 **Security and performance**
ensuring both security and performance, supported by deployable solutions where necessary, to deliver reliable and mission-ready mobile broadband capabilities.

2 **Spectrum sharing**
The governance and spectrum-sharing frameworks outlined in this outlook will guide the implementation of IMT for defence and security, ensuring transparent decision-making, effective coordination, and efficient spectrum utilization throughout the deployment process.

07

Monitoring of WRC-27

Monitoring of WRC-27

There will be monitoring of WRC-27 activities relevant to Defence and Security Spectrum Outlook. An overview of relevant WRC-27 Agenda Items is provided below.

Table 1: WRC- 27 Agenda Items

Item	Technology or Service	Agenda Item
1.2	Satellite Earth stations	Technical and operational limitations to allow smaller antennas for GSO / NGSO including revised power limitations. Update 5.502 and 5.503 as necessary
1.5	Satellite FSS and MSS	Studies on development of regulatory measures, and implementability, to limit the unauthorized operations of NGSO earth stations in the FSS and MSS and associated issues related to the service area of NGSO FSS and MSS satellite systems
1.7	IMT	Access to further IMT spectrum / associated technical conditions.
1.12	Satellite MSS	Possible allocations to the mobile-satellite service and possible regulatory actions required for the future development of low-data-rate non-geostationary mobile-satellite systems
1.13	Satellite MSS	Studies on possible new allocations to the MSS for direct connectivity between space stations and IMT user equipment to complement terrestrial IMT network coverage.

CST

هيئة الاتصالات والفضاء والتقنية

Communications, Space & Technology Commission

cst.gov.sa