

5G

is a Military Gamechanger

Akkodis Group Nordics



Contents

03

Critical assignment communication is key

04

High speeds and low latency on the 5G network

05

Separate “defence area” on the 5G network

07

IoT in the military domain; IoMT

09

Infrastructure, vulnerability and frequency range

10

The military have applications in all frequency bands

11

Without 5G, we can't exploit the potential of new technologies to the full

Written by:



Mikkel Helweg

Business Development Director
at Data Respons Solutions

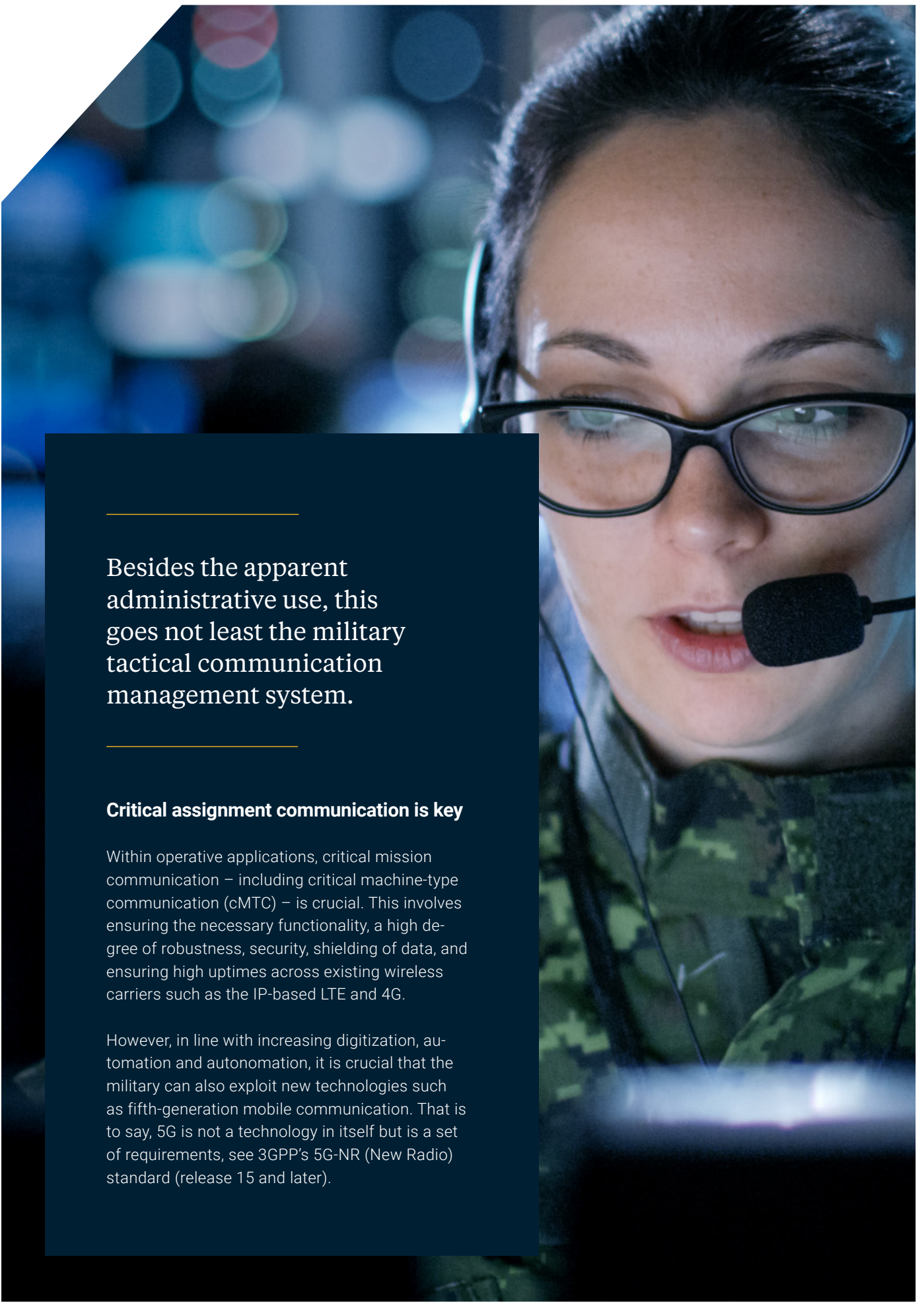
AKKODIS | data:respons
SECURITY



Terje Jensvik

CTO of Data Respons Solutions

AKKODIS | data:respons
SECURITY



Besides the apparent administrative use, this goes not least the military tactical communication management system.

Critical assignment communication is key

Within operative applications, critical mission communication – including critical machine-type communication (cMTC) – is crucial. This involves ensuring the necessary functionality, a high degree of robustness, security, shielding of data, and ensuring high uptimes across existing wireless carriers such as the IP-based LTE and 4G.

However, in line with increasing digitization, automation and autonotation, it is crucial that the military can also exploit new technologies such as fifth-generation mobile communication. That is to say, 5G is not a technology in itself but is a set of requirements, see 3GPP's 5G-NR (New Radio) standard (release 15 and later).



High speeds and low latency on the 5G network

5G's speed of 10 gigabits per second (see eMBB or Enhanced Mobile Broadband) is estimated to be 100 times faster than 4G. And the technology's theoretical delay of just a few thousandths of a second (1 ms) is 400 times faster than the blink of an eye...

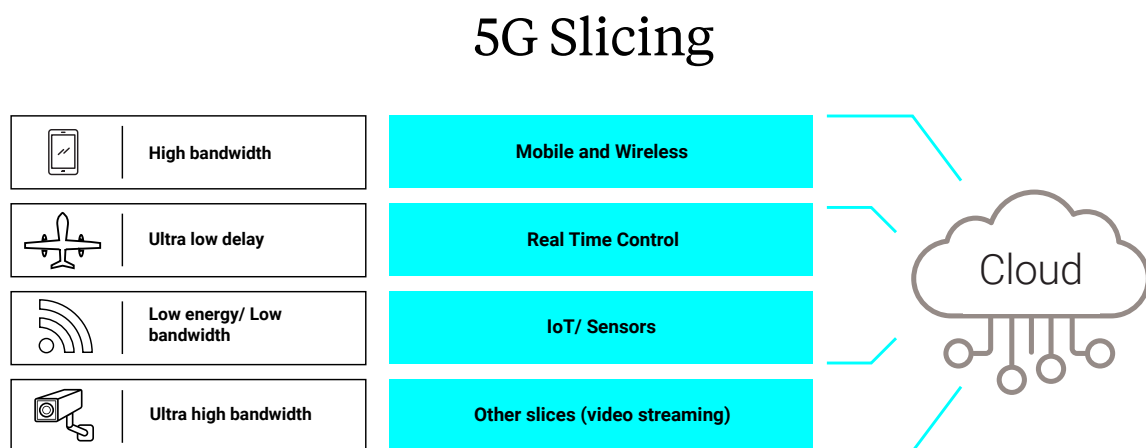
5G terminology likes to talk about URLLC (or Ultra-Reliable Low-Latency Communications) with regards to the above. The low delay is achieved among other things with the help of so-called Edge computing where data processing and data generation (systematic indicators, trends and performance data) is executed as close as possible to the endpoints, including sensors and effectors, where these can exchange data with one another locally with practically zero waiting time.

Separate defence area on the 5G network

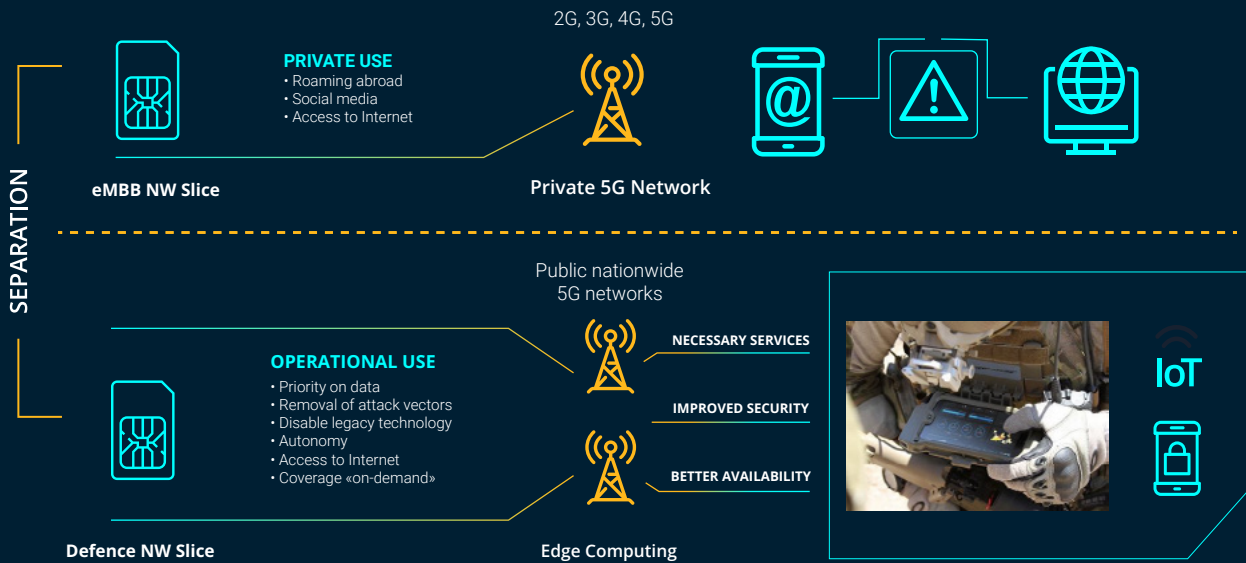
With the help of Software-Defined Networking (SDN) and Network Function Virtualization (NFV), it is possible to assign private, specially adapted user areas – so-called “network slices” – to different sectors, industries and enterprises on the 5G core network. These areas are built on top of the underlying mobile network. They are central to 5G technology since it is not possible to combine all the capacities previously mentioned without extreme investments. For example, it is impossible to combine very low delay with massive area coverage (up to 1 million units per square kilometer, ref. massive machine-type communication; mMTC). The private slices are therefore adapted based on critical parameters for each sector or enterprise, or different defence applications.

For example, a private 5G “Defence Slice” with high, prioritized speed and low latency will simplify heavy end-to-end encryption using keys that can only be read by the recipients. This is what is being tested in the 5G Vertical Innovation Infrastructure (VINNI) project which the Armed Forces are participating in.

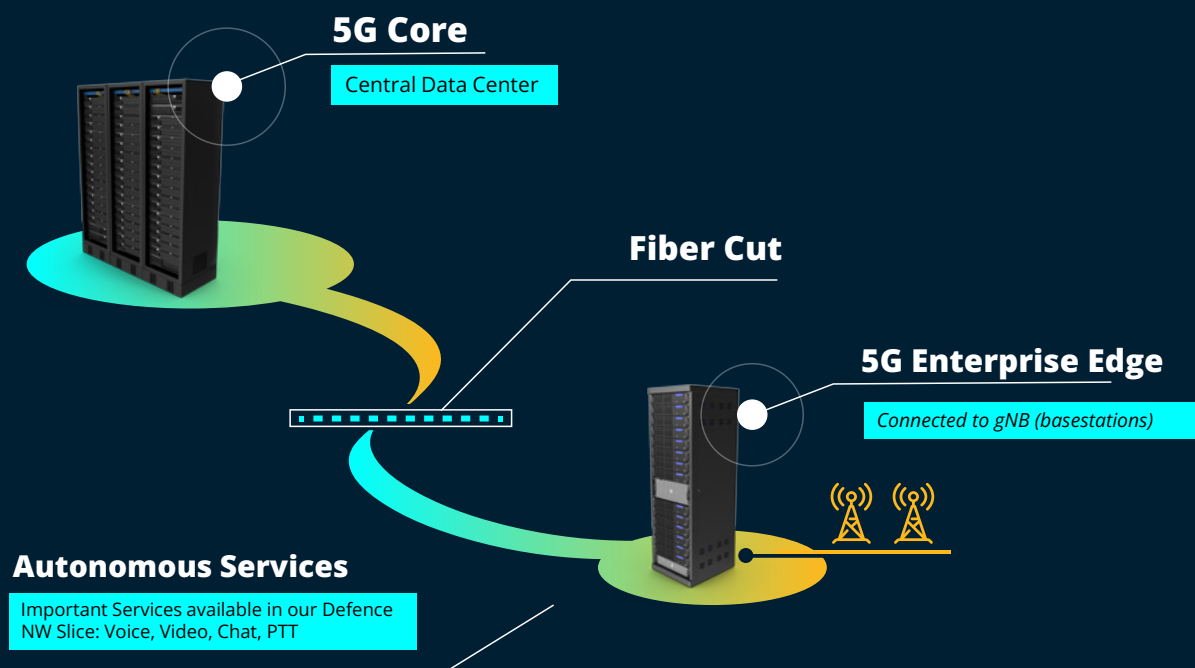
These sorts of private areas are also of interest for other key agencies in the public sector, regardless of whether these agencies are part of a national defence structure or not. It is, for example, an expectation that a dedicated 5G network slice will replace the current emergency network in Norway from 2027 (after the Norwegian government decided back in 2017 that the next generation emergency network – NGN – should be based on a commercial mobile network). This network then recognizes that the coupled unit belongs to the “emergency services slice” and prioritizes it over other network traffic and communication.



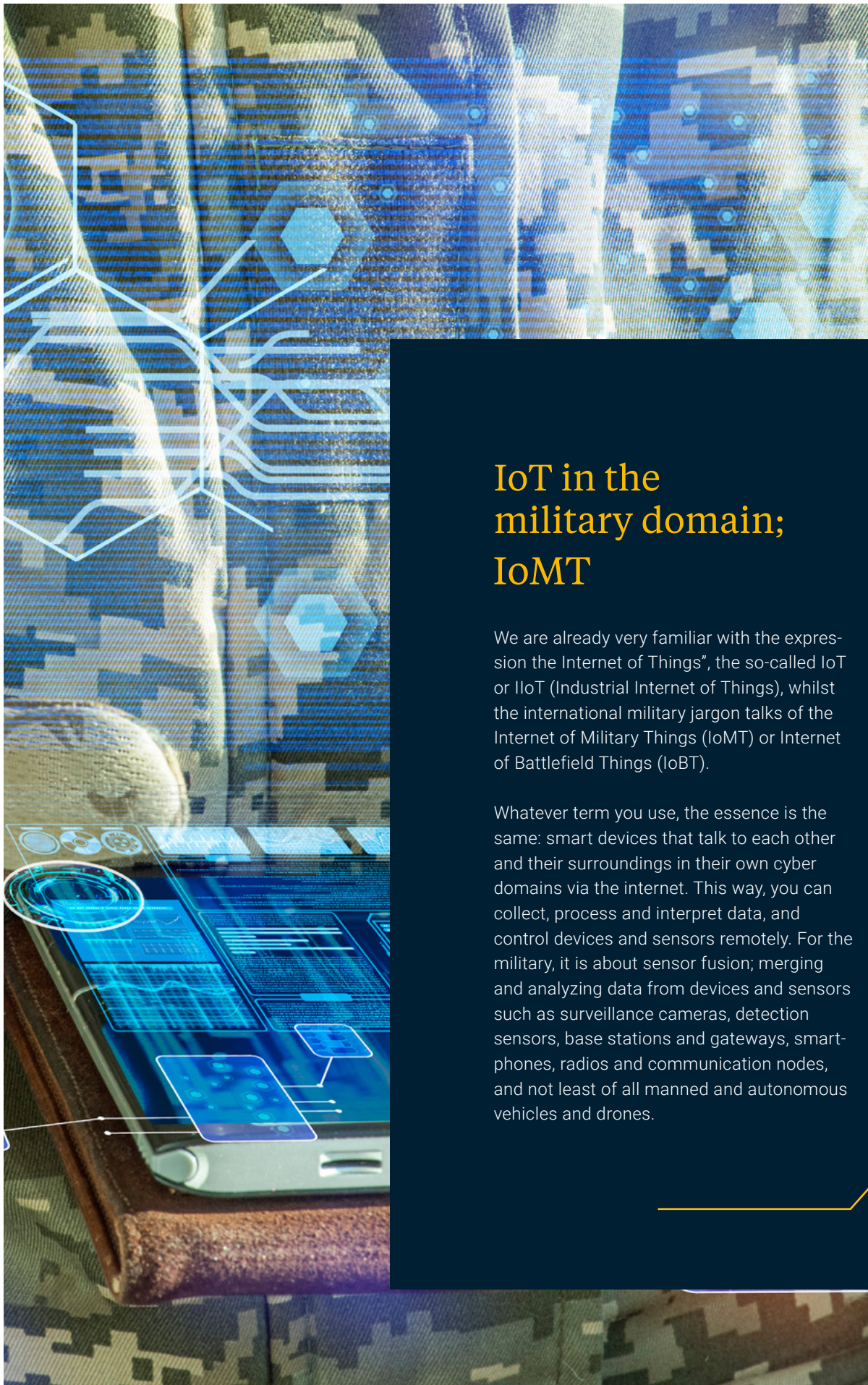
5G slicing illustration



Slicing up the 5G network



5G Autonomous Service. Edge Computing nodes in airports, hospitals, in a municipality to provide essential services when the central 5G Core is not available.



IoT in the military domain; IoMT

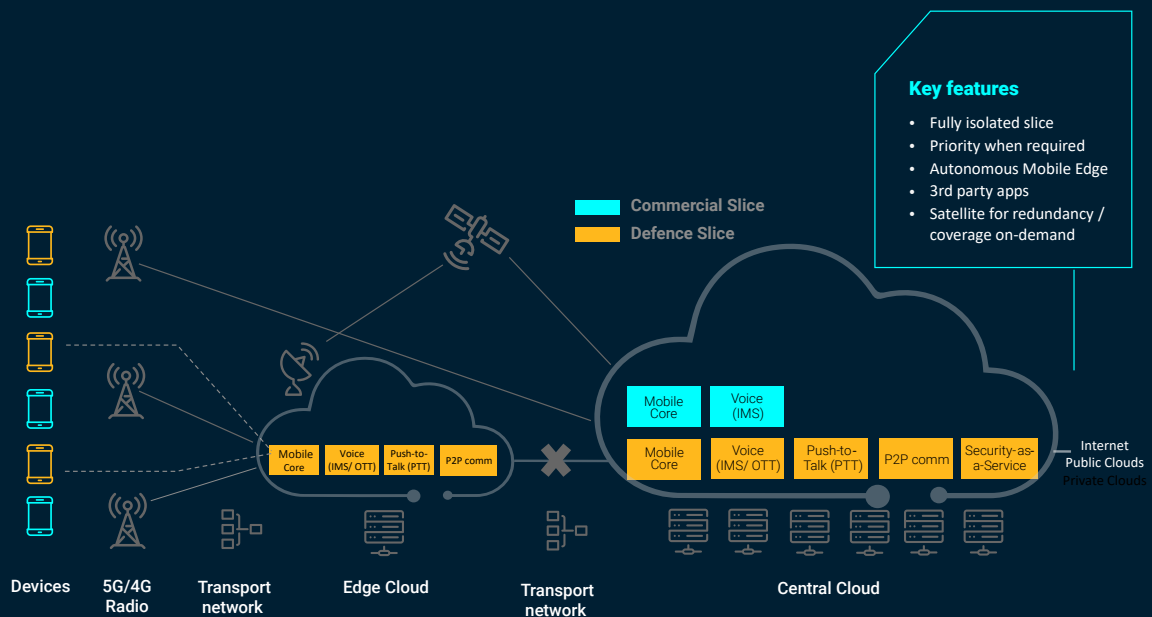
We are already very familiar with the expression the Internet of Things", the so-called IoT or IIoT (Industrial Internet of Things), whilst the international military jargon talks of the Internet of Military Things (IoMT) or Internet of Battlefield Things (IoBT).

Whatever term you use, the essence is the same: smart devices that talk to each other and their surroundings in their own cyber domains via the internet. This way, you can collect, process and interpret data, and control devices and sensors remotely. For the military, it is about sensor fusion; merging and analyzing data from devices and sensors such as surveillance cameras, detection sensors, base stations and gateways, smartphones, radios and communication nodes, and not least of all manned and autonomous vehicles and drones.

Based on this information, models and usable real-time data are generated for logistics and area control, intelligence and situational awareness, command and control, and finally active protection of combatant units and bases.

With the properties and capacities offered by 5G technology, we can take a giant leap forward and (as previously mentioned) the military can gather their IoMT together into one dedicated slice – a “defence NW slice” – with robust security algorithms and procedures, and where the properties and real-time speed of 5G technology (with performance in line with fibre optics) mean the guaranteed quality of service (QoS).

This all means that the military can get the most out of artificial intelligence (AI), virtual reality (VR) and advanced reality (AR). They can also react to emergency situations and control drones and vessels – individually or in swarms- in real-time via the mobile network.



Defence NW slice



Infrastructure, vulnerability and frequency range

Infrastructure, vulnerability and frequency range

There has also been a great deal of debate surrounding 5G and its vulnerability, not least in relation to radio equipment and key components for the 5G core network from the Chinese company Huawei. Several countries have chosen to ban Chinese technology from their critical infrastructure, the digital foundations of the nation. The largest telecommunications companies in Norway have also decided against Huawei ever since the new Norwegian Security Act came into force in 2019.

It is also about what frequency range the military will use. In Europe, there are three so-called 5G pioneer bands, two of which fall under Frequency Range 1 (<6GHz), specifically the low band (700MHz-2.3GHz) and the medium band (3.5GHz). The third falls under Frequency Range 2 and is often called the millimetre wave or high-frequency band (26GHz+).

There are opportunities and limitations, advantages and disadvantages to the different frequency bands, including with respect to the military's future use. The low band, known in Norway as the national network, is characterized by a high degree of robustness and increased area coverage. Still, it is not particularly fast compared to the other two bands. The medium band handles bigger volumes of data and is typically built up in suburban areas. The high-frequency band is characterized as being super-fast but only over short distances, meaning it requires a high cell density and extensive use of repeaters (millimetre waves suffer significant attenuation or are completely blocked by building walls and physical obstacles, and are absorbed in the atmosphere).

The military have applications in all frequency bands

No military cannot rely solely on borrowing frequencies from commercial operators, and instead must be able to establish and manage their own coverage where necessary. Military organizations also realize that frequencies within all three of the ranges are useful but for different applications. Frequencies in the low band are useful for deployable broadband solutions and tactical radio lines (outside of built-up areas where the risk of WiFi interruptions is lower).

In the medium band, the military already have existing licences for radar installations and depend on these frequencies being taken into consideration going forwards. There are also parts of this range that are of interest to the military in connection with the group and direction-defined antenna technology (MIMO/beamforming) and 5G drone detection (multi-static radar). The medium band is also widely used in the USA for radars, missile defence, electronic warfare and monitoring airspace.

However, the American Department of Defence (DoD) recently approved 3.4 and 3.5GHz frequencies for helping national technology companies to compete with China. Finally, the high-frequency band is interesting for the Armed Forces in terms of ultra-broadband card communication at bases and headquarters, for distributed sensors which require a lot of data communication, and for 5G satellite technology.

Regardless of the range, having their own dedicated and harmonized frequencies will allow the military to develop new, robust and secure technology solutions for administrative and operational applications.



Future tactical communication over the 5G network

**Without 5G,
we can't exploit
the potential of
new technologies
to the full**



There is also a debate raging internally within NATO regarding the vulnerability, infrastructure and range, but what is certain is that without 5G communication it would be close to impossible to fully exploit the possibilities offered by big data, artificial intelligence and cloud processing in both the military and other sectors. The same goes for getting the full-capacity effect out of hi-tech platforms such as the multi-role F35 aircraft in so-called multi-domain operations where situational information from Land, Sea, Air and Space is processed in a fifth domain – the cyber domain- allowing us to react by combining effectors from these domains.

The current government has stated in various forums that “the military must be the best at utilizing technology” and that this should be achieved through a high degree of independent technological competence, and cooperation between the military and governmental agencies.

In Norway the military is therefore also working on several 5G technology experiments, including experimental and pilot projects such as the 5G-VINNI project where new and secure speech and data architecture is also being integrated and tested in the “defence slice”. Many of these projects are being conducted in collaboration with commercial stakeholders and businesses, which is important since Norway is home to a highly competitive environment both within and outside of the military in the area of wireless, operational and tactical communication.

Some abbreviations we have used:

SDN: Software Defined Network. **NFV:** Network Functions Virtualisation. **LTE:** Long Term Evolution. **cMTC:** Critical Machine type communication. **mMTC:** Massive Machine type communication. **QoS:** Quality of Service. **MIMO:** Multiple Input Multiple Output.

Sources:

The only external sources used in this information was publicly available information, including reports and consultations from the Norwegian Defence Research Establishment (FFI), Norwegian Defence

Engineering a Smarter Future Together.



Contact

Sebastian Eidem

VP Operations Akkodis Nordic

E: sei@akkodis.no