AARMS Vol. 21, No. 3 (2022) 5–20.

10.32565/aarms.2022.3.1

The Use of 5G in Military Cloud of Things Solutions[1]

András TÓTH[2]

In military operations, battlefield sensor systems and various solutions supporting reconnaissance and surveillance are increasingly important. Networked battlefield and military devices deployed in the operational theatre can be the best solution to this, ensuring that they are designed to collect all the data generated in their environment, which they are programmed to acquire. These devices continuously share the information they collect with each other and with a central storage and processing server. The required interconnections are typically two-way communications with all the criteria necessary to share the collected data in the shortest possible time. The data collected and analysed in this way can contribute significantly to the near real-time monitoring of the real operational situation and environment. This capability will enable the acquisition and maintenance of information superiority and can significantly speed up decision-making processes. Therefore, networked battlefield intelligent devices are essential for achieving operational objectives and successfully executing operations. In this paper, the author examines the integration of various levels of military IoT devices into the cloud environment and the use of 5G technology as a possible future solution for developing the communication environment. To achieve the research objectives, the author performs a comparative analysis between relevant international academic publications and technical reports on the topic, based on which he formulates his research results.

Keywords: Cloud of Battlefield Things, Cloud of Military Things, military 5G, network slicing

Introduction

Digitalisation has a major impact on our everyday environment. Consequently, the European Union and its Member States have recently emphasised developing digitisation strategies and frameworks. Almost all these frameworks deal with developing smart cities, smart

[1] This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences and the ÚNKP-22-5-NKE-88 New National Excellence Program of the Ministry of Innovation and Technology.

[2] PhD, Associate Professor, University of Public Service, Signal Department, e-mail: toth.hir.andras@uni-nke.hu

environments and ecosystems. In all of these, Internet of Things (IoT) devices and systems are inevitable, and through their widespread deployment, they have a major impact on our everyday lives. IoT devices constantly monitor their environment, collect data, and share it with other elements of the system and users according to their pre-programmed tasks. Since these devices collect much information from their environment, it is of paramount importance that this information is collected in a place with a large storage capacity and a sufficiently large computing capacity if needed. A cloud environment is the best solution for this. Hence, the combination of IoT and cloud computing is called the Cloud of Things (CoT). These tools appear in the civilian environment and are also increasingly used in military operations, where they can support soldiers in tracking the operational situation in real time and help make decisions as quickly as possible. In this context, some publications have been published in the past year describing the basic requirements[3] and possible solutions[4] for using IoT devices in military environments. IoT devices used in military environments are called the Internet of Battlefield Things (IoBT) or the Internet of Military Things (IoMT), depending on the operational environment and level. If these devices are connected to the cloud environment, we can talk about Cloud of Battlefield Things (CoBT) or Cloud of Military Things (CoMT) solutions.

Research contributions

After defining the basic concepts of this paper, the author presents the theoretical possibility of linking 5G and IoT devices in military operational environments. To do so, the author seeks answers to the following research questions:

- Can 5G technology provide the right communications connectivity for cloud-based interconnection of IoT devices on the battlefield?
- Can 5G private radio networks be used in military networks?
- What are the biggest security challenges in the use of military 5G?

To answer these questions, the author has examined the characteristics of 5G technology and its applicability in military communication environments. To achieve the Cloud of Things transmission requirements, he examined the possibilities of 5G deployment.

The conceptual framework of the Cloud of Battlefield Things and the Cloud of Military Things

To understand the concepts of the Cloud of Battlefield Things and the Cloud of Military Things, it is first necessary to clarify the difference between the Internet of Battlefield

[3] Csaba Kollár: Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai. *Hadmérnök*, 12, no. 4 (2017). 146–158.

[4] Eszter Katalin Bognár: Possibilities and Security Challenges of Using IoT for Military Purposes. *Hadmérnök*, 13, no. 3 (2018). 378–390.

Things and the Internet of Military Things. The IoBT is a set of devices that use two-way communication with each other and can transmit operational battlefield data, information, and situational awareness to other devices and share it in near real-time using some technology (databases, file sharing, cloud-based systems) to support decision-making at the tactical level. In contrast, the IoMT is a higher-level solution, where information is not only available from the battlefield but also from a much more extensive set of assets. Strategic assets such as long-range unmanned aerial vehicles (UAVs), reconnaissance aircraft and satellites with various cameras are also deployed. Accordingly, the IoMT is a set of devices and systems that use two-way communication with each other, which can transmit strategic data, information and operational situational awareness generated during their operation to other devices and share it in near real-time using some technology (databases, file sharing, cloud-based systems) to support strategic decision-making.

It can be seen from the above that, as stated in the introduction, the basic purpose of IoT tools in an operational environment is to provide real operational situational awareness and support decision-making processes. Therefore, an extremely large amount of data is required, which must always be available in the right place, time and format. Cloud computing is an excellent solution for this. There is enough storage space in a cloud environment to store the large amount of data collected, and the high computing capacity helps analyse data quickly. It is the most optimal solution for connecting widely used IoT devices. In a military environment, the integration of battlefield IoT devices into a cloud environment is called the Cloud of Battlefield Things. A CoBT is a system that integrates networked battlefield assets into a common cloud environment to make the collected battlefield information available to authorised personnel at the appropriate time, place and format to provide a real-time operational situational picture. The system can thereby contribute to the acquisition of information superiority, thus helping the successful execution of operations. The strategic-level system is called the Cloud of Military Things, a system that integrates networked military devices into a common cloud environment to make the collected information available to authorised personnel at the appropriate time, place and format to provide a real-time operational situational picture at all levels of the operation. The system can thereby contribute to the acquisition of information superiority, thus helping the successful execution of operations.

The CoMT and the CoBT have a layered architecture, and the focus of this article is on the communication solutions between the layers. The conceptual structure of the layers is illustrated in Figure 1, where the first layer contains the different sensing devices (sensors, sonars, cameras, radars), the second layer is the cloud layer itself, where the storage and computing capacities are located, and the third layer is the access layer, where users access the information stored in the cloud through applications. Finally, the cloud layer contains the cloud layer of CoBT, which in the case of CoMT is the Multi-access Edge Computing solution.

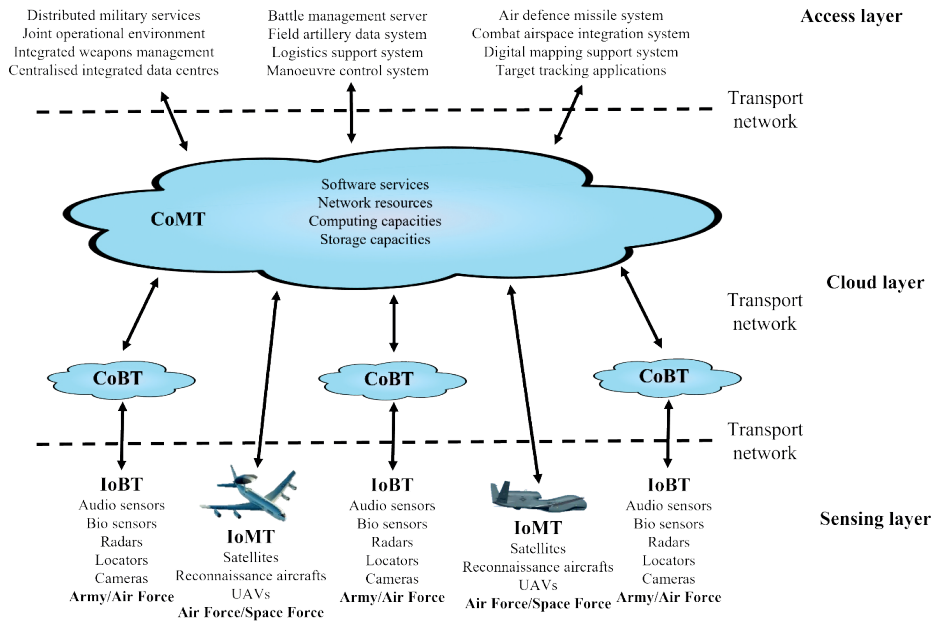

Figure 1: Layered architecture of the Cloud of Military Things

Source: Compiled by the author.

Immediate information sharing is very important in military applications, so the use of low latency systems, where the key is to process information at a nearby point, is of utmost importance. In the case of IoMT, this is made possible by the Multi-access Edge Computing (MEC) solution used in IoBT, which is an autonomous processing unit at the edge of the network. This solution is an essential element of 5G-based infrastructures such as transport infrastructure, where low latency is essential (self-driving cars, unexpected traffic information, etc.), where the data is processed directly by the radio access network (RAN) without any intervention from the central system in the MEC so that only the aggregated data is provided to the central network (in this case the CoMT).[5]

Characteristics of 5G networks

5G wireless technology aims to deliver high data speeds, reliability, availability, ultra-low latency, massive network capacity and a more consistent user experience for more users than in previous generations of technology. The performance of 5G networks should be assessed using three parameters: user bandwidth, device density and latency. The International Telecommunication Union (ITU) has set requirements for the minimum

[5] Abderrahime Filali et al.: Multi-Access Edge Computing: A Survey. *IEEE Access*, 8 (2020). 197017–197046.

values of these parameters in Recommendation ITU-R M.2083-0. This Recommendation sets out the framework and overall objectives for international mobile telecommunications (IMT) for 2020 and beyond, the framework for its future development, including a wide range of capabilities related to the intended use scenarios, and further development of existing capabilities of IMT and the development of IMT-2020. In addition, it identifies eight core areas for the capabilities, each of which has developed a target to support the development of 5G capabilities. These parameters and goals are illustrated in Table 1.

Table 1: IMT-2020 development goals

Key capabilities	**Parameters**	**Aims**
Peak data rate	Maximum data transfer rate per user/device (in Gbit/s) achievable under ideal conditions.	1 Gbit/s → 20 Gbit/s
User experienced data rate	Data rate (Mbit/s or Gbit/s) available to the mobile user/device everywhere in the coverage area.	10 Mbit/s → 100 Mbit/s
Spectrum efficiency	Average data throughput per unit of spectrum resource and per cell (bits/s/Hz).	1x → 3x
Mobility	A maximum achievable speed (in km/h) to ensure a specified QoS and seamless transmission between radio nodes, which may belong to different layers and/or radio access technologies (multilayer/RAT).	350 km/h → 500 km/h
Latency	The contribution of the radio network to the time (in ms) between the packet sent by the source and the packet received by the destination.	10 ms → 1 ms
Connection density	Total number of connected and/or accessible devices per unit area (per km^2).	10^5 → 10^6 devices/km^2
Network energy efficiency	Energy efficiency has two aspects: on the network side, energy efficiency refers to the number of bits of information transmitted to and received from users per unit of energy consumption (in bits/Joule) of the radio access network (RAN) on the device side, the energy efficiency refers to the amount of information bits per unit of energy consumption of the communication module (in bits/Joule)	1x → 100x
Area traffic capacity	Total traffic throughput served per geographical area (in $Mbps/m^2$).	0.1 $Mbps/m^2$ → 10 $Mbps/m^2$

Source: ITU-R (2020): op. cit.

The table illustrates the key objectives that the International Telecommunication Union has identified as a priority for the development of 5G. These objectives can also contribute greatly to developing communications capabilities currently used in the military environment. 5G offers several capabilities that can benefit military networks, especially tactical networks, such as manageability, dynamic spectrum management, ample bandwidth and low latency. The standards framework developed by the 3rd Generation Partnership Project[6] (3GPP) provides a good basis for this, setting out the basic requirements needed to

[6] A collaborative project of a group of telecommunications associations whose original aim is to develop globally applicable specifications for third generation (3G) mobile systems.

build 5G systems and networks. However, this development is subject to different phases, of which Release 17 was frozen in March 2022. Thus, the framework and requirements set out therein will be enforceable for all 5G networks, and devices and systems used in military environments will be able to comply with the triangle of requirements set out in ITM-2020. The adaptation of these requirements to the military environment is illustrated in Figure 2.

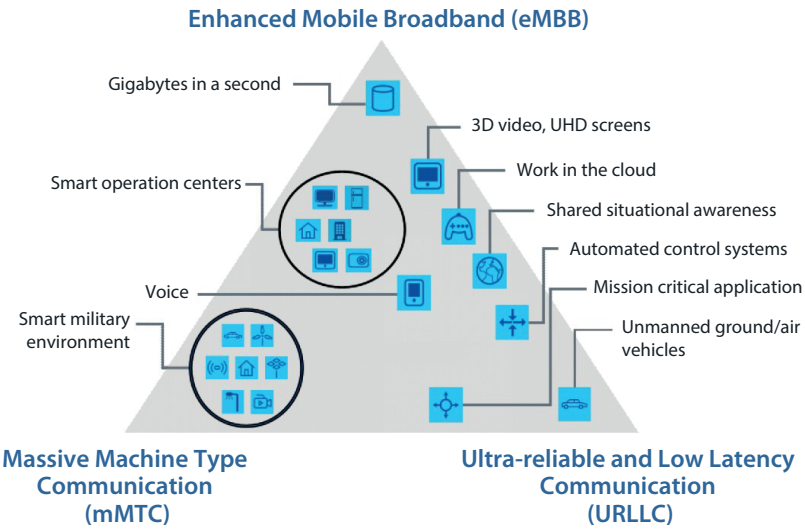

Figure 2: Triangle of requirements for the military 5G system

Source: ITU-R (2020): op. cit.

Some characteristics of the elements defined in the triangle of requirements are:

- Enhanced mobile broadband (eMBB): this typically covers people centric IMT services with high traffic bandwidth, high user density, and low to medium mobility needs. Its basic function is to provide fixed wireless access (FWA) in areas without wired access (this is essentially the case for operational areas).
- Massive machine type communications (mMTC): these communication services are targeted at Internet of Things (IoT) applications that use many connected devices with poor radio connectivity that require low throughput but high data transfer capability over time.
- Ultra-reliable and low latency communications (uRLLC): this communication service provides low throughput but also provides low latency and high availability data services for applications that do not require high throughput but need high connectivity in a mobile environment. Application examples include near real-time human–machine (or machine–machine) interfaces such as remote control or automatic/semi-automatic (weapon) control systems.[7]

[7] Luis Bastos et al.: Potential of 5G Technologies for Military Application. *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, (2021). 1–8.

These capabilities mean that 5G can handle – and interconnect – much more data than previous systems, can be used in a much wider range of applications (including a broad spectrum of military operations), and is much more complex, making security a much bigger issue than before. To achieve these, the following systems engineering objectives must be met:

- flat network architecture
- separation of the control plane and the data plane
- all functions in a self-contained unit – support for cloud computing
- optimal resource utilisation – network slicing
- high-level coordination

The use of 5G in the Cloud of Battlefield Things and the Cloud of Military Things

The architecture of 5G systems is defined by a reference model developed in 2018 for the 3GPP Release 15 framework. The 5G system architecture consists of, among others, the following network functions (NF):

- 5G Next Generation NodeB (5G gNB)
- Access and Mobility Management Function (AMF)
- Authentication Server Function (AUSF)
- Centralized Unit (CU)
- Data Network (DN)
- Distributed Unit (DU)
- Network Exposure Function (NEF)
- Network Repository Function (NRF)
- Network Slice Selection Function (NSSF)
- New Radio (NR)
- Policy Control Function (PCF)
- Radio Access Network (RAN)
- Session Management Function (SMF)
- Unified Data Management (UDM)
- User Equipment (UE)
- User Plane Function (UPF)

The relationships between the elements are defined by the following reference points in the 5G system architecture:

- N1: Reference point between the User Equipment and the Access and Mobility Management Function.
- N2: Reference point between the Radio Access Network and the Access and Mobility Management Function.
- N3: Reference point between the Radio Access Network and the User Plane Function.
- N4: Reference point between the Session Management Function and the User Plane Function.

- N6: Reference point between the User Plane Function and a Data Network.
- N9: Reference point between two User Plane Functions.[8]

The above elements are typical of 5G networks and systems, and therefore, if they are deployed in a military environment, the same elements will be present. However, what is necessary for the security of military networks is partial or complete isolation from public networks. The primary reason for this is security, but it is also important to be independent and to ensure that military networks function properly in the event of the failure of a public system element. 5G private networks and network slicing provide solutions to this. In the case of private networks, some elements may still reside on the public network (for example, the Access and Mobility Management Function), but with network slicing, the private network manages the entire data plane, so data generated and stored there cannot be leaked from the internal network. In addition, the system used must be standalone (SA). This solution will provide the above requirements, enable the full 5G capacities (eMMB, uRLLC, mMTC), and provide a significantly more flexible architecture and dynamic interconnection of network functions. In the SA configuration, the 5G network is built with dedicated equipment and network functions, 5G radios are coupled with cloud-native, service-based core network functions, and these network functions are fully virtualised and cloud-native. Figure 3 shows the conceptual architecture of an isolated military 5G network, where the standalone elements of the network are completely physically and logically separated from the public network.

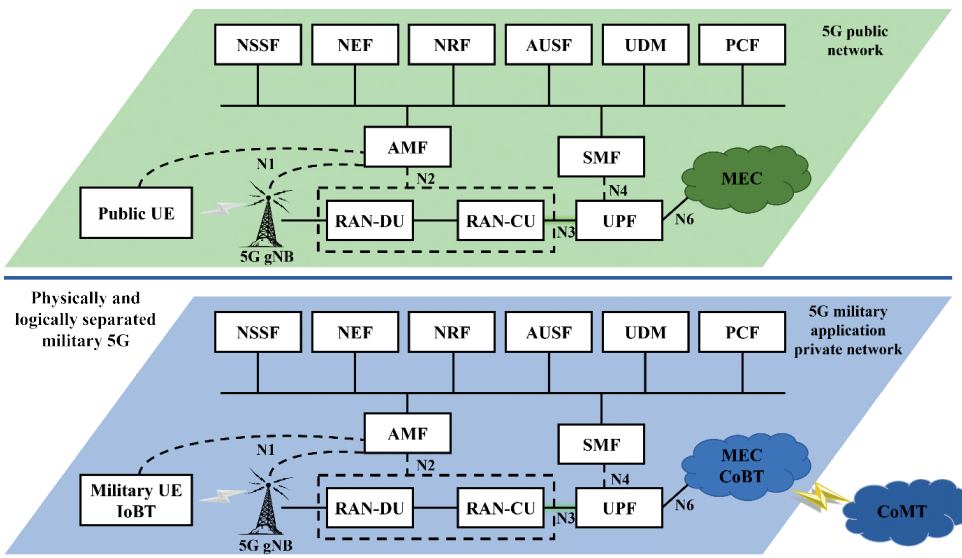

Figure 3: Triangle of requirements for the military 5G system

Source: Liao–Ou (2020): op. cit.

[8] ETSI: *5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.3.0 Release 15).* 2020.

As shown in the figure above, an independent private network has been created for the military application, where both the control plane and the user plane are isolated from the public network. Accordingly, the frequency bands used in the military environment are also different from the public one, so it can be completely independent from the service providers. This configuration guarantees absolute data security for military applications as it is completely isolated from the public network. In addition, both the core network and the wireless access network can be deployed on combat platforms, with short round-trip data transmission distances and low network latency. Finally, this solution ensures that military user devices (IoBT) can be connected to the control plane via non-terrestrial networks (NTN). Following Release 17, NTN-based eMBB and massive IoT services will be supported by NR, Narrowband-Internet of Things (NB-IoT) and LTE for Machine Type Communication (LTE-M) solutions, which provide reliable and bandwidth-adequate wireless connectivity for IoBT devices. Communication between devices can be done directly through the Access and Mobility Management Function, but typically this is done through some 5G gNB[9] node that connects IoBT elements to the user plane. Interconnections are managed by the Radio Access Network, where devices integrated into the network are connected to distributed units, which are interconnected and managed by the centralised unit. The collected data is then sent to the User Plane Function and subsequently to the Multi-access Edge Computing autonomous processing unit. All activities that support real-time monitoring of the operational situational picture, operations planning and decision-making occur here. In the resulting system, 5G, with the software-defined radios and MIMO technology used, can realise the data transmission requirements between IoBT devices and cloud technology.

Network slicing

For 5G networks, network slicing technology is available to enable the logical and physical separation of network resources to ensure the customisation, separation, and support of services and multi-tenancy on common physical network infrastructure. The technology provides a flexible way to facilitate multi-tenancy, greater network coverage, and a reliable solution for infrastructure and cloud service providers. Network slicing can be set up on an on-demand or permanent status, dedicated to a specific person or group, or to separate different services. The fundamental goal of the 5G ecosystem is to support full mobility and continuous availability in all conditions. Accordingly, it is perfectly suited for use in military environments. Therefore, the 5G technology with network slicing provides the following capabilities:

- Enhanced broadband access everywhere: providing high bandwidth access throughout the entire territory of operation, ensuring the connectivity of the end devices located in the whole area.

[9] The 5G base station uses new radio (NR) technology and is called gNodeB (gNb). The gNodeB radios have software-defined radio (SDR), such as Massive MIMO (multiple-input and multiple-output) options for higher capacity.

- High user mobility: providing broadband support for fast-moving vehicles, for example to support connectivity for military convoys on the move.
- Massive Internet of Things: supports broadband access to extremely dense networks of sensors and actuators, considering among others long-range and low-power devices.
- Extreme real-time communication: providing ultra-low latency connectivity, for example for IoBT devices.
- Extremely reliable communication: provide extremely low latency, reliable and available network connectivity to support, for example, autonomous weapon systems.
- Mission-critical communications: supports connectivity in the event of disasters and emergencies and has the flexibility to handle sudden increases in traffic while providing resilient connectivity.
- Broadcaster-like service: providing network connectivity to any service that supports, for example, the delivery of patches sent to firmware updates or fix security vulnerabilities.
- Easy communication: provides a network connection for generating, configuring, and maintaining basic service information.
- Multiple connectivity: provides network connectivity to deployed and operated smart devices using multiple access technologies.[10]

As seen above, network slicing for 5G is a solution that enables the creation of logical networks on a common infrastructure with appropriate isolation, resources and optimised topology to serve a predefined use case. In their paper,[11] the authors describe the different implementation options and ways of network slicing, based on which Figure 4 illustrates one of the possible 5G technology designs for military environments.

[10] Ibrahim Afolabi et al.: Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions. *IEEE Communications Surveys & Tutorials*, 20, no. 3 (2018). 2429–2453.

[11] Akihiro Nakao et al.: End-to-end Network Slicing for 5G Mobile Networks. *Journal of Information Processing*, 25 (2017). 153–163.

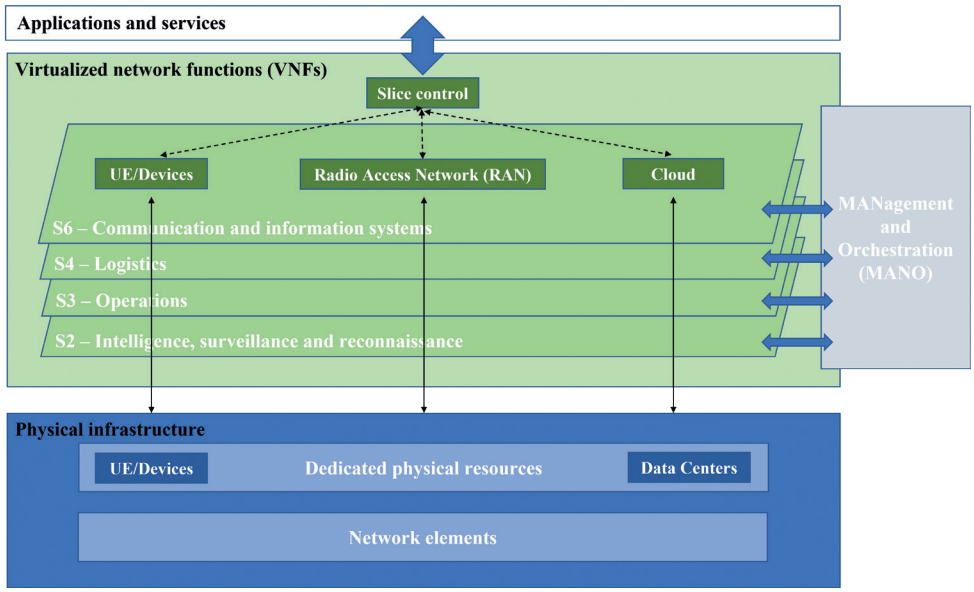

Figure 4: Network slicing in military 5G

Source: Nakao et al. (2017): op. cit.

In case of 5G systems used in military networks, separating segments and tasks can be the basis for network slicing. In this case, the different sections each use a separate virtualised network. The services running here are the virtualised network functions (VNF), which are managed and administered by the management and orchestration (MANO), which is a key component of the network functions virtualisation (NFV) architecture. The NFV is the service that enables 5G network slicing, allowing different virtual networks to run on a single physical infrastructure. In addition, it allows the partitioning of a physical network into virtual networks capable of supporting multiple radio access networks.

Satellite communication

The data processed and stored in the CoBT can also be delivered to the CoMT over 5G networks, but different communication solutions are typically used due to their large scale. 5G non-terrestrial networks extend the reach of 5G NR technology and its associated benefits to non-terrestrial platforms. The on-air 5G NR architecture will enable mobile network operators to provide 5G-based services in locations where terrestrial networks are unavailable, or longer distances need to be covered. These solutions provide the required services without any intermediate protocol or technology changes. 5G NTNs can be provided by satellites, High Altitude Platform Stations (HAPS), or any

other aircraft capable of carrying the NTN payload.[12] Focusing on the convergence of satellite and terrestrial networks, the authors[13] have presented different implementation options for satellite-terrestrial networks, such as generic, software-defined network (SDN), information-centric network (ICN), content delivery networks (CDN), based satellite-terrestrial networks. Figure 5 illustrates the conceptual possibility of 5G satellite interconnection of CoMT.

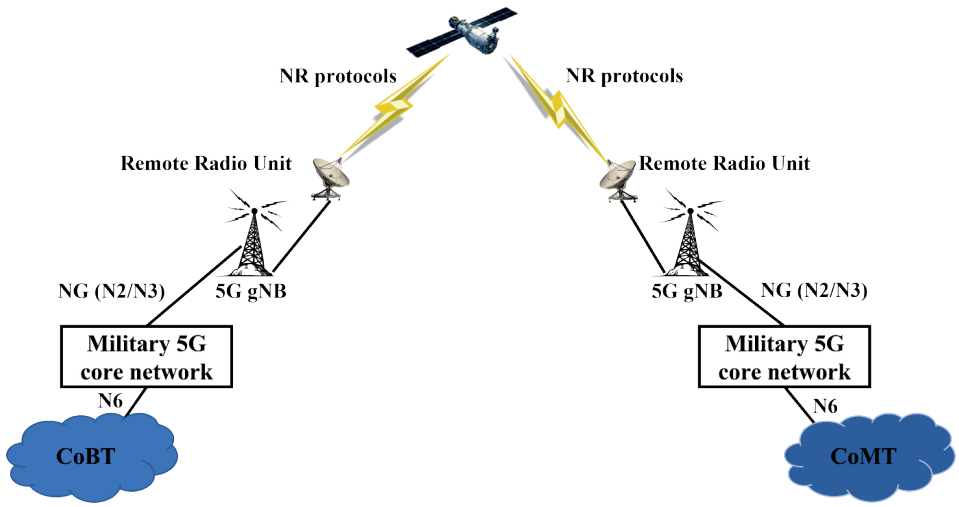

Figure 5: 3GPP military 5G satellite communication architectures

Source: Wang et al. (2020): op. cit.

5G Security issues in the Cloud of Battlefield Things and Cloud of Military Things

5G networks deployed in CoBT environments have many useful features described above but also present several security challenges. Ensuring adequate security is also a big issue for IoT devices used in military operations. From an operational safety point of view, it is of paramount importance to guarantee the safety of the equipment or systems used because if the equipment or systems used are damaged, it can seriously impact the whole operation and even endanger the lives of several soldiers. For CoBT, it is not only the user devices that are a problem, but vulnerabilities or threats can occur at all levels of the system that can have a negative impact on operations. The authors describe these risks in

[12] Bastos et al. (2021): op. cit.

[13] Peng Wang et al.: Convergence of Satellite and Terrestrial Networks: A Comprehensive Survey. *IEEE Access*, 8 (2020). 5550–5588.

their article[14] for civilian use, and the transfer of these risks to a military environment is illustrated in Table 2.

Table 2: Threats and vulnerabilities in Cloud of Battlefield Things and Cloud of Military Things

Domain	**Threats**
Military UE (IoBT)	Firmware issues Malware Botnet Device tempering Device capture
RAN	Jamming DDos Node damaging Rogue base station Man-in-the middle attack
Edge and core network	SDN, MEC platform vulnerabilities DDoS Eavesdropping Spoof attack Man-in-the middle attack 3rd party application
Service	Unidentified and unauthorised access Service hijacking Abusing cloud computing Insecure or compromising interfaces and API Data leakage and breaches Key compromise and the breakage of cryptographic protocols

Source: Kim (2020): op. cit.

To ensure adequate security, developing an information security CIA triad is a basic requirement for both CoBT and CoMT. Accordingly, the system and network developed must have the appropriate confidentiality, integrity and availability capabilities.

Confidentiality means preventing unauthorised persons from reading or accessing sensitive material. This security aspect hides information by encrypting the payload to a significant level. In the design, there should be a strong emphasis on the fact that obfuscation of information entering, leaving and passing through the CoBT and CoMT system is a critical requirement. This will prevent information from being exposed to intrusion and eavesdropping attacks.

The manipulation and destruction of data to mislead the parties involved in the communication constitute a breach of integrity. Like confidentiality, integrity is a widely discussed concept in information security. Moreover, integrity plays a key role in the context of CoBT and CoMT, as the services hosted there are typically automated, and accurate information is required for the efficient operation of autonomous services.

[14] Hwankuk Kim: 5G Core Network Security Issues and Attack Classification from Network Protocol Perspective. *Journal of Internet Services and Information Security (JISIS)*, 10 (2020). 1–15.

Availability means that CoBT and CoMT resources are available everywhere for customers who want to use the services. This factor depends primarily on network performance and the efficiency of network interfaces. Therefore, the performance of the designed network is of paramount importance for CoBT and CoMT.[15]

In addition to these, in their article[16] Sicari et al. also specify other important factors that must be guaranteed for the safety of the systems designed:

- non-repudiation
- authentication methods
- access control
- data protection of information and devices
- trust between 5G network components and end-users
- compliance with specific security and privacy policies

Conclusions

New types of private sector communications technologies and information services solutions offer opportunities for military applications that can make a major contribution to the successful conduct of military operations. For example, integrating IoT devices, which are becoming more widespread in the military environment, into the cloud can provide a real operational situational awareness to gain and maintain information superiority, contributing to the successful execution of operations. A very good basis for this is the isolated 5G technology presented in this article, which guarantees absolute security of data for military applications, as it allows military networks to be completely isolated from public networks. The author has thus obtained a positive answer to his first research question since 5G technology can be used to develop a robust, reliable, high-bandwidth system with low network latency that can be deployed on various combat platforms. Furthermore, with a private 5G network, high mobility, trusted and secured connections can be established to support battle command and control management and various support activities. As a result, the author also received a positive answer to the second question, but for private networks it should be highlighted that their deployment is associated with high deployment costs and a very heavy workload for the operating staff. Network slicing can be an excellent solution, where a separate 5G private network does not need to be established. However, a logical layer can be created by virtualising the existing public network to provide a more appropriate environment for military operations. Into this virtualised network, battlefield and military IoT devices can be integrated and deployed into a cloud infrastructure. The designed system will meet all the requirements of any technical solution deployed in an operational environment.

---

[15] Pasika Ranaweera et al.: Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Communications Surveys & Tutorials*, 23, no. 2 (2021). 1078–1124.

[16] Sabrina Sicari et al.: 5G in the Internet of Things Era: An Overview on Security and Privacy Challenges. *Computer Networks*, 179 (2020).

All in all, the author has successfully identified the fundamental security challenges for some segments of 5G technology in military environments, which could seriously impact the overall system operation. In a previous article,[17] the author has already made suggestions for securing Cloud of Things solutions, where he presented technical and technological solutions that can greatly contribute to building and maintaining a secure network in a military cloud environment.

References

Afolabi, Ibrahim – Tarik Taleb – Konstantinos Samdanis – Adlen Ksentini – Hannu Flinck: Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions. *IEEE Communications Surveys & Tutorials*, 20, no. 3 (2018). 2429–2453. Online: https://doi.org/10.1109/COMST.2018.2815638

Bastos, Luis – Germano Capela – Alper Koprulu – Gerard Elzinga: Potential of 5G Technologies for Military Application. *2021 International Conference on Military Communication and Information Systems (ICMCIS)*, (2021). 1–8. Online: https://doi.org/10.1109/ICMCIS52405.2021.9486402

Bognár, Eszter Katalin: Possibilities and Security Challenges of Using IoT for Military Purposes. *Hadmérnök*, 13, no. 3 (2018). 378–390.

ETSI: *5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.3.0 Release 15).* 2020.

Filali, Abderrahime – Amine Abouaomar – Soumaya Cherkaoui – Abdellatif Kobbane – Mohsen Guizani: Multi-Access Edge Computing: A Survey. *IEEE Access*, 8 (2020). 197017–197046. Online: https://doi.org/10.1109/ACCESS.2020.3034136

ITU-R: *Recommendation ITU-R M.2083-0, IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond.* 2020.

Kim, Hwankuk: 5G Core Network Security Issues and Attack Classification from Network Protocol Perspective. *Journal of Internet Services and Information Security (JISIS)*, 10 (2020). 1–15. Online: https://doi.org/10.22667/JISIS.2020.05.31.001

Kollár, Csaba: Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai. *Hadmérnök*, 12, no. 4 (2017). 146–158.

Liao, Jingjing – Xinjian Ou: 5G Military Application Scenarios and Private Network Architectures. *2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA)*, (2020). 726–732. Online: https://doi.org/10.1109/AEECA49918.2020.9213507

Nakao, Akihiro – Ping Du – Yoshiaki Kiriha – Fabrizio Granelli – Anteneh Atumo Gebremariam – Tarik Taleb – Miloud Bagaa: End-to-end Network Slicing for 5G Mobile Networks. *Journal of Information Processing*, 25 (2017). 153–163. Online: https://doi.org/10.2197/ipsjjip.25.153

[17] András Tóth: Cloud of Things Security Challenges and Solutions. *2021 Communication and Information Technologies (KIT)*, (2021). 1–6.

Ranaweera, Pasika – Anca Delia Jurcut – Madhusanka Liyanage: Survey on Multi-Access Edge Computing Security and Privacy. *IEEE Communications Surveys & Tutorials*, 23, no. 2 (2021). 1078–1124. Online: https://doi.org/10.1109/COMST.2021.3062546

Sicari, Sabrina – Alessandra Rizzardi – Alberto Coen-Porisini: 5G in the Internet of Things Era: An Overview on Security and Privacy Challenges. *Computer Networks*, 179 (2020). Online: https://doi.org/10.1016/j.comnet.2020.107345

Tóth, András: Cloud of Things Security Challenges and Solutions. *2021 Communication and Information Technologies (KIT)*, (2021). 1–6. Online: https://doi.org/10.1109/KIT52904.2021.9583760

Wang, Peng – Xing Zhang – Zhi Yan – Barry G. Evans – Wenbo Wang: Convergence of Satellite and Terrestrial Networks: A Comprehensive Survey. *IEEE Access*, 8 (2020). 5550–5588. Online: https://doi.org/10.1109/ACCESS.2019.2963223