telecom

MDPI

Article

Harnessing the Potential of Emerging Technologies to Break Down Barriers in Tactical Communications

Laura Concha Salor [1] **and Victor Monzon Baeza** [2,*]

[1] Nokia, 28108 Madrid, Spain; laura.concha_salor.ext@nokia.com
[2] SIGCOM Group, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, L-1855 Luxembourg, Luxembourg
* Correspondence: victor.monzon@uni.lu

Abstract: In the realm of military communications, the advent of new technologies like 5G and the future 6G networks holds promise. However, incorporating these technologies into tactical environments presents unique security challenges. This article delves into an analysis of these challenges by examining practical use cases for military communications, where emerging technologies can be applied. Our focus lies on identifying and presenting a range of emerging technologies associated with 5G and 6G, including the Internet of things (IoT), tactile internet, network virtualization and softwarization, artificial intelligence, network slicing, digital twins, neuromorphic processors, joint sensing and communications, and blockchain. We specifically explore their applicability in tactical environments by proposing where they can be potential use cases. Additionally, we provide an overview of legacy tactical radios so that they can be researched to address the challenges posed by these technologies.

Keywords: tactical communications; 5G; 6G; military networks; emerging technologies

Citation: Concha Salor, L.; Monzon Baeza, V. Harnessing the Potential of Emerging Technologies to Break Down Barriers in Tactical Communications. *Telecom* **2023**, *4*, 709–731. https://doi.org/10.3390/telecom4040032

Academic Editor: Peppino Fazio

Received: 19 July 2023
Revised: 13 September 2023
Accepted: 2 October 2023
Published: 16 October 2023

1. Introduction

Tactical communications refer to transmitting information, including orders and military intelligence, between different commands, individuals, or locations on the battlefield, particularly during combat. These communications encompass various delivery forms, such as verbal, written, visual, or auditory, and have often driven advancements in wireless technologies. For example, frequency hopping in second-generation mobile communication and direct sequence spread spectrum in 3G (third generation) originated from military communications. However, wireless communications have evolved independently of military needs since the advent of 4G or fourth generation. In the present day, the fifth [1] and sixth generations (5G/6G) have introduced new technologies and paradigms, such as the virtualization of network elements, which are considered crucial and highly appealing for enhancing tactical communication. Virtualization also holds the potential to improve network security.

An analysis is conducted in [2] on the tactical and commercial security guidelines provided by 5G, specifically focusing on communications for the public environments. The objective is to determine whether the security level achieved in a public 5G network can be extrapolated to military scenarios. As 5G is poised to dominate future telecommunications networks and facilitate new applications, its significance in shaping future societies cannot be overlooked. Consequently, there is a pressing need to integrate advancements in military and civil communications, which presents numerous challenges and security considerations for the broader community. However, it also brings forth fresh opportunities in various military domains, including capability interoperability, development, resilience, and secure communications. This integration empowers tactical communication networks with heightened protection and security for all elements involved in a tactical scenario.

Furthermore, the advancements brought by 5G offer significant enhancements to defense systems across land, sea, air, and space, particularly in terms of safety.

In this context, the North Atlantic Treaty Organization (NATO) and NATO Communications and Information Agency (NCIA) performed a preliminary evaluation of 5G technologies and their potential for tactical applications in [3], identifying four main areas where 5G could have a place:

1. Static mission communications.
2. Communications and information systems (CISs) for expeditionary missions and operations.
3. Maritime missions and operations.
4. Tactical missions and operations.

However, it fails to establish the correlation between emerging technologies and their applicability in various operational scenarios within these domains. Recent independent studies have been conducted to explore the potential of integrating 5G capabilities into military operations. One such critical 5G technology, network slicing, was initially proposed for military use in [4]. Alongside 5G, software-defined networking (SDN) plays a pivotal role in ensuring enhanced network scalability. The work presented in [5] introduces a mechanism that dynamically guarantees quality of service (QoS) for user data flow by leveraging SDN in diverse tactical networks. Sensor networks hold indispensable significance on the battlefield, and with the advent of the Internet of things (IoT), these networks can provide even greater advantages in the tactical realm as scrutinized in [6]. Achieving interoperability between systems is paramount in defense operations, particularly between command and control (C2) systems. In [7], the authors delve into the concepts and pathways that C2 systems should adopt, incorporating IoT networks.

Moving past the realm of 5G, the study conducted by NCIA as outlined in [3] holds significant importance in the NATO 2030 agenda as highlighted in [8]. This agenda emphasizes the strategic consideration of artificial intelligence, data autonomy, quantum-enabled technologies, hyper-sonic technologies, and biotechnology in the evolutionary path of military communications. These technologies collectively chart the course from 5G towards the anticipated sixth generation (6G) as discussed in [9], with AI taking center stage. Initial proposals are outlined in [10], where reinforcement learning, as an AI technique, is employed to enable autonomous learning by agents within tactical networks, ultimately enhancing situational awareness.

In the framework of improving tactical scenarios with emerging technologies, we highlight introducing artificial intelligence in the systems and the technology evolution roadmap because this will be the key to the next generation of networks, 6G [9]. In the 2030 Agenda, not only technologies are taken into account but there is also an initiative to strengthen NATO both militarily and politically and to adopt a more global approach for the Alliance in terms of space, novel materials and manufacturing, and energy and propulsion.

1.1. Background

A review of the literature is carried out to contextualize and identify the gaps in this analysis with the sake of identifying the possible technologies to renew communications in tactical scenarios. Table 1 contains the main surveys related to this proposal. The following criteria were taken into account in the analysis:

1. Legacy criteria: works that have considered the state of tactical radios and current waveforms for military communications.
2. Fifth-generation technologies criteria: works that consider explanations of the bases of the new emerging technologies with 5G but applied and explained from the point of view of military needs or tactical communications.
3. Sixth generation technologies criteria: works that begin to consider the technologies that are being proposed for the future 6G.
4. Use case criteria: relate and explain the application of 5G technologies to the different use cases within military operations where telecommunications systems are used.

As seen in Table 1, no survey includes and collects information about waveforms and tactical radio. This is an important gap since, to renew and improve current tactical radios, we need to know the properties of those waveforms used in transmission in a current scenario. There are also no works that consider possible technologies for 6G, such as neuromorphic processes and digital twins. Likewise, no proposal talks about the options of artificial intelligence in tactical scenarios.

Table 1. State-of-the-art review compared to our proposal.

Reference	Year	Legacy	5G Technologies	Proposals for 6G	Use Cases
[11]	2021	No	Partial	No	Partial
[12]	2020	No	Partial	No	No
[13]	2020	No	Partial	No	Partial
[14]	2020	No	Partial	No	No
[15]	2018	No	Partial	No	No
[16]	2020	No	Partial	No	Partial
Our Proposal	2023	Yes	Yes	Yes	Yes

Regarding the application of 5G, we partially found works that have considered this integration in military communications. Rather, they have not had all the possible technologies and have not related their application to the use cases within a mission. The work in [11] focuses on explaining the characteristics of 5G, not the component technologies. The focus is on the new radio (NR) and the virtualization properties of the core. Also, ref. [11] does not go into detail on tactical missions. Similarly, ref. [12] focuses on the radio part, in this case, analysis of a classic multi-antenna system. He does not consider new signal processing such as those proposed in this work to solve the inconveniences posed by the growing number of antennas used by these systems in NR. Ref. [13] focuses on the spectral part, analyzing the new spectral bands that 5G implies. Ref. [14] only presents an overview of the fundamental technologies of 5G that only include unmanned aerial vehicles (UAVs) for military application without going into the details of the use. In [15], an overview of 5G is presented, where the possibility of application in tactical scenarios is mentioned. Finally, ref. [16] presents a 5G proposal for security networks as required by the tactical scenarios. Instead, this work is focused more on public networks compared to military networks.

Concerning the use cases, there is also no other work to our knowledge that analyzes the use case options with 5G and 6G. Only [11,13] consider the tactical scenarios. However, these proposals do not show the relation between technology and the use case.

1.2. Motivation: Gap Identification

Against this background, the main gap detected is that the investigation of emerging technologies in the civil field is diverging and forgetting their application in the military field as well. There is a lack of analysis of the technologies that could be used to improve the tactical scenarios and how the risk posed by a war scenario can be minimized or solved with the help of modern technologies. New techniques and strategies, for example, are emerging in the field of encryption. Everything is being proposed for civil applications, not dedicating or actively focusing on the tactical field. The junction of emerging civil technologies with military or tactical scenarios presents promising opportunities and notable gaps which have not been identified in the literature so far. While there exists substantial potential for leveraging advancements such as artificial intelligence and unmanned systems in defense applications, several gaps must be addressed. Additionally, interoperability challenges between disparate civil and military systems can hinder seamless integration and communication on the battlefield. Moreover, cybersecurity vulnerabilities and data privacy concerns demand robust measures to safeguard sensitive information from adver-

sarial exploitation. Adequate training and education for military personnel to effectively operate and harness the capabilities of these emerging technologies are also imperative. Bridging these gaps will require collaborative efforts among policymakers, technologists, and military strategists to capitalize on the potential while mitigating risks and ensuring a balance between innovation and ethical principles. For all this motivation, a first analysis and compilation of the technologies that can be used in the different military uses must be carried out, which is the origin of this work and base for future research.

1.3. Our Contribution

Based on the previous motivation, this work is an analysis to select emerging technologies and their application to the military field, with special emphasis on tactical scenarios, improving such scenarios, and therefore serving as a starting point for new scientists to open up new lines of research. The focus is placed on tactical scenarios because it is the medium that includes the greatest application of communications. The tactical scenario is a term or concept to encompass all actions, operations, and decisions during a mission. For this reason, it is the term that includes the most possibilities of renewal within the military field. This analysis is not merely a compilation but a critical basis in a tutorial mode for future work. The contribution lines are as follows:

- We chose cutting-edge technologies advocated by both 5G and 6G that hold the potential to enhance tactical communications.
- We conducted a comprehensive overview of these technologies to pinpoint potential military applications. This description proves invaluable for field personnel in the military who may not be familiar with these technologies.
- We offer the reader a framework for comprehending how these technologies can be applied in the suggested tactical scenarios or use cases.
- Our work is a starting point for future lines of research that promote the use of civilian technology to help military development.

The rest of this paper is organized as follows: Section 2 presents a brief panoramic view of the two main elements in tactical scenarios. Section 3 proposes a group of emerging technologies as a potential candidate in tactical communications, performing an overview to understand the main features. In Section 4, the use cases are presented. In Section 5, the future trend and challenges are discussed. Finally, the conclusions are summarized in Section 6.

2. Picture of Tactical Communications: A Panoramic View

The analysis commences with an exploration of the core elements in tactical communications slated for advancement through the utilization of 5G/6G-driven emerging technologies: namely, the tactical radios and the waveforms employed for transmitting information on the battlefield. The waveform is the shape of a signal in the time domain and imparts information about the signal beyond its spectral characteristics.

2.1. Legacy Tactical Radios

During military operations, tactical radios serve as a vital tool for soldiers, enabling seamless communication and fostering a shared understanding of the entire operational landscape. Presented below are a few instances of military radios presently in use.

- **Land mobile radio** [17]: This constitutes the primary tactical system utilized within military bases for garrison communications, encompassing both single-channel analog systems and digital trunk systems. It primarily facilitates crucial communications within tactical environments or with public networks. Hence, the enhanced security level offered by 5G networks would be instrumental in modernizing this category of radio equipment. An example of this type of radio is the CSEL [18]. This radio is mainly used for search and rescue satellite aided tracking (SARSAT) systems by special operations forces and aviation units to support personnel survival, evasion, and recovery operations. It provides multi-functions, such as secure two-way data communications

over the horizon in real time, secure voice and data with six programmable ultra high frequency (UHF) voice frequencies for usage in satellite communications (SATCOM), among others.

- **PNR500** [19]: This radio is a personal, lightweight network portable radio used for platoon and squad-level communications over a very short range (over 800–1000 m range) in the UHF band.
- **RF-5800H-MP** [20]: This radio is a member of the Harris Corporation's FALCON II family of multi-band system types. it is an advanced radio that provides reliable tactical communications on the very high frequency (VHF) band and includes the latest voice mode that transmits digital voice using ultra-robust 3G waveforms, such as electronic counter-countermeasures (ECCM), to operate in channels where other waveforms do not work, offering secure communications in the presence of interference.
- **RF-7800H-MP** [21]: It is a terminal working in the high-frequency (HF) broadband. This is the lightest, smallest, and fastest portable radio available today. It is part of the FALCON II family from Harris Corporation, and thanks to its interoperability, the L3Harris broadband tactical system easily integrates into existing networks. It has capabilities for long-range, beyond-line-of-sight (BLOS) environments, which is compatible with an SDN-compatible architecture and provides continuous coverage on the power of a single battery.
- **AN/PRC-117G (V)1(C)** [22]: It is a multi-mission manpack, multiband radio for tactical combat-net radio (CNR) family that offers integrated satellite communications and communications security. It offers breakthrough broadband data rates and legacy narrowband performance. Moreover, its hardware is compatible with the mobile user objective system (MUOS), which supports multi-service users worldwide in ultra-high frequency bands.
- **PR4G** [23]: It is a tactical VHF radio belonging to CNR. It mainly supplies VHF band military units with a command, control, communications, and intelligence system with a complete system for electronic counter-countermeasures.
- **SPEARNET** [24]: This radio operates on a mobile ad hoc network model, optimizing network coverage, particularly in challenging terrains, where consistent coverage is difficult to sustain. In an ad hoc network, connected computers communicate directly without relying on a router. A key attribute of this radio is its capability to transmit data at high speeds.

These radios primarily and legacy operate within three main frequency bands designated for military applications: HF covering 3–300 MHz, VHF spanning 30–300 MHz, and UHF ranging from 300 MHz to 3 GHz. Satellite communications (SatCom) for military use are conducted in the L-band (1–2 GHz) and X-band (8–12 GHz) frequencies, enabling access to remote locations in military missions. However, a significant drawback of these frequency bands in adopting new 5G/6G technologies lies in their restricted bandwidth capacity, limiting the amount of data that can be transmitted.

2.2. Legacy Tactical Waveforms

Given the expanding battlespace and the presence of formidable adversaries, the presence of robust military communication systems has become exceptionally imperative. Tactical waveforms, being pivotal components, play a crucial role in ensuring the dependable and secure exchange of information to and from combatants on the battlefield. The most frequently employed waveforms in tactical scenarios are outlined in Figure 1.

- **HAVE-QUICK:** It is a waveform designed for an electromagnetic-resistant frequency-hopping system that protects the military. It is used in the UHF band for aeronautical mobile traffic.
- **SINCGARS:** Employing a non-IP, low-bandwidth voice coding format called CNR, this waveform has been integrated into numerous legacy tactical radios. Additionally, it facilitates low-rate data communications and finds application in vehicle-mounted, backpack, airborne, and handheld devices.

- **ECCM:** It is a waveform used especially in SDN-type radio. It is mainly designed to improve information security and resist interference. This waveform has the frequency hopping technique, which allows for quick change of the frequency of the energy that is being transmitted and received at only that frequency. In this way, it is difficult for enemies to detect frequency changes or predict the next frequency jump.
- **SRW:** This open-standard voice and data waveform, designed for mobile ad hoc usage, serves the purpose of extending wideband battlefield networks to the tactical periphery. SRW operates as a node or router within a wireless network, enabling the transmission of crucial information across significant distances. Additionally, it is employed by soldiers, small units, and even very compact sensors, like ground or air vehicles.
- **WNW:** This narrowband waveform is specifically crafted to establish network connectivity between aircraft and ground vehicles beyond line of sight (BLOS). It also serves the purpose of software-defined radio (SDR), offering connectivity to command posts at various levels, including company, platoon, and battalion.
- **MUOS:** It is a narrowband tactical satellite communication system that provides enhanced and secure communication capabilities, including simultaneous voice, video, and data for mobile and remote users. It is mainly used by terminal and manpack radios in software-defined radios (SDR) to provide narrowband communication in the UHF band.

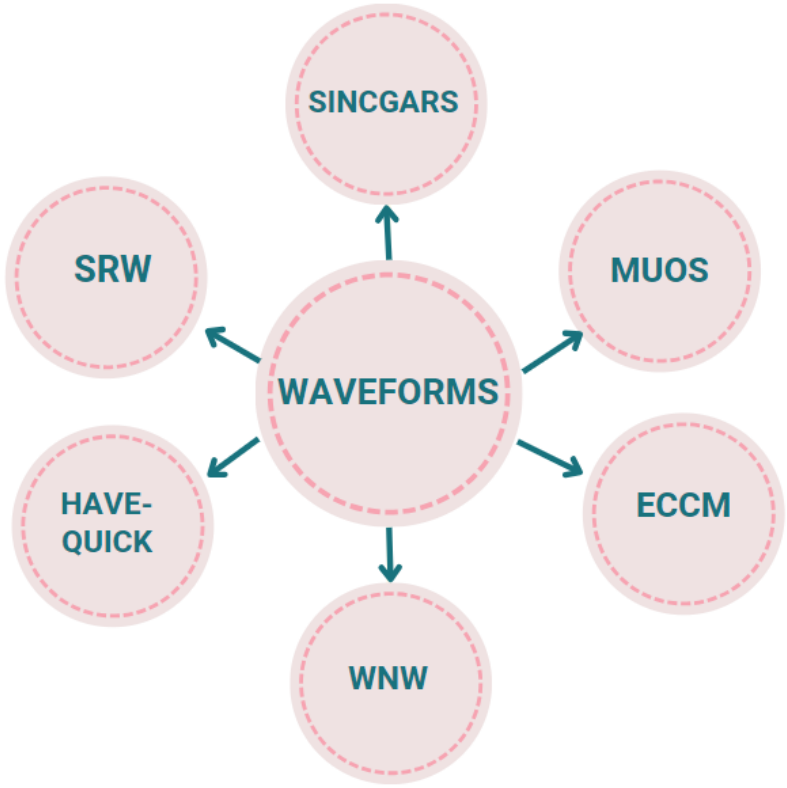

Figure 1. Waveforms used in tactical communications.

3. Emerging Technologies as Potential Candidates: Overview

In this study, we identified a specific set of these technologies, as depicted in Figure 2, aimed at enhancing tactical communications. The primary focus lies in delivering increased bandwidth and heightened levels of security and encryption. Below, a concise overview of each is presented to establish their relevance in military settings. It is important to note that this list is not exhaustive, but rather curated based on criteria for enhancing the tactical network. For more detailed technical information on these technologies, one can refer to dedicated literature. Additionally, future works may incorporate additional technologies.

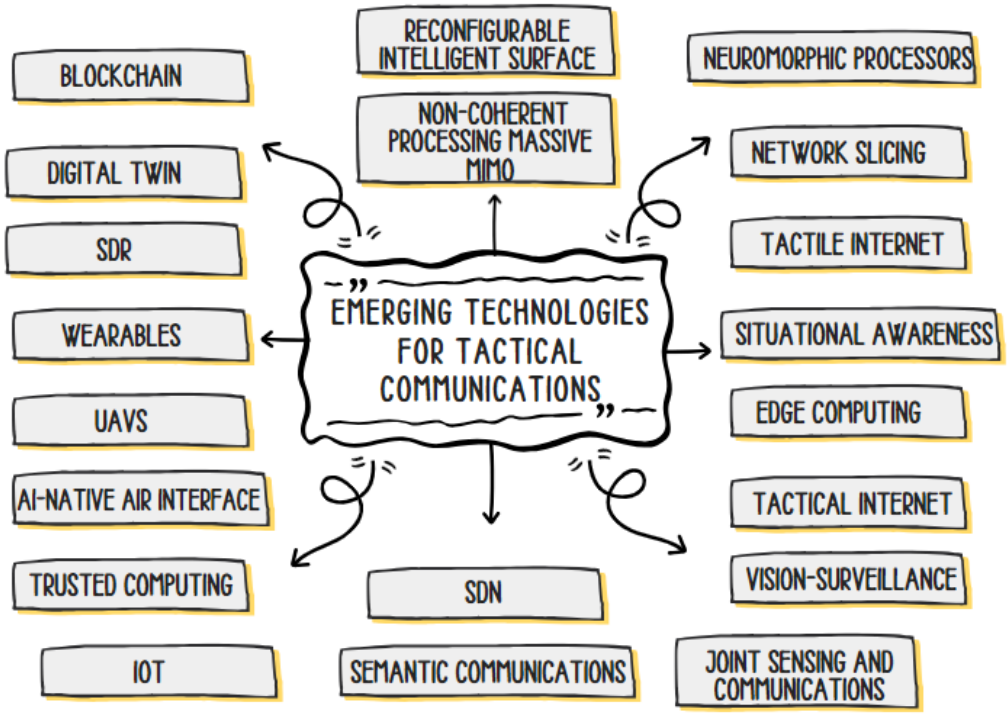

Figure 2. List of emerging technologies for tactical communications.

- **Internet of things (IoT)**: This is a network of everyday physical objects connected to other device systems with IoT connectivity to collect, store and share data. This technology has been around since the fourth generation (4G), but with advances in data processing, it is becoming more and more powerful and promising for new use cases. In the literature, we can find many references, of which we have selected the following as representative [25–27]. In these surveys, the reader can find an extension of information about IoT. The main characteristics of IoT are as follows:
    1. **Connectivity** IoT devices can be connected via radio waves, Bluetooth, Wi-Fi, Li-Fi, etc. In addition, one of the most used communication technologies currently used is NB-IoT, which allows wide, long-range coverage.
    2. **Scalability** These devices are used for different scenarios, from smart home automation to large factory automation.
    3. **Intelligence** IoT devices are used to store and share data. Thus, through the development of machine learning, it is possible to manage massive data to obtain highly useful information.
    4. **Power** Most devices are extremely small and are designed with low-power consumption technologies, powered by small batteries that last for years.
    5. **Security** The information handled by these devices is increasingly sensitive, which means an increase in the number of vulnerabilities that can come to affect them. All this makes it essential to keep all the information as secure as possible by protecting the integrity and confidentiality of the data, such as data encryption and cloud security.

    There is a new term, military Internet of things (MIoT), which refers to the IoT for military applications such as weapons, robots, or vehicles [28]. Some MIoT applications are military equipment logistics to facilitate efficiency, visibility, and military equipment. Some MIoT applications are as follows:

    1. **Military equipment logistics**: The adoption of MIoT can enhance military operational efficiency and visibility, for example, through the implementation of radio frequency identification tags and standardized barcodes. These technologies

enable the tracking of individual supplies and offer real-time visibility into the supply chain.

2. **Battlefield knowledge**: The IoT can serve a crucial function by gathering, processing, and promptly delivering synthesized information for swift decision making on the battlefield. Within *command*, *control*, *communications*, *computers* (C4) and *intelligence*, *surveillance*, and *reconnaissance* (C4ISR) systems, millions of IoT sensors can be integrated across various platforms, including UAVs, radars, infrared sensors, wearable devices, and more. This empowers combat troops with real-time data, enhancing coordination and control within the operational area.
3. **Personal detection soldier healthcare**: Through the integration of IoT sensors measuring vital signs, like temperature, blood pressure, blood glucose levels, and heart rate via body area networks, it becomes possible to monitor the health of soldiers in real time. This system can promptly notify soldiers of any abnormal conditions, such as dehydration, elevated heart rate, or low blood sugar. If necessary, it can also alert a medical response team at a base hospital.
   Soldiers are equipped with specialized helmets featuring integrated monitoring sensors designed to detect potential concussions and other brain traumas. The deployment of small, intelligent telemetric health monitoring devices and medical care equipment is becoming increasingly prevalent in combat scenarios. This allows for unmanned first aid to be administered promptly to soldiers in need.
4. **Military training**: IoT technology can find application in military training through the use of virtual simulations depicting various combat scenarios. With virtual reality, scenarios can be accurately replicated using sensors that track the position and physiological states of soldiers during training. The data gathered by these sensors can then be analyzed for later evaluation.

Similarly, MIoT can also be seen as IoT in the battlefield, the *Internet of battlefield things* (IoBT) [29,30].

- **Tactical internet**: It is a fluid network of very different subnets, which have various characteristics but must keep communication links without a fixed infrastructure [31]. Hence, tactical internet in tactical networks seeks to enhance the efforts of C4ISR with Internet-based applications. Military organizations use this type of network to provide communications services that connect strategic decision makers with commanders deployed at headquarters and extend that connection to all soldiers and vehicles.
  The most fundamental feature differentiating the tactical internet from a standard internet is core mobility; that is, you cannot rely on any other elements of the tactical internet to be present. Therefore, it must be able to adapt to situations where the paths between networks are constantly changing. The ideal tactical internet communication solution is to connect the low bandwidth tactic to the higher bandwidth core of the network, consolidating must-have network features into an easy-to-manage network device designed for your use in tactical vehicles with space constraints.
- **Tactile internet**: It is a technology for improving accuracy in human–machine and machine–machine interaction [32]. Key examples can be found in robotics, virtual reality, augmented reality, and the military, among others. The advantages of the tactile internet are diverse, such as high availability and security, ultra-fast reaction times, and high reliability. This offers low enough latency to build interactive systems in real time. In principle, all our human senses can interact with machines, but among the senses, visual–tactile interaction between humans is becoming more and more important, especially due to the proliferation of smartphones. For all these reasons, the tactile internet adds a new dimension to human–machine interaction by allowing tactile and haptic sensations to interact with their environment in real time.
  A tactile internet application is virtual reality. Low-latency communications enable "shared haptic virtual environments", where multiple users are physically coupled through a virtual reality simulation to perform tasks that require fine motor skills.

Another application is augmented reality. The tactile internet reaches new frontiers in assistance systems. Now, it is possible to virtually extend the field of vision in real time to achieve the concept of "seeing what others are not able to see".

- **Wearables**: These devices can operate at higher speeds with fewer interruptions and cover larger areas. This technology was originally proposed with health objectives in mind for medical applications [33], which can also be extended to military applications, such as assessing the soldier's health.
- **Unmanned aerial vehicles (UAVs)**: Commonly referred to as drones, these are aircraft that are guided autonomously, by remote control or both, and that carry some combination of sensors, receivers, and transmitters. They are used for strategic and operational reconnaissance for battlefield surveillance.
  The unmanned aerial system (UAS) consists of a UAV or drone, a ground controller, and a communication system (usually RF) between two or more drones. The wide variety of UAVs can be classified according to various roles within the military area: UCAV, ISTAR, multipurpose, radar and communications relay, and finally, delivery and air supply. Each of these types of UAVs are explained below:
  1. **Unmanned combat aerial vehicles (UCAV)**
     This refers to aircraft that are highly maneuverable that engage in combat and even, provide precision weapons delivery to surface targets.
  2. **Intelligence, surveillance, target acquisition, and reconnaissance (ISTAR)**
     This is a system that uses UAVs to collect enemy information and locate targets and hostile airspace without risking the lives of soldiers.
  3. **Multipurpose UAV**
     It is a combination of ISTAR and combat UAV. Its main function is the prohibition and carrying out of armed reconnaissance against critical and perishable targets.
  4. **Radar and communications relay UAV**
     They are usually a hot air balloons with helium and air, used for the low-level surveillance system that uses aerostats as radar platforms. They also provide radio and television signals.
  5. **UAV for delivery and air supply**
     These UAVs are designed for the precise delivery of small cargo items such as ammunition and food supplies for the Armed Forces.
- **Situational awareness**: This is essential in tactical operations to anticipate possible complications that may occur during the mission in unknown scenarios and environments for military personnel that can result in catastrophe [34–36]. Therefore, it is important to train in this aspect in order to reduce the response time to any unexpected situation. Situational awareness can be increased through visual interface technologies worn by soldiers, such as thermal cameras, night vision goggles, or AR technology to train soldiers for unknown environments. By means of the combination of these technologies, soldiers can better understand their environments and make decisions faster.
- **Trusted computing**: As the importance of data exchange increases, so does information security. Trusted computing is the key element of wearables to avoid exposing information to the enemy. This is a group of technologies, such as distributed learning, federated learning, SDN, and blockchain [37]. Distributed learning improves efficiency and performance, while federated learning complements and corrects the bottleneck of distributed learning.
- **Edge computing**: This technology involves storing and processing data closer to the edge of a user's network and not through a centralized data center [38]. This is used mainly by IoT devices since they exchange large amounts of information. In this way, the data do not experience latency problems in real time, as this can affect the performance of the application. This technology is proposed for the military field as a generic architecture based on remote and distributed computing, which serves to

assist in human assistance and disaster recover operations [39]. The main advantages of architectures with edge computing are as follows [40]:

1. Users receive faster and more reliable services with low latency and high availability.
2. Avoid bandwidth restrictions, reduce transmission delays, and controls the transmission of confidential data.
3. Ability to aggregate and analyze big data in services, which makes it possible to make decisions quickly. In the case of the military sector, it is very useful since it is no longer necessary to wait for information from the central command to directly make decisions in an intelligent and safe way.

- **Vision surveillance**: It is possible to increase the vision and vigilance abilities of the soldiers, thanks to the use of helmets and smart glasses or portable cameras. Thanks to these wearable sensors, soldiers can communicate information about individual situations in real time [41].
- **Network slicing (NS)**: It is implemented as a logical end-to-end (E2E) network across the entire network infrastructure [42]. The NS approach leverages technology such as network functions virtualization (NFV), sdn, virtual private networks (VPNs), and network E2E orchestration services to automate the deployment and operation of the segments. Therefore, it is possible to organize and customize the capacity, latency, and cybersecurity of each segment to meet the specific needs of each user, leading to a more cost-effective way of building dedicated networks. The next features are highlighted for future communications:

  1. **Enhanced mobile broadband**: This allows the operator to ensure reliable, ultra-high-speed data connections.
  2. **Very low latency**: Enables applications such as drones that fly beyond visual range. For example, the control of UAVs requires an extremely short response time.
  3. **Massive IoT**: Thousands of IoT devices, such as sensors, can be installed, enabling a wide variety of applications.

  The NS paradigm for the military sector [4] is considered to be the definition of a slice of its own for the technical scenario, which can simultaneously separate civilian and tactical communications and have them coexist.
- **Blockchain (BC)**: This technology comprises sets of data that are digitally signed, time-stamped, published, and linked in a chain. It enables multiple users to post simultaneously through a secure algorithm in various locations, eliminating any risk of data tampering [43,44]. There is only one version of the data, and all users can access it and confirm data authenticity. BC technology offers greater trust and data availability that can help logistics and military planning [45]. Data exchange through the BC can improve seamless communication and reduce data variation.
  One possible application of BC in military environments is in managing supply chains since the army transports equipment and personnel to difficult terrain around the world, which means that the process can be manipulated due to a series of critical points. However, with the BC, these problems can be addressed by offering a more secure record for the entire supply chain and allowing greater audibility and identification of responsibilities in real time, as well as providing supply personnel with real-time visibility of the material, parts, and equipment, thus offering greater precision in orders through smart contracts.
  Another potential application lies in access and identity management. It is imperative for advocacy organizations to have a clear understanding of who is gaining access to both physical and virtual locations. This necessitates substantial investments in databases that store and manage extensive volumes of sensitive and personal information. Blockchain technology can alleviate these challenges by interfacing with existing directories and databases, employing signature chains to function as a personal blockchain for each user. Other BC applications include supporting food security and healthcare challenges on the battlefield, building data-sharing platforms to increase

security and efficiency, and tracking critical and temperature-sensitive situations, such as pharmaceutical products and food.

- **SDN**: This technology is a new approach to networks, where the resources of a network are isolated in a virtualized system. SDN separates data forward functions from control (signaling) functions to design a network that can be centrally scheduled and managed [46]. The main purpose is to centrally control all network resources to optimize and automate their scheduling based on requirements. SDN networks are more efficient than traditional networks since they are managed from a single place and in a much simpler way. By dividing the data and control plane, SDN networks allow for more efficient load balancing and traffic distribution to bypass any potential blocking point, thereby improving network performance. Likewise, this type of network is configured automatically, which leads to a reduction in operating costs [47]. SDN benefits from network virtualization to better adapt to changes and increase network security by being more robust due to process automation, which is essential in the case of the military field [48]. In this sector, there is a large amount of data flow and applications that are handled, and thus, the requirement to reduce reaction time during missions is paramount.
- **SDR:** This system uses software to process various tasks in the transceiver (modulation, demodulation, encoding, etc.) instead of traditional hardware components [49]. The typical SDR setup involves an RF interface connected to a computer that performs analog-to-digital and reverse conversions to send or receive signals [50]. In the military field [51], it is recognized as a great solution capable of shaping more powerful and flexible tactical radios since they have a design that allows radio communications in areas not covered by telecommunications infrastructures and provides firm and resistant connectivity on the battlefield. The next features for SDR are highlighted considering future military missions:
    1. High "probability of intercept" also known as "probability of interception", within the ultra-wideband RF range. This improves detection capabilities and shortens response time.
    2. High data throughput, enabling low latency and real-time services.
    3. Ability to coordinate communications in real-time in various locations and combat operations.
    4. Re-transmission of radio signals that overcomes physical obstacles, expands network coverage, and allows flexibility in entering radio networks operating in different RF bands.
- **Reconfigurable intelligent surface (RIS)**: This novel antenna, constructed from cost-effective meta-surfaces, possesses the capability to manipulate signals for desired reflections, greatly augmenting data transmission from the sender to the receiver. In [52], challenges for RIS can be found to understand the opportunities that a new antenna architecture offers to wireless communications. This proves beneficial in tactical scenarios to evade interference from enemy signals, serving as an effective anti-jamming technique [53]. Currently, there is not a designated RIS design tailored for tactical scenarios.
- **Joint sensing and communications (JSC)**: New waveforms can perform both simultaneous functions [54]. This is applied specifically to radar systems. Radar can detect and identify targets, while communication transmits information between assets, giving us new enhanced radars [55,56]. In addition, we can include the internet functionality to obtain a new concept called "Internet of radars" [57].
- **AI-native air interface (AINAI)**: It delineates a revolutionary shift from the traditional approach to designing, standardizing, and developing communication systems. The aim is to provide an architecture with the most crucial data in the most efficient manner, taking into account the limitations of the existing hardware and radio environment [58]. Wireless communications are researching this new approach, which is a challenge for military communications.

- **Non-coherent processing in massive MIMO**: It is one of the base technologies of the new radio (NR) defined by 5G for access. It consists of equipping base stations or terminals with multiple antennas. Advances in signal processing have raised a massive number of antennas, giving rise to massive multiple-input multiple-output (MIMO) systems. As the number of antennas increases, we need to estimate and know more information about communication channels, complicating signal processing. For this reason, non-coherent processing techniques are emerging as a potential candidate associated with massive MIMO [59–64]. This is interesting for tactical scenarios since these techniques do not need pilot signals, where a lot of useful system information is carried. In this way, it reduces the risk of capture by the enemy.
- **Semantic communications (SC)**: This novel approach for communication systems involves transmitting only pertinent information directly related to the specific task at hand, resulting in an intelligent system that markedly reduces data traffic [34]. This presents a substantial advantage for tactical radios, particularly those outlined in the preceding section, as they typically operate with limited bandwidth [35].
- **Neuromorphic processors**: These refer to computing functions that emulate the human brain through finely grained parallel processing and real-time learning. The benefits of neuromorphic computing include enabling event-based low-energy consumption, scalable parallel processing, and the integration of memory and computation within a neuron unit [65]. In tactical scenarios, where swift responses to threats are crucial, the incorporation of neuromorphic processors into tactical radios aids in enhancing situational awareness.
- **Digital twin (DT)**: It constitutes a dynamic representation of the physical asset or system, persistently adjusting to operational alterations guided by continuously gathered online data and information [66]. The DT network can forecast the future of the corresponding physical counterpart [67]. In military contexts, this technology holds great significance, as it allows for the testing and evaluation of assets before subjecting them to physical testing. This results in substantial cost savings and significant time reductions by avoiding unnecessary testing and rebuilds. Additionally, it has the capability to anticipate future engine failures and vulnerabilities, enabling predictive maintenance based on historical and real-time data. This foresight allows for the early prediction of potential issues and improves response times.
  Furthermore, emerging technologies, like artificial intelligence and machine learning, can be integrated into digital twins. These techniques enable virtual representations to predict errors and help prevent costly consequences.

Based on this literature review and to the best knowledge of the authors, we compiled in Table 2 the status of each technology mentioned within the tactical and military scenarios. We classified the technologies by their level of implementation in tactical communications systems into two groups: technology proposed for military application, or if it is currently a challenge. If it has been considered in a scenario, we assessed whether it is in an inevitable or operational state, differentiating between fully or partially operational.

Table 2. Status of emerging technologies in tactical communications and networking.

	Existing			Challenge
	Research	**Full Operative**	**Partial Operative**	
MIoT	✓			
Tactile Internet		✓		
Tactical Internet		✓		
Wearables	✓		✓	
UAV		✓		
Situational awareness		✓		

Table 2. *Cont.*

	Existing			Challenge
	Research	**Full Operative**	**Partial Operative**	
Trusted Computing	✓			
Edge Computing	✓			
Network Scaling	✓			
Vision surveillance		✓		
Blockchain	✓			
SDN	✓		✓	
SDR	✓		✓	
Reconfigurable Intelligent Surface (RIS)				✓
Joint Sensing and Communications (JSC)	✓			
Non-Coherent Processing in massive MIMO				✓
AI-Native Air Interface (AINAI)				✓
Semantic Communications (SC)				✓
Neuromorphic Processors				✓
Digital Twin (DT)	✓			

4. Use Cases

In this study, a specific subset of operations and military scenarios that can be conducted on the battlefield is chosen to illustrate the application of various emerging technologies in tactical communications. Table 3 presents a list with the use cases selected to be analyzed, as well as the correspondence between the possible technologies presented as candidates in the renewal of the tactical panorama and each of the use cases.

Table 3. Association between use cases (UC) and emerging technologies for tactical scenarios.

# Use Cases	Operational in Tactical Scenarios	Selected Emerging Technologies
UC 1	Combat Search and Rescue (CSAR)	IoT, UAVs, wearables, Edge Computing
UC 2	Classic Voice Service Virtualization	Network slicing
UC 3	Medical Evacuation (MEDEVAC)	IoT, Wearables
UC 4	Fire Control/Support	IoT, UAVs
UC 5	Electronic warfare	Semantic Communications, SDR, Blockchain, RIS, AI-native interface
UC 6	Troop Training	Edge computing, Tactical Internet, AI, Tactile internet, Wearables, Trusted computing
UC 7	Situational Awareness	SDR, AI-native interface, Neuromorphic processors, JSC
UC 8	Military logistic report	Tactical Internet, IoT, Neuromorphic processors, AI-native interface
UC 9	Command and Control Post (CCP)	Neuromorphic processors, Trusted Computing, Network slicing
UC 10	Military Intelligence Operations	Trusted Computing, UAVs, Semantic Communications, SDN, Blockchain, Network slicing, AINAI
UC 11	Military data networks	Situational awareness, Network Slicing

4.1. Use Case 1: Combat Search and Rescue—CSAR

This scenario pertains to a military air rescue operation carried out amidst wartime conditions, either within or in close proximity to combat zones. The primary aim of the

rescue operation is to locate, communicate with, and retrieve aircrew downed during combat and any potential survivors. Other operational tasks within this use case could be supplying equipment and materials to train the soldiers in everything necessary for the rescue mission, carrying out medical evacuation operations, and configuring all the necessary equipment for the correct and efficient deployment, among others.

Any military tactical scenario needs reliable, secure, and fast communications. Fifth-generation technology allows this reliable connectivity, reduces latency, and, above all, has wide bandwidths, which is especially important in scenarios where operations are extremely urgent since many lives are at stake. The exchange of information and connectivity, for example, between military tactical radios, which make it possible to locate and communicate with troops in remote locations, can potentially reduce response time in emergencies such as rescues.

IoBT allows great technological development in military operations, battle scenes, equipment production, and war machinery, among others. Moreover, it uses sensors, wearables, and UAVs and makes use of edge computing, reducing communication latency between IoT devices and managing network bandwidth for better operational efficiency. One of the great applications of these technologies in the CSAR scenario is the use of UAVs equipped with advanced hardware, such as IoT sensors and cameras, that are capable of locating and obtaining a first visualization of the real-time terrain to track and find potential survivors on the battlefield.

4.2. Use Case 2: Classic Voice Service Virtualization

The network slicing mechanism employs numerous virtual networks within a shared physical network, each tailored to meet the unique requirements of individual users. This capability to isolate and restrict segments ensures that in the event of an enemy attack, not all network segments are affected. This offers significantly enhanced protection, security, reduced latency, and increased bandwidth, making it a crucial mechanism for tactical environments.

While essential communication services, such as voice, data, messaging, and video, are staples for military troops, additional value-added services necessitate the utilization of network slicing mechanisms to ensure ultra-reliable communications. Some of them are listed below:

1. **Push-to-talk (PTT):** It is a method that allows conversations over semi-duplex communication lines, that is, bidirectional communication. PTT devices are always listening, and by using a button, it is possible to change the voice reception mode to transmission mode. The "mission-critical push-to-talk (MCPTT)" standard is a functionality that meets the requirements for mission-critical voice communication, which include high availability, reliability, low latency, and emergency calls, among others.
2. **Fixed mobile convergence (FMC):** This service involves communication between military users connected through fixed and mobile military networks.
3. **Quality of service (QoS):** This capacity allows the network to control traffic by adapting resources such as bandwidth and thus ensuring good performance of voice services in critical communications. This is important to preserve the basic voice service in tactical scenarios with total security and criticality required at all times. Defining different QoS, we can assign priority to voice traffic over other types of traffic, ensuring that voice packets are processed first.
4. **Satellite Backhaul:** In the event that the fiber or microwave backhaul connection is lost, satellite backhaul could be useful for certain scenarios and locations to guarantee secure communications for these basic services [68–72]. In addition, 3GPP standardization [73] is defining the integration of the satellite in future terrestrial networks.

4.3. Use Case 3: Medical Evacuation—MEDEVAC

This scenario is based on a system for transporting wounded combatants from one location to a specialized hospital. Evacuations are generally carried out in air vehicles used

as "air ambulances", which have everything necessary, such as specialized health personnel and first aid material, to transfer the patient as quickly as possible to the specialized hospital. It is vital in these platforms to keep fast and efficient communications to guarantee patient safety. In the context of this MEDEVAC scenario, certain 5G technologies, such as IoT devices or wearables, hold potential applications, for instance, smart clothing incorporates sensors (wearables) capable of measuring parameters like temperature, heart rate, or blood pressure. This enables the real-time monitoring of soldiers' health with a high degree of accuracy. The gathered data can be directly transmitted to specialized doctors for personalized follow-up, enabling early diagnosis and prompt evacuation when necessary. Depending on the specific functions to be monitored, these wearables can be integrated into helmets or glasses for head-worn applications, worn as bracelets on the wrist, or integrated into garments, like T-shirts. Additionally, they can even be applied as electronic tattoos on the body.

4.4. Use Case 4: Fire Control/Support

Fire control encompasses the coordinated utilization of resources by commanders during the execution of a combat task. It stands as a crucial and fundamental element for enhanced combat control. IoT technology facilitates the transmission of data on a massive scale and in real time, even in complex environments like combat situations. This is achieved at high speeds, ensuring extensive coverage by leveraging the low-band spectrum, particularly frequencies below 1 GHz. Another technology that is of great help in fire support is UAVs. Employing a drone equipped with thermal sensors, it is possible to track the fire and send an alarm with the exact coordinates of the location, in addition to transmitting a multitude of information, such as time speed, temperature, and real-time images of the situation, and all this without putting any human being at risk since everything is automated. Also, due to the autonomy of drones, it is possible that the control center can take control of the drone to manually collect and track the environment. The main advantage of using UAVs is the anticipation and early detection of fires in real time since it analyzes the main factors that can cause the fire, even when there is little visibility on the ground.

4.5. Use Case 5: Electronic Warfare

This scenario involves the utilization and manipulation of an adversary's electromagnetic spectrum, which includes actions like blocking or disrupting communications within that spectrum. It also encompasses intercepting, interrupting, and deciphering communications to gather intelligence from the enemy. With the increasing number of threats posed by adversaries, it has become imperative to cover the highest 5G frequencies (24–44 GHz) due to their expansive capacities and accelerated speeds.

In this use case, it is crucial to emphasize the significance of blockchain technology, as it plays a central role in managing access and identity. This is essential for preventing potential breaches in communication security. Edge computing operates in a decentralized manner, positioning computation and data storage closer to where they are needed. This approach enhances response times and conserves bandwidth. The distributed characteristic helps the data to be more protected, more controlled, and that makes it more complicated for malicious access in electronic warfare. Through trusted computing, an external third party can trust the software running on your computer when your computer interacts with its server. This also helps in the validation and control of the data in a secure manner. Looking at the application layer, improving information transmission can be achieved through semantic communications for intruder detection and RIS to mitigate interference. SDR technology has become pivotal in communication during any combat operation, owing to its impressive performance and adaptability. This technology greatly bolsters electronic warfare with its multifaceted capabilities, including support for various waveforms, advanced cryptology, and heightened processing capabilities. This leads to superior real-time communication and decision making, all facilitated by a single radio.

4.6. Use Case 6: Troop Training

Augmented reality seamlessly blends the virtual world with reality. In a military context, this technology greatly enhances soldiers' capacity to spot adversaries and acquire real-time battlefield information. Notably, augmented reality proves indispensable for military training. By donning virtual reality glasses, it becomes feasible to simulate a computer-generated scenario that closely mirrors reality. This enables soldiers to train with authentic equipment they would employ on actual missions.

Virtual reality glasses have several uses within military training; one of them is to connect directly with the image recorded by the surveillance cameras on a supposed battlefield in such a way that they can intercept the enemy much faster. Additional technologies like trusted and edge computing, tactile interfaces, and tactical internet play a pivotal role in advancing virtual and augmented reality technology. These technologies primarily center around interactions between humans and machines, as well as between different machines. They incorporate tactile and haptic feedback to facilitate real-time interaction with the environment. This setup ensures high availability, security, and exceptionally swift response times, particularly when using virtual reality glasses. Furthermore, artificial intelligence aids in the recreation of environments, allowing troops to immerse themselves in simulated scenarios.

4.7. Use Case 7: Situational Awareness

Situational awareness (SA) involves having a comprehensive understanding of the overall environment surrounding a combatant or military platform. Given the dynamic nature of battle scenarios, real-time SA is imperative. JSC plays a crucial role in enhancing information collection efficiency by utilizing the same signal for both radar and communication functions. The data are then swiftly processed by neuromorphic processors, significantly outpacing the capabilities of conventional processors. This enables the extraction of a larger volume of pertinent information for situational awareness. Additionally, AI can assist in streamlining computational complexity.

4.8. Use Case 8: Military Logistic Report

This UC holds paramount importance in military operations, as it guarantees the precise allocation of resources to units for their military endeavors. Among the technologies exerting a substantial influence on logistics, IoT stands out. These devices enhance security in overseeing logistic procedures, elevate transparency in the supply chain, and most importantly, deliver real-time updates on the status of products and services. In addition, they provide great energy efficiency due to the low-consumption technologies with which they are designed, thus also reducing costs. The tactical internet stands out as another noteworthy technology. It facilitates communication services that link strategic decision makers with commanders, enabling real-time access to information (supplied by neuromorphic processors) regarding the service's status. Additionally, it ensures dependable and secure communications, preventing the enemy from intercepting them and exploiting resource status during a military operation.

4.9. Use Case 9: Command and Control Post

Command and control posts (CCPs) are establishments where military personnel strategize, oversee, synchronize, and manage forces and operations to achieve mission objectives. These points serve as hubs for extensive information. Neuromorphic processors offer the capacity to handle this substantial volume of data, while trusted computing ensures the integrity of the information. Additionally, the post can be integrated into IoT networks or designated as one of the slices within network slicing.

4.10. Use Case 10: Military Intelligence Operations

These operations serve as crucial foundations for the triumph of military endeavors. Their role encompasses gathering and scrutinizing data pertaining to the forces, strategies,

and operations of other nations. This aids in uncovering potential intentions of adversaries and criminal organizations, allowing for the exploitation of their weaknesses and furnishing commanders with vital insights for orientation and decision-making.

Within intelligence operations, one technology of paramount significance is trusted computing. Given the extensive global data exchange, ensuring information security is of the utmost importance. Trusted computing offers a key advantage in safeguarding information from exposure to adversaries. SDN and blockchain are related to trusted computing and can mutually benefit from ensuring security both in the software that defines the networks and in the transactions carried out on the blockchain. Network virtualization enables the enhancement of network security through increased robustness achieved via automated processes. Semantic communication and AINAI play crucial roles in identifying data within this specific type of operation. It is also worth mentioning UAVs, which are one of the advanced low-cost solutions for intelligence missions in short-range operations.

4.11. Use Case 11: Military Data Networks

In the military field, it is essential to establish communications between the different platforms during a tactical operation or mission since, in this way, it is possible to make efficient decisions quickly, accurately, and, above all, safely. This is made by "tactical data links", which ensure optimal situational awareness and command and control capabilities in increasingly challenging environments. In general, the most popular data links used are Link 11, Link 16, and Link 22.

Link 11, also known as the "tactical digital information link" (TADIL), provides an exchange of tactical information on naval, air, and land operations. It operates with HF or UHF radios. Link 16 is an improved data link standard used mainly by NATO and whose main objective is to transmit and exchange information in real-time, mainly between planes by means of RF signals that operate within the line of sight of other network members. This Link 16 has more security, speed, and an increase in the volume of information that can be transmitted compared to Link 11. Link 16 operates on the TDMA principle, where time slots are allocated between all participating Links 16 for transmitting and receiving data.

Link 22 is also known as the "NATO-improved Link Eleven" (NILE) program and is the most recent standard. This link replaces Link 11 and complements Link 16, improving low data rate, robustness, and susceptibility to interference. Link 16 provides short-range information exchange, while Link 22 enhances this feature by providing long-range information exchange. The most characteristic of this new data link is the automated bandwidth and the ability to use HF, UHF, and frequency-hopping networks. It is worth highlighting the tactical data link, especially for helicopters, the "variable message format" (VMF). It is especially important in bandwidth-constrained communications situations, for example, when using CNR. VMF is mostly transmitted by single-channel radio systems, like SINCGARS, CNR, or HAVEQUICK.

Each of these protocols includes a series of messages with a specific format to transmit certain information necessary in an operation or mission. For example, the positions of troops or combatants, information about possible mines, SOS messages, obstacle positions, enemy information, evacuations, etc. All of this helps to understand the environment on the battlefield during a mission. We selected two technologies as shown in Table 3: situational awareness (potentially seen as telepresence technologies) and NS. On the one hand, situational awareness helps to enhance knowledge of everything that surrounds the situation within a mission or operation. This is a concept widely used in the military field. It has also been extended to the space sector recently. On the other hand, the other technology that we selected is NS, which arises with 5G. This choice is based on the fact that by having so many different data links, each of them can be processed in a different slice. This allows not having multiple terminals as now happens in a traditional scenario. Currently, each data link to create the data transmission network is made with a different

terminal. NS enables you to manage and orchestrate everything within the same terminal, thanks to the virtualization characteristics.

5G NR is a fundamental part of this type of scenario as it allows greater flexibility in the way resources are allocated. That is, multiple types of waves or signals are sent in a given bandwidth. This provides much more capacity and, with it, the possibility of transmitting many more messages simultaneously in real time.

5. Discussion and Future Trends

Today, the modern battlefield has undergone a radical change, where multiple assets of different types come into play, carrying out new military missions with more complex tactical scenarios. In this evolving landscape, conventional tactical radios and waveforms fall short in addressing critical requirements like security, flexibility, speed, and cost effectiveness. These constraints need to be met in order to effectively navigate the demanding conditions of the modern battlefield. Therefore, potential lines of action to renew tactical communications must be considered. On the one hand, from a technological point of view, and on the other hand, from a signal processing point of view, to define new waveforms which enhance and overcome the current network performance.

5.1. From a Technological Point of View

The technologies mentioned in this work are mostly part of 5G and future generation 6G. For this reason, as is analyzed in this paper, the integration of these technologies, which entails the integration of 5G and 6G in tactical networks, opens up many possibilities to improve performance, security, and reliability in military environments. Below, we highlight these possibilities for further investigation.

1. Network virtualization: Implement virtualized networks using 5G technology to provide greater flexibility, scalability, and security. Explore ways to optimize network slicing, which allows the creation of dedicated virtual networks tailored to specific tactical communication requirements.
2. Software-defined networks: Deploy SDN solutions in tactical communications to enable centralized control and management of network resources. SDN can enhance network agility, optimize bandwidth allocation, and improve network resilience in dynamic tactical environments.
3. Internet of things: Utilize IoT sensors and devices to enhance situational awareness, collect real-time data, and enable seamless connectivity among military assets. Explore the integration of IoT with tactical communication networks to enable efficient data exchange and decision making.
4. Blockchain technology: Enhance the integrity, security, and trustworthiness of tactical communications. Implement decentralized architectures that provide secure peer-to-peer communication, identity management, and tamper-proof data storage.
5. Semantic communications: Enable intelligent information exchange and interoperability among different tactical communication systems. Develop standardized ontologies and protocols for seamless communication and data sharing.
6. Neuromorphic processors: Explore using neuromorphic processors and cognitive computing in tactical communications. Investigate their potential for advanced signal processing, pattern recognition, and cognitive decision making in resource-constrained environments.
7. Resilient communication architectures: Design resilient communication architectures that can withstand disruptions, jamming and cyber threats. Explore redundancy mechanisms, dynamic routing protocols, and adaptive communication strategies to ensure uninterrupted connectivity in challenging tactical scenarios.
8. Human–machine interfaces with AINAI: Develop intuitive and user-friendly interfaces that enable efficient interaction between military personnel and advanced communication technologies. Focus on designing interfaces that reduce cognitive load, enhance situational awareness, and facilitate rapid decision making.

These lines of action can help drive the renewal of tactical communications by leveraging the capabilities of 5G technologies and emerging technologies with 6G, ultimately enhancing the efficiency, security, and performance of military communications in tactical scenarios.

5.2. From a Signal Processing Point of View

Foundational components like radios and waveforms require initial upgrades. The classical waveforms mentioned earlier utilize multiplexing and various access schemes based on conventional resources, like frequency-division multiple access, time-division multiple access, or code-division multiple access. However, these prove limiting, given the high number of active components in today's tactical scenarios. Consequently, the innovative nonorthogonal multiple access technique shows promise, surpassing the performance of traditional MAS but also posing challenges for tactical networks. Furthermore, these radios and waveforms are designed for low-communication bandwidths, which proves incompatible with the advanced technologies driven by 5G.

Apart from the emerging technologies outlined in Section 3, it is worth highlighting the progress in massive multi-antenna systems, enabling the integration of non-coherent communications [59–61]. This form of communication relies on the capability to demodulate signals without requiring channel estimation information. While non-coherent communications are not novel technologies, they have re-surged in interest and significance due to technological progress. They hold potential value in the tactical field, as the ability to detect without relying on channel information mitigates interception and signal attack concerns. The Doppler effect in high-speed varying channels is solved with non-coherent processing. Enhanced anti-jamming techniques can be improved using the same proposals, which is a challenge for new tactical radio.

6. Conclusions

The utilization of 5G and prospective 6G networks poses challenges to military communications in tactical situations. This study carefully chose and examined a set of cutting-edge technologies that facilitate the advancement of tactical networks. The implementation of network virtualization through 5G plays a crucial role in ensuring enhanced security. These advancements are pivotal in enhancing the practicality of military applications that truly embrace network-centric operations. Software-defined networks, the IoT, blockchain, AI, semantic communications, and neuromorphic processors all contribute to the enhancement of communication performance. These technologies notably improved eleven traditional military use cases. This study serves as a foundational analysis, providing a starting point for new researchers to explore fresh avenues of inquiry. It is not simply a compilation; rather, it serves as an analytical framework for guiding future research initiatives.

Author Contributions: Conceptualization, methodology, investigation, validation, resources, writing—original draft preparation and visualization, L.C.S. and V.M.B.; writing—review and editing, L.C.S. and V.M.B.; supervision, V.M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Not applicable.

Conflicts of Interest: All authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as potential conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AINAI	AI-Native Air Interface
AR	Augmented Reality
BC	Blockchain

BLOS	Beyond Line Of Sight
CCP	Command and Control Post
CIS	Communications and Information Systems
CNR	Combat-Net Radio
CSAR	Combat Search and Rescue
CSEL	Combat Survivor Evader Locator
C4ISR	Command, Control, Communications, Computers (C4) Intelligence, Surveillance and Reconnaissance
ECCM	Electronic Counter-Countermeasures
FMC	Fixed–Mobile Convergence
GPS	Global Positioning System
HF	High Frequency
IoBT	The Internet of Battlefield Things
IoT	Internet of Things
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
JSC	Joint Sensing and Communications
MCPTT	Mission-Critical Push To Talk
MEDEVAC	Medical Evacuation
MIMO	Multiple-Input Multiple-Output
MIoT	Military Internet of Things
mMTC	Massive Machine-Type Communications
MUOS	Mobile User Objective System
NATO	North Atlantic Treaty Organization
NILE	NATO Improved Link Eleven
NB-IoT	NarrowBand IoT
NCIA	NATO Communications Information Agency
NFV	Network Functions Virtualization
NS	Network Slicing
PTT	Push To Talk
QoS	Quality of Service
RIS	Reconfigurable Intelligent Surface
SA	Situational Awareness
SARSAT	Satellite-Assisted Tracking System
SATCOM	Satellite Communication
SC	Semantic Communications
SDN	Software-Defined Networking
SDR	Software-Defined Radio
SINCGARS	Single Channel Ground and Airborne Radio System
SRW	Soldier Radio Waveform
TADIL	Tactical Digital Information Link
UAS	Unmanned Aerial System
UCAV	Unmanned Combat Aerial Vehicles
UC	Use Case
UHF	Ultra High Frequency
VMF	Variable Message Format
VPN	Virtual Private Network
VHF	Very High Frequency
WNW	Wideband Networking Waveform

References

1. Agiwal, M.; Roy, A.; Saxena, N. Next Generation 5G Wireless Networks: A Comprehensive Survey. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 1617–1655. [CrossRef]
2. Suomalainen, J.; Julku, J.; Vehkaperä, M.; Posti, H. Securing Public Safety Communications on Commercial and Tactical 5G Networks: A Survey and Future Research Directions. *IEEE Open J. Commun. Soc.* **2021**, *2*, 1590–1615. [CrossRef]
3. NCIA. NATO Tech Agency Explores the Potential of 5G for the Alliance. Available online: https://www.ncia.nato.int/about-us/newsroom/nato-tech-agency-explores-the-potential-of-5g-for-the-alliance.html (accessed on 7 October 2023).

4. Malik, M.; Kothari, A.; Pandhare, R.A. Network Slicing In 5g: Possible Military Exclusive Slice. In Proceedings of the 2022 1st International Conference on the Paradigm Shifts in Communication, Embedded Systems, Machine Learning and Signal Processing (PCEMS), Nagpur, India, 6–7 May 2022; pp. 48–52.
5. Eswarappa, S.M.; Rettore, P.H.L.; Loevenich, J.; Sevenich, P.; Lopes, R.R.F. Towards Adaptive QoS in SDN-enabled Heterogeneous Tactical Networks. In Proceedings of the 2021 International Conference on Military Communication and Information Systems (ICMCIS), The Hague, Netherlands, 4–5 May 2021; pp. 1–8.
6. Pannetier, B.; Dezert, J.; Moras, J.; Levy, R. Wireless Sensor Network for Tactical Situation Assessment. *IEEE Sens. J.* **2022**, *22*, 1051–1062. [CrossRef]
7. Pradhan, M.; Manso, M.; Michaelis, J.R. Concepts and Directions for Future IoT and C2 Interoperability. In Proceedings of the MILCOM 2021—2021 IEEE Military Communications Conference (MILCOM), San Diego, CA, USA, 29 November–2 December 2021; pp. 231–236.
8. NATO. Emerging and Disruptive Technologies. Available online: https://www.nato.int/cps/eb/natohq/topics$_$184303.html (accessed on 7 October 2023).
9. Hong, E.K.; Lee, I.; Shim, B.; Ko, Y.C.; Kim, S.H.; Pack, S.; Lee, K.; Kim, S.; Kim, J.H.; Shin, Y.; et al. 6G R&D vision: Requirements and candidate technologies. *J. Commun. Netw.* **2022**, *24*, 232–245.
10. Möhlenhof, T.; Jansen, N.; Rachid, W. Reinforcement Learning Environment for Tactical Networks. In Proceedings of the 2021 International Conference on Military Communication and Information Systems (ICMCIS), The Hague, The Netherlands, 4–5 May 2021; pp. 1–8.
11. Bastos, L.; Capela, G.; Koprulu, A.; Elzinga, G. Potential of 5G technologies for military application. In Proceedings of the 2021 International Conference on Military Communication and Information Systems (ICMCIS), The Hague, The Netherlands, 4–5 May 2021, pp. 1–8.
12. Bhardwaj, A. 5G for Military Communications. *Procedia Comput. Sci.* **2020**, *171*, 2665–2674. [CrossRef]
13. Elmasry, G.F. *DSA and 5G Adaptation to Military Communications*; Wiley: Hoboken, NJ, USA, 2020.
14. Zhang, H.; Song, L.; Han, Z. Overview of 5G and Beyond Communications. In *Unmanned Aerial Vehicle Applications over Cellular Networks for 5G and Beyond*; Springer International Publishing: Cham, Switzerland, 2020; pp. 1–25.
15. Barb, G.R.; Otesteanu, M. 5G: An Overview on Challenges and Key Solutions. In Proceedings of the 2018 International Symposium on Electronics and Telecommunications (ISETC), Timisoara, Romania, 8–9 November 2018; pp. 1–4.
16. Liao, J.; Ou, X. 5G Military Application Scenarios and Private Network Architectures. In Proceedings of the 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 25–27 August 2020; pp. 726–732.
17. NCSWIC, S. Land Mobile Radio (LMR) 101. Available online: https://www.cisa.gov/sites/default/files/publications/LMR$%$20101_508FINAL_0_0.pdf (accessed on 7 October 2023).
18. Navy, N. Combat Survivor Evader Locator (CSEL) System. Available online: https://www.navair.navy.mil/product/combat-survivor-evader-locator-csel-system (accessed on 7 October 2023).
19. Army, L. Lightweight Radiophone PNR500. Available online: https://ejercito.defensa.gob.es/unidades/Guipuzcoa/ril67/Organizacion/materiales/Transmisiones/index.html (accessed on 7 October 2023).
20. Harris. FALCON ®II RF-5800H-MP High-Frequency Manpack Radio. Available online: http://www.railce.com/cw/casc/harris/rf-5800h-mp.pdf (accessed on 7 October 2023).
21. Technologies, L3Harris. FALCON III® RF-7800H-MP WIDEBAND HF/VHF MANPACK RADIO. Available online: https://www.l3harris.com/all-capabilities/falcon-iii-rf-7800h-mp-wideband-hf-vhf-manpack-radio (accessed on 7 October 2023).
22. Harris. L3HARRIS FALCON III® AN/PRC-117G(V)1(C). Available online: https://www.l3harris.com/sites/default/files/2021-01/cs-tcom-an-prc-117g-multiband-networking-manpack-radio-datasheet.pdf (accessed on 7 October 2023).
23. Ministry of Defense, M. PR4G Radiotelephone. Available online: https://ejercito.defensa.gob.es/materiales/transmisiones/Radiotelefono.html (accessed on 7 October 2023).
24. Army. SPEARNET. Available online: https://ejercito.defensa.gob.es/en/materiales/transmisiones/Spearnet.html (accessed on 7 October 2023).
25. Zhao, Q.; Li, G.; Cai, J.; Zhou, M.; Feng, L. A Tutorial on Internet of Behaviors: Concept, Architecture, Technology, Applications, and Challenges. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 1227–1260. [CrossRef]
26. Shi, F.; Zhou, F.; Liu, H.; Chen, L.; Ning, H. Survey and Tutorial on Hybrid Human-Artificial Intelligence. *Tsinghua Sci. Technol.* **2023**, *28*, 486–499. [CrossRef]
27. Zhang, L.; Liang, Y.C.; Xiao, M. Spectrum Sharing for Internet of Things: A Survey. *IEEE Wirel. Commun.* **2019**, *26*, 132–139. [CrossRef]
28. Gotarane, V.; Raskar, S. IoT Practices in Military Applications. In Proceedings of the 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 23–25 April 2019; pp. 891–894.
29. Sánchez, P.M.S.; Celdrán, A.H.; Bovet, G.; Pérez, G.M.; Stiller, B. SpecForce: A Framework to Secure IoT Spectrum Sensors in the Internet of Battlefield Things. *IEEE Commun. Mag.* **2023**, *61*, 174–180. [CrossRef]
30. Kott, A.; Swami, A.; West, B.J. The Internet of Battle Things. *Computer* **2016**, *49*, 70–75. [CrossRef]
31. Zhang, S. Topology Structure Model of Tactical Internet Based on Complex Network. In Proceedings of the 2022 4th International Conference on Frontiers Technology of Information and Computer (ICFTIC), Qingdao, China, 2–4 December 2022; pp. 1052–1055.

32. Fitzek, F.H.; Li, S.C.; Speidel, S.; Strufe, T.; Seeling, P. Frontiers of Transdisciplinary Research in Tactile Internet with Human-in-the-Loop. In Proceedings of the 2021 17th International Symposium on Wireless Communication Systems (ISWCS), Berlin, Germany, 6–9 September 2021; pp. 1–6.
33. Seneviratne, S.; Hu, Y.; Nguyen, T.; Lan, G.; Khalifa, S.; Thilakarathna, K.; Hassan, M.; Seneviratne, A. A Survey of Wearable Devices and Challenges. *IEEE Commun. Surv. Tutor.* **2017**, *19*, 2573–2620. [CrossRef]
34. Lokumarambage, M.U.; Gowrisetty, V.S.S.; Rezaei, H.; Sivalingam, T.; Rajatheva, N.; Fernando, A. Wireless End-to-End Image Transmission System Using Semantic Communications. *IEEE Access* **2023**, *11*, 37149–37163. [CrossRef]
35. Yang, W.; Du, H.; Liew, Z.Q.; Lim, W.Y.B.; Xiong, Z.; Niyato, D.; Chi, X.; Shen, X.; Miao, C. Semantic Communications for Future Internet: Fundamentals, Applications, and Challenges. *IEEE Commun. Surv. Tutor.* **2023**, *25*, 213–250. [CrossRef]
36. Baeza, V.M.; Ortiz, F.; Lagunas, E.; Abdu, T.S.; Chatzinotas, S. Multi-Criteria Ground Segment Dimensioning for Non-Geostationary Satellite Constellations. In Proceedings of the 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 6–9 June 2023; pp. 252–257.
37. Wang, G.; Tian, D.; Gu, F.; Li, J.; Lu, Y. Design of Terminal Security Access Scheme based on Trusted Computing in Ubiquitous Electric Internet of Things. In Proceedings of the 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 11–13 December 2020; Volume 9, pp. 188–192.
38. Xinwang, Y.; Zhidong, X.; Xin, T. Anti-jamming Channel Allocation in UAV-Enabled Edge Computing: A Stackelberg Game Approach. In Proceedings of the 2022 18th International Conference on Mobility, Sensing and Networking (MSN), Guangzhou, China, 14–16 December 2022; pp. 936–941.
39. Pradhan, M.; Poltronieri, F.; Tortonesi, M. Generic Architecture for Edge Computing Based on SPF for Military HADR Operations. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 225–230.
40. Douch, S.; Abid, M.R.; Zine-Dine, K.; Bouzidi, D.; Benhaddou, D. Edge Computing Technology Enablers: A Systematic Lecture Study. *IEEE Access* **2022**, *10*, 69264–69302. [CrossRef]
41. Janani, K.; Gobhinath, S.; Santhosh Kumar, K.V.; Roshni, S.; Rajesh, A. Vision Based Surveillance Robot for Military Applications. In Proceedings of the 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 25–26 March 2022; Volume 1, pp. 462–466.
42. Afolabi, I.; Taleb, T.; Samdanis, K.; Ksentini, A.; Flinck, H. Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions. *IEEE Commun. Surv. Tutor.* **2018**, *20*, 2429–2453. [CrossRef]
43. Monrat, A.A.; Schelén, O.; Andersson, K. A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
44. Houda, Z.A.E.; Beaugeard, J.; Sauvêtre, Q.; Khoukhi, L. Towards a Secure and Scalable Access Control System Using Blockchain. In Proceedings of the 2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dubai, United Arab Emirates, 1–5 May 2023; pp. 1–8.
45. Wrona, K.; Jarosz, M. Use of blockchains for secure binding of metadata in military applications of IoT. In Proceedings of the 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Limerick, Ireland, 15–18 April 2019; pp. 213–218.
46. Scott-Hayward, S.; Natarajan, S.; Sezer, S. A Survey of Security in Software Defined Networks. *IEEE Commun. Surv. Tutorials* **2016**, *18*, 623–654. [CrossRef]
47. YAN, G.; Wu, Q.; Chen, R.; Du, L.; Ren, S. A Literature Review of Resiliency Technologies in Military Software Defined Networks. In Proceedings of the 2022 5th International Conference on Data Science and Information Technology (DSIT), Shanghai, China, 22–24 July 2022; pp. 1–7.
48. Marcus, K.M.; Chan, K.S.; Hardy, R.L.; Yu, P.L. An Environment for Tactical SDN Experimentation. In Proceedings of the MILCOM 2018—2018 IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018; pp. 1–9.
49. Krishnan, R.; Babu, R.G.; Kaviya, S.; Kumar, N.P.; Rahul, C.; Raman, S.S. Software defined radio (SDR) foundations, technology tradeoffs: A survey. In Proceedings of the 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), Chennai, India, 21–22 September 2017; pp. 2677–2682.
50. Ulversoy, T. Software Defined Radio: Challenges and Opportunities. *IEEE Commun. Surv. Tutor.* **2010**, *12*, 531–550. [CrossRef]
51. Bergstrom, C.; Chuprun, S.; Gifford, S.; Maalouli, G. Software defined radio (SDR) special military applications. In Proceedings of the MILCOM 2002, Anaheim, CA, USA, 7–10 October 2002; Volume 1, pp. 383–388.
52. Jiao, H.; Liu, H.; Wang, Z. Reconfigurable Intelligent Surfaces aided Wireless Communication: Key Technologies and Challenges. In Proceedings of the 2022 International Wireless Communications and Mobile Computing (IWCMC), Dubrovnik, Croatia, 30 May–3 June 2022; pp. 1364–1368.
53. Jiang, W.; Ren, Z.; Huang, K.; Yang, J.; Chen, Y.; Sun, X. A Joint Space-Frequency Anti-jamming Scheme Based on Reconfigurable Intelligent Surface. In Proceedings of the GLOBECOM 2022—2022 IEEE Global Communications Conference, Rio de Janeiro, Brazil, 4–8 December 2022; pp. 6408–6414.
54. Zhou, W.; Zhang, R.; Chen, G.; Wu, W. Integrated Sensing and Communication Waveform Design: A Survey. *IEEE Open J. Commun. Soc.* **2022**, *3*, 1930–1949. [CrossRef]
55. Feng, Z.; Fang, Z.; Wei, Z.; Chen, X.; Quan, Z.; Ji, D. Joint radar and communication: A survey. *China Commun.* **2020**, *17*, 1–27. [CrossRef]

56. Zhang, J.A.; Rahman, M.L.; Wu, K.; Huang, X.; Guo, Y.J.; Chen, S.; Yuan, J. Enabling Joint Communication and Radar Sensing in Mobile Networks—A Survey. *IEEE Commun. Surv. Tutorials* **2022**, *24*, 306–345. [CrossRef]
57. Akan, O.B.; Arik, M. Internet of Radars: Sensing versus Sending with Joint Radar-Communications. *IEEE Commun. Mag.* **2020**, *58*, 13–19. [CrossRef]
58. Hoydis, J.; Aoudia, F.A.; Valcarce, A.; Viswanathan, H. Toward a 6G AI-Native Air Interface. *IEEE Commun. Mag.* **2021**, *59*, 76–81. [CrossRef]
59. Baeza, V.M.; Armada, A.G. Orthogonal versus Non-Orthogonal multiplexing in Non-Coherent Massive MIMO Systems based on DPSK. In Proceedings of the 2021 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Porto, Portugal, 8–11 June 2021; pp. 101–105.
60. Baeza, V.M.; Armada, A.G. Performance and Complexity Tradeoffs of Several Constellations for Non Coherent Massive MIMO. In Proceedings of the 2019 22nd International Symposium on Wireless Personal Multimedia Communications (WPMC), Lisbon, Portugal, 24–27 November 2019; pp. 1–6.
61. Baeza, V.M.; Armada, A.G. Analysis of the performance of a non-coherent large scale SIMO system based on M-DPSK under Rician fading. In Proceedings of the 2017 25th European Signal Processing Conference (EUSIPCO), Kos, Greece, 28 August–2 September 2017; pp. 618–622.
62. Baeza, V.M.; Armada, A.G. User Grouping for Non-Coherent DPSK Massive SIMO with Heterogeneous Propagation Conditions. In Proceedings of the 2021 Global Congress on Electrical Engineering (GC-ElecEng), Valencia, Spain, 10–12 December 2021; pp. 26–30.
63. Baeza, V.M.; Armada, A.G.; Zhang, W.; El-Hajjar, M.; Hanzo, L. A Noncoherent Multiuser Large-Scale SIMO System Relying on M-Ary DPSK and BICM-ID. In Proceedings of the 2021 Global Congress on Electrical Engineering (GC-ElecEng), Valencia, Spain, 10–12 December 2021; pp. 26–30.
64. Baeza, V.M.; Multiuser Non Coherent Massive Mimo Schemes Based on Dpsk for Future Communication Systems. Ph.D. Thesis, Universidad Carlos III de Madrid, Getafe, Spain, 2019.
65. Yang, Y.S.; Kim, Y. Recent Trend of Neuromorphic Computing Hardware: Intel's Neuromorphic System Perspective. In Proceedings of the 2020 International SoC Design Conference (ISOCC), Yeosu, Republic of Korea, 21–24 October 2020; pp. 218–219.
66. Mihai, S.; Yaqoob, M.; Hung, D.V.; Davis, W.; Towakel, P.; Raza, M.; Karamanoglu, M.; Barn, B.; Shetve, D.; Prasad, R.V.; et al. Digital Twins: A Survey on Enabling Technologies, Challenges, Trends and Future Prospects. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 2255–2291. [CrossRef]
67. Liu, Z.; Meyendorf, N.; Mrad, N. The role of data fusion in predictive maintenance using digital twin. In Proceedings of the 44th Annual Review of Progress In Quantitative Nondestructive Evaluation, Provo, Utah, USA, 16–21 July 2017; Volume 37.
68. Liu, S.; Zhu, X.; Chen, H.; Han, Z. Secure Communication for Integrated Satellite–Terrestrial Backhaul Networks: Focus on Up-Link Secrecy Capacity Based on Artificial Noise. *IEEE Wirel. Commun. Lett.* **2023**, *12*, 1369–1373. [CrossRef]
69. Wang, P.; Di, B.; Song, L. Multi-layer LEO Satellite Constellation Design for Seamless Global Coverage. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain, 7–11 December 2021; pp. 1–6.
70. Wang, Q.; Zhang, H.; Wang, J.B.; Yang, F.; Li, G.Y. Joint Beamforming for Integrated Mmwave Satellite-Terrestrial Self-Backhauled Networks. *IEEE Trans. Veh. Technol.* **2021**, *70*, 9103–9117. [CrossRef]
71. Mendoza, F.; Ferrús, R.; Sallent, O. SDN-based traffic engineering for improved resilience in integrated satellite-terrestrial backhaul networks. In Proceedings of the 2017 4th International Conference on Information and Communication Technologies for Disaster Management (ICT-DM), Munster, Germany, 11–13 December 2017; pp. 1–8.
72. Baeza, V.M.; Ha, V.N.; Querol, J.; Chatzinotas, S. Non-coherent massive MIMO integration in satellite communication. In Proceedings of the 39th International Communications Satellite Systems Conference (ICSSC 2022), Stresa, Italy, 18–21 October 2022; Volume 2022, pp. 200–205.
73. 3rd Generation Partnership Project (3GPP) Standardization, Technical Report. TR38.811: Study on New Radio (NR) to Support Non-Terrestrial Networkss. Technical Specification in 3GPP, Group Radio Access Network. Release 15, 2020. Available online: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3234 (accessed on 7 October 2023).