Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

Review

Synergy Between 6G and AI: Open Future Horizons and Impending Security Risks

Elias Yaacoub

Computer Science and Engineering Department, Qatar University, Doha, Qatar
E-mail: eliasy@ieee.org

Received: 5 May 2023; **Revised:** 22 May 2023; **Accepted:** 25 May 2023

Abstract: This paper explores the potential synergies between 6G and AI, arguing that their combination has the power to unlock new horizons by addressing future challenges in healthcare, transportation, virtual reality, education, resource management, robotics, public safety, and warfare. However, these opportunities also come with greater risks. Therefore, the paper provides an overview of the security risks and challenges associated with this convergence, as well as possible mitigation techniques.

Keywords: 6G, artificial intelligence (AI), Internet of things (IoT), Internet of nano-things (IoNT), security

1. Introduction

With the standardization of 5G becoming a reality, research into 6G is rapidly accelerating [1–6]. 5G identified three primary use cases [7]: Enhanced Mobile Broadband (eMBB), which involves increased human traffic on the network due to the widespread use of multimedia, gaming, and virtual reality (VR) services; Massive Machine-Type Communications (mMTC), which primarily deals with machine traffic over the network and is necessary to accommodate the billions of sensors and actuators deployed under the Internet of Things (IoT) paradigm; and Ultra-Reliability and Low-Latency Communications (URLLC), which is focused on highly critical services that are intolerant to delays, such as remote surgery.

6G, which is more than just "5G on steroids", relies heavily on the use of artificial intelligence (AI) [1,2]. In fact, as shown in Figure 1, beyond simply taking the 5G use cases to the next level, intelligence, fueled by AI, will be an integral part of 6G. Thus, if 5G marked the transition from “connected people to connected people and things”, 6G will lead to a transition “from connected people and things to connected intelligence” [1]. It should be noted that, although sensing is prominent in 5G networks through IoT deployments, it will be even more prevalent in 6G, as it will continuously feed the intelligence part of the network with real-time accurate data. For this reason, both sensing and intelligence are shown as new 6G use case scenarios in Figure 1(b). The synergy between AI and 6G is expected to open unprecedented future horizons. Not only will AI be extensively used in the network to optimize 6G performance, but 6G will also provide the necessary infrastructure for the explosive use of AI in almost every sector, including healthcare, transportation, and industry. New use cases, such as mobile broadband reliable low-latency communication (MBRLLC) and massive URLLC (mURLLC), will emerge from the combination of two or more of the 5G use cases [2,3].

These 6G use cases, along with advancements in AI, will unlock a range of novel services, such as Extended Reality (XR), Connected Robotics and Autonomous Systems (CRAS), and Human-Centric Services (HCS). The convergence of communications, computing, control, localization, and sensing (3CLS) enabled by the 6G-AI synergy will make these services possible [2]. In fact, 6G is expected to achieve unprecedented performance levels that exceed those of 5G by orders of magnitude, such as: Data rates in the order of Tbps,

DOI: https://doi.org/10.37256/cnc.1120232969

end-to-end delay less than 1 ms, communication in the Terahertz (THz) band, use of reconfigurable intelligent surfaces (RIS), integrated ground, airborne, and spaceborne networks, extremely high connection density and increased energy efficiency [1,2].

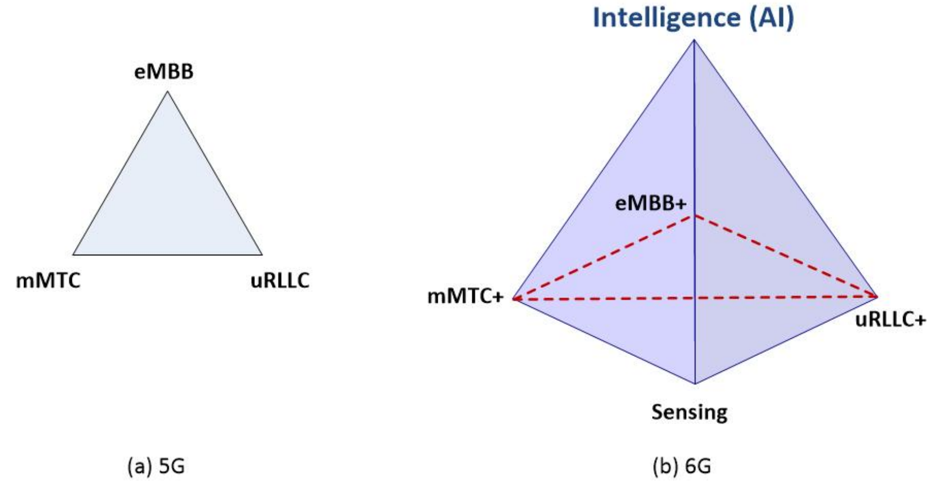

Figure 1. From 5G to 6G.

However, it is important to note that the deployment of adequate infrastructure to support these services is critical. While such infrastructure is mostly available in urban areas [8], significant connectivity gaps exist between these areas and rural areas in developing countries [9]. Global initiatives like "Basic Internet Connectivity" or "Global Access to the Internet for All (GAIA)" have emerged with the aim of bridging or at least reducing this gap by providing affordable broadband in these areas [10]. Although full-fledged 6G connectivity may not be achievable in these areas, several initiatives and techniques can be adopted to provide a certain degree of connectivity, thus leading to digital inclusion [11]. These techniques, mostly relying on satellite and unmanned aerial vehicle (UAV) platforms [5,6,12], are aligned with the United Nations' (UN) Sustainable Development Goals (SDGs) [4]. The human-centric aspect of 6G was also stressed in [13].

There are several surveys related to 6G, including the use of AI, e.g., [13–16]. However, most of the existing surveys focus on the technical aspects of 6G deployment and the use of AI in 6G. Despite the necessity of having these surveys and the value of the technical information therein, there is a need to complement the existing works with a higher-level overview strengthening the link between their technical contributions and the real-world scenarios and applications that can be unlocked with the successful deployment of 6G and AI. This article aims to address this problem, by providing a unique perspective on the potential applications of the 6G and AI synergy, as well as the security risks associated with it. The main contributions of this paper can be summarized as follows:

i. Analyze the related literature by grouping the relevant works into seven major application areas, called "Horizons" in this paper, that showcase the promise of the synergy between 6G and AI,
ii. Then, after showing the promising avenues of the synergy between 6G and AI, we turn our attention into the risks that accompany the combination of these technologies, and discuss the main challenges and threats that might hinder the success of the 6G/AI synergy, along with potential solutions, and
iii. Afterwards, we discuss future research directions that could build on the achievements of the existing literature in order to reach a better 6G/AI synergy in the future.

The paper is structured into four main sections. Section 2 discusses the open horizons that can be enabled with the 6G and AI synergy, which were previously thought to be only possible in science fiction. This section highlights the potential impact of 6G and AI on various sectors, including healthcare, transportation, virtual reality, education, resource management, and robotics, in addition to public safety and warfare. In Section 3, the security risks associated with the deployment of 6G and AI are analyzed, along with possible mitigation techniques. This section provides an overview of the potential threats and vulnerabilities that can arise with the use of AI and 6G technologies and emphasizes the need for robust security measures to protect against them. Then, Section 4 provides a discussion recapitulating the concepts surveyed in the previous two sections, and indicates open challenges and fertile areas for future research. Finally, Section 5 concludes the paper by summarizing the key findings and highlighting the importance of considering both the potential benefits and risks associated with the 6G and AI synergy. Overall, this paper provides valuable insights into the potential impact of 6G and AI on various sectors, while also emphasizing the need for careful consideration of security risks and mitigation techniques.

2. Horizons

This section describes some important new horizons unlocked by the synergy between 6G and AI. The focus is on seven main topics, shown in Figure 2, that are attracting significant research interest, and are expected to do so in the near future.

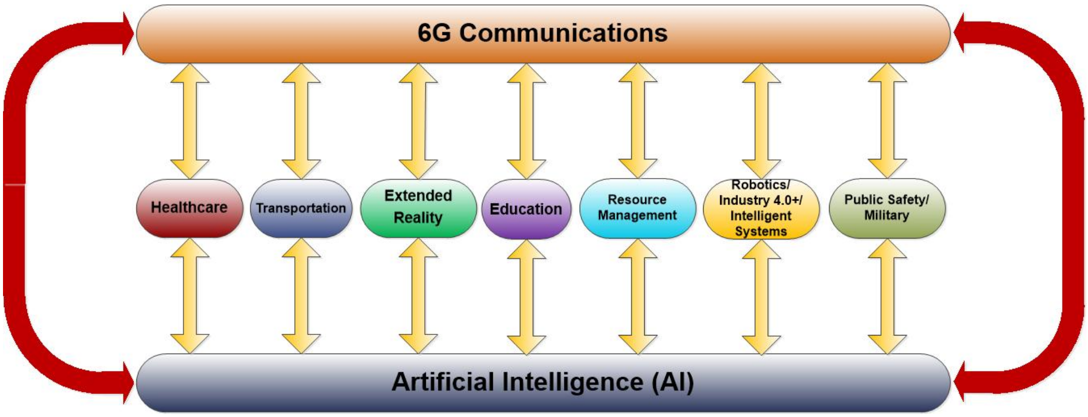

Figure 2. Main topics discussed in this paper, unlocked by the 6G-AI synergy.

2.1 *Healthcare*

The integration of 6G and AI with mobile health techniques can lead to significant advancements in healthcare and ambient assisted living. Wearable sensors can collect data, which can be processed, analyzed, stored, and exploited using edge/cloud techniques and AI. This can be used to monitor patients, detect illnesses/anomalies, and notify medical response teams accordingly [17]. With 6G and AI, continuous measurements of health parameters and vital signs can be used to generate a "digital twin" of the monitored person. Advanced AI techniques can perform heavy computations to identify any illnesses or provide recommendations on a healthier lifestyle to increase the longevity of the person [18]. The "digital twin" can also be used for virtual testing and simulations of risky surgeries before attempting them on the actual patient.

The Internet of Nano-Things (IoNT) can be used for more extensive and accurate measurements of health parameters and vital signs, especially with the use of nano-devices or nano-nodes, nano-routers, nano-controllers, and gateways. The IoNT mainly uses two communication types, namely nano scale communications using electromagnetic waves, mostly terahertz communications, and molecular communications based on the exchange of molecules in the body [19–22]. While molecular communications are slower and subjected to various biological parameters that can affect them, they can still be used for secure communication with appropriate security mechanisms. Channel models have been investigated for the propagation of electromagnetic signals in the blood, making it easier to design security schemes for IoNT in the human body [21]. Figure 3 shows an example of the deployment and interaction between the various IoNT devices.

Securing communications between nodes and routers/controllers in IoNT is a challenging task. While physically accessing the nodes is difficult, compromising the router or controller can lead to serious threats such as control over the nano-sensors/actuators. This could cause network malfunction or communication disruption and even affect the life of the patient. Traditional security methods used for IoT can be applied to secure communications between controllers and gateways [17,23,24]. However, innovative approaches are needed to secure communications between the nodes, routers, and controllers [25–27].

In terms of cloud security, federated learning (FL) can be used to protect patient privacy assuming zero trust. This involves transmitting the weights of the machine learning (ML) system instead of transmitting the actual data. In fact, with FL, training is performed at the “edge”, where copies of the machine learning model are kept with each device. Then, these devices transmit the weights of their models to the cloud server, instead of transmitting the whole data. The server can then combine the weights of these “local” models to obtain a “global” model that can be shared again with the edge devices, who can retrain it to enhance performance, and so on. Thus, FL preserves privacy by not transmitting the actual user data, as the server only aggregates the weights received without knowledge of the actual measurements or sensor readings [28].

However, this method requires the presence of intelligence at the edge to perform training and may not be applicable when creating a digital twin at the cloud. Additionally, measures need to be taken to identify and mitigate the effect of malicious nodes that send fake weights to tamper with the server's results communicated to legitimate nodes [28].

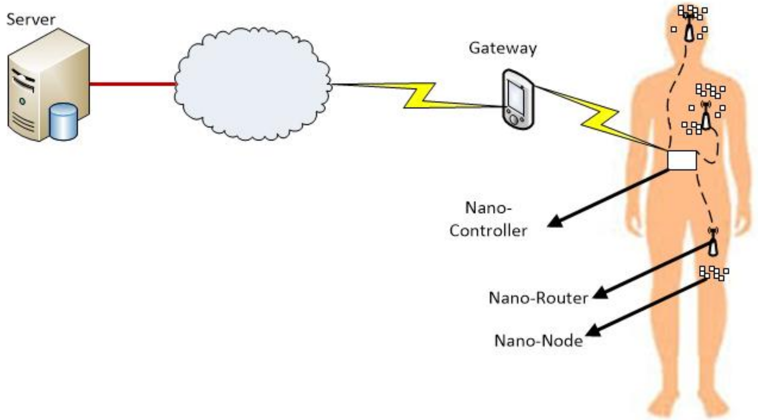

Figure 3. IoNT devices in a health scenario. Terahertz communication used between nano-nodes is one of the key technologies investigated in 6G.

2.2 *Transportation*

The advances in intelligent transportation systems have been extensively studied in the research literature of the last two decades [29–31]. Connected cars, V2X connectivity, and self-driving cars are among the technologies that have been investigated. The synergy between AI and 6G is expected to take this research to the next level, allowing for large-scale adoption of these technologies.

In fact, better AI leads to safer and more efficient self-driving cars/vehicles. With 6G connectivity, these self-driving vehicles can communicate faster and respond with ultra-low latency to emergency events, enabling better road safety. Once legal and psychological concerns are overcome, this would allow for vast adoption of self-driving cars and autonomous vehicles.

Furthermore, this could give rise to new business models. For instance, instead of having their self-driving car locked in a parking lot, an owner can put it to better use and earn money. The car can be rented out or used as a taxi (similar to a driverless Uber) to carry passengers while the owner stays at home. Hence, cars can generate revenue for their owners when they are not using them [32]. Ordering and dispatching of cars would be done through 6G connectivity, whereas AI can be used to optimize trajectories, locate the nearest car that fits specific passenger criteria, alert the owner for preventive maintenance, among other things.

Similarly, this technology could revolutionize supply chains and delivery networks. Self-driving trucks could be sent on optimized routes by a central AI, with their position monitored in real-time, and their cargo unloaded by waiting robots at destination warehouses. With 6G connectivity, every single item can be tracked throughout the process. This approach is also expected to be applied to boats (autonomous shipping) [30,33].

However, as mentioned earlier, legal and psychological challenges still need to be addressed. For example, some people may prefer to have control while in a self-driving car and not feel safe otherwise. Also, if a self-driving car causes an accident, who will be held legally responsible - the car owner, the car manufacturer, or the car itself? Nevertheless, advances in AI and 6G connectivity are expected to minimize the risk of accidents, optimize traffic routes, and increase the revenues of car owners (while disrupting the taxi industry).

2.3 *XR*

The advancements in 6G and XR technology have the potential to revolutionize virtual meetings and encounters, making them feel more realistic than ever before. The real-time MBRLLC 6G capabilities will enhance the virtual environment, while haptics and holograms can make virtual handshakes and romantic encounters feel more authentic. Natural language processing (NLP) can also allow for immediate translation, allowing participants speaking different languages to communicate seamlessly [34].

The integration of AI and digital twin techniques can also be used to create holograms of deceased loved ones, with their avatars summoned from the cloud where their digital twin is stored [35]. In healthcare, digital twins can be used to help surgeons practice complex and risky surgeries multiple times on the patient's digital twin before performing it on the actual patient (as illustrated in Figure 4). Additionally, vital signs monitoring of the surgeons can ensure that they are not too stressed while performing the surgery.

Despite the potential benefits of these technologies, it should be noted that there may be ethical concerns surrounding their use in some of the above application areas, and it is important to carefully consider these issues before implementing such technologies.

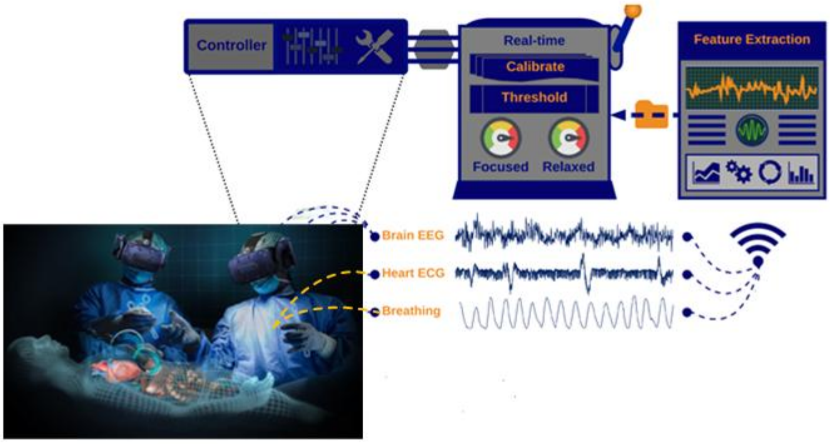

Figure 4. Example of surgeons practicing surgery on a digital twin using virtual reality.

The tourism industry can benefit tremendously from such advances in augmented reality. For example, a visit to a historical castle can be augmented by “meeting” avatars of the inhabitants who lived there centuries ago. Moreover, one can have virtual tours or virtual “trips” from the comfort of their home, where VR would allow them to be immersed in the destination of their choice before deciding to make the actual trip [36]. Advances in haptics and e-touch/e-smell, coupled with 6G MBRLLC communications, can allow even having a taste of the local cuisine, or enjoying the aroma of local flowers, for example. Similarly, with 6G, haptics, and XR, people can attend an event or concert without physically being there. The entertainment industry could thus have different types of tickets for physical and virtual attendance.

XR is also expected to revolutionize the retail industry. Shopping can be done at home, where an immersion in a virtual shop allows a shopper to try dresses on her avatar, which has similar body measurements calculated from IoT wearable sensors. With 6G connectivity, a literal “blink” in the head mounted display or VR glasses allows the purchase to be made, the payment being charged to the shopper’s credit card, and a drone can deliver the product the next day at the shopper’s doorstep [37].

However, as with any emerging technology, there are ethical considerations that must be taken into account. For instance, there may be concerns about the psychological effects of spending extended periods of time in virtual environments, and the potential for addiction. Additionally, the impact on privacy and data protection needs to be considered, as the use of XR may involve the collection and processing of sensitive data. It is important to address these concerns through responsible development and implementation of XR technologies [38].

2.4 *Education*

The advances in technology will allow classrooms of the future to bypass traditional education systems and learning techniques. The adoption of modern, digitally-enriched techniques will enable students to learn more efficiently and be better equipped to face modern challenges, and contribute to society and the economy [39]. In addition to the now-common use of tablets, laptops, and interactive boards, the adoption of VR/AR applications will be essential in these enhanced education systems. In addition, XR can play a significant role in education, by providing immersive and interactive learning experiences. Students can visit historical sites or participate in lab experiments through virtual simulations, and teachers can create personalized and engaging content for their students. This can lead to better retention of knowledge and improved learning outcomes [39].

Beyond the use of VR/AR techniques as a learning tool, they can also be used to increase students' attention and concentration levels. Electroencephalography (EEG) headsets have evolved and now mostly use non-invasive electrodes, and the brain signals they measure are transmitted wirelessly without the use of cumbersome wires. Furthermore, they can be used in conjunction with VR headsets in a combined and integrated fashion (e.g., [40]). With edge processing, there is no need to transmit the EEG signals themselves. They can be processed locally and analyzed with adequate AI algorithms, and only the values of the metrics related to focus/attention/concentration could be sent to the teacher [41].

With this technology, biofeedback, or more specifically NeuroFeedback (NFB) in the case of EEG, can be implemented. Using EEG NFB, brain waves are measured, and a feedback signal (generally an audio-visual signal) is provided through the VR headset to train subjects to increase their concentration and focus levels, for example [42]. Using this technology, the learning process can be significantly enhanced. Less-performing students could be identified and receive the needed assistance. Moreover, electrocardiography (ECG) signals could be used to detect the stress levels [43] of the students during exams or during the explanation of challenging material. ECG is the process of recording the electrical activity of the heart over a period of time using electrodes placed on the skin. Recent advances with the photoplethysmography (PPG) technique allow measuring the heart rate without the need to place electrodes on the skin. This technique allows the detection of the pulse wave traveling through the body by detecting changes in the amount of blood in a specific body part using light transmission through tissue (e.g., a finger), and then capturing the light through a probe [44]. Simple techniques for measuring heart rate can now be performed using a smartwatch [45] or a smart ring [46]. Hence, ECG signals can be monitored through simple wearable devices, and the levels of stress can be reported back to the instructor. Figure 5 illustrates the scenario of immersive education with ECG measurement.

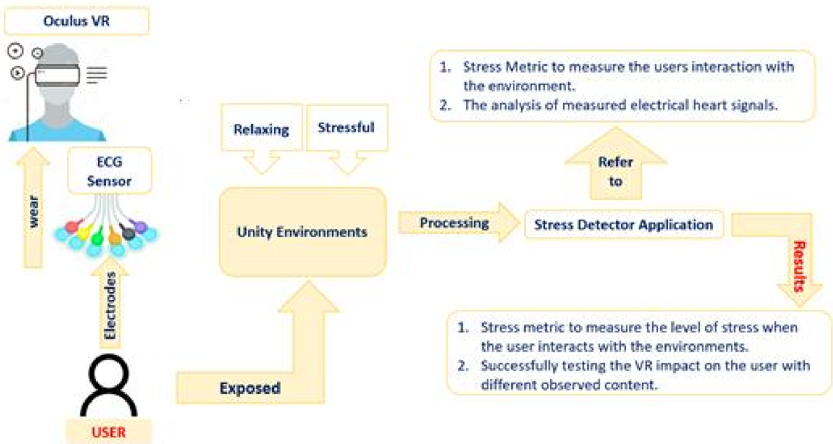

Figure 5. ECG measurement while the student is immersed in a VR educational environment.

Thus, 6G technology allows online education to be more pervasive, with support for VR/XR applications that provide a virtual classroom environment where students can attend class with avatars of their colleagues. In such an environment, AI, through the use of IoT for vital signs monitoring, can not only detect the engagement levels of students, but also adopt necessary measures through biofeedback. Depending on the EEG/ECG measurements, the educational content can be adapted to the needs of a particular student, or the teacher can intervene to take appropriate action and help increase the attention and/or reduce stress of certain students.

Although the current cost of some equipment needed for the above scenario is high, e.g., [40], it is expected to decrease with technological progress and market adoption. In addition, other less costly EEG devices using fewer electrodes, e.g. [47], can be considered as consumer electronics and are commercially available. These simplified EEG devices [47] can be used by students at home with a mobile application and NFB provided through music, in order to improve their concentration before studying. They can also be used in conjunction with a separate VR headset.

The approach described above can be used not only for education but also for employee training or continuous learning. In fact, one of the societal challenges due to exponential progress in technology is that innovation might destroy jobs in some sectors but create jobs in others. The challenge is to meet the demand for the skill sets required in the new jobs. Thus, employees should adopt a lifelong learning style, and educational systems should be reformed to cope with technological advances. The problem here is that low-skilled workers might be strongly affected, whereas medium-skilled workers would be better able to enhance their skills and move to jobs requiring higher skills. The educational enhancements discussed previously should allow the educational system to closely follow technological advances.

2.5 *Resource Management/Optimization*

This section describes the use of AI and 6G to optimize resource management, where "resource" is used in a very general sense and could refer to energy, water, oil and gas, or the resources of the 6G network itself [48].

In fact, not only 6G is serving AI to address the verticals discussed in this paper such as healthcare and transportation, but also AI is serving 6G to optimize the network performance. This can include radio resource management, network slicing, and optimized power consumption for green networking, among other issues [49–52]. As shown in Table 1, a variety of AI techniques are being applied to optimize the performance of 6G networks.

Table 1. Some Recent Contributions using AI/ML for 6G Resource Allocation and Management.

Reference	Learning Technique	Algorithm	Target Solution in 6G
[53,54]	Unsupervised Learning	K-Means Clustering	Resource allocation in uplink non-orthogonal multiple access (NOMA) with electromagnetic emission awareness
[55]	Unsupervised Learning	K-means and clustering algorithm perception decision-CAPD	Reducing non linearity in 6G visible light communications (VLC) systems
[56]	Supervised learning Unsupervised learning Reinforcement learning	Deep Neural Network Deep Q-Learning	Resource management for data rate maximization
[57,58]	Supervised learning Unsupervised learning Reinforcement learning	Deep Learning	URLLC Communications
[59]	Supervised learning Reinforcement learning	Deep Neural Network (DNN) Convolutional Neural Network (CNN)	Medium Access Control (Resource allocation and random access) in 6G
[60]	Reinforcement learning	Deep Reinforcement Learning	Resource provisioning for the Internet of everything (IoE)
[61]	Reinforcement learning	Deep Reinforcement Learning	Handover in 6G VLC
[62]	Reinforcement learning	Deep Q Network and Dueling Deep Q Network	Channel Monitoring
[63]	Reinforcement learning	Hierarchical deep actor-critic networks	Network Control and Resource Allocation for 6G Space-Terrestrial Integrated Network
[64]	Reinforcement learning	Deep reinforcement learning scheme with sequential actor-critic model	Reducing delay and error rate in URLLC
[65]	Reinforcement learning	Modified deep deterministic policy gradient (DDPG) and double deep-Q-network algorithm	Spectrum efficient network slicing in 6G
[66]	Reinforcement learning	Federated deep reinforcement learning and deep Q networks	Access and handover control in open radio access network (O-RAN)

These techniques range from deep reinforcement learning to fuzzy logic and convolutional neural networks. The problems addressed also vary from resource allocation and power control to green networking and network slicing. By optimizing these aspects of 6G networks, AI can help ensure the efficient use of resources and improve the overall performance of the network. This contributes to achieving the ambitious key performance indicators (KPIs) of 6G, listed in Table 2. Thus, the techniques listed in Table I are mainly based on using AI to help achieve the 6G KPIs of Table 2.

To address the conflicting requirements of the various use case scenarios shown in Figure 1, different network slices need to be planned to cater for the various quality of service (QoS) and quality of experience

(QoE) requirements of the different use cases and application scenarios. Thus, network slicing in 6G needs to be significantly more efficient than in 5G, and such advanced and complex resource provisioning cannot be properly performed without resorting to AI [65]. For example, two controllers are proposed in [65]: an upper-level controller adjusts the slice configuration based on the traffic dynamics, whereas a lower-level controller works within the slice configurations set by the upper-controller to perform radio resource allocation at each transmission time interval (TTI), thus orchestrating the resources to meet the target requirements.

Table 2. Main 6G KPIs [1, 2].

KPI	Value
Peak Rate	1 Tbps
Experienced Rate	10-100 Gbps
Device Density	10 million devices/km^2
Reliability	99.99999%
Latency	0.1 ms
Energy efficiency	100x with respect to 5G
Network Capacity	1000x with respect to 5G

In addition, the use of AI can also enable the development of new services and applications that can benefit from the capabilities of 6G. Indeed, the combination of 6G and AI has the potential to revolutionize resource management in various sectors, from energy and water distribution to environmental monitoring and agriculture [67–69]. The ability to gather massive amounts of data through the mURLLC use case and analyze it in real-time using AI can lead to more efficient resource use, better prediction and planning of network load, and optimized network expansion.

Moreover, the use of edge computing is essential in these techniques, as it allows for faster computation, reduced network bandwidth load, and increased energy efficiency. With edge computing, AI can seamlessly integrate with the network and become fully edge-native in 6G, thus enabling self-learning AI for edge-computing. This can lead to even more efficient and effective resource management in various fields [70].

2.6 *Robotics/Industry 4.0+/Intelligent Systems*

The permanent connection of robots to the cloud through highly reliable, continuously available 6G networks allows them to share their learning experiences. Hence, when a robot self-learns something, the knowledge is instantaneously shared with all connected robots, enabling these AI systems to evolve exponentially [38,71,72].

With XR, IoT, and 6G, intelligent systems can be run even more effectively. For instance, an IT technician can wear a VR headset and see a virtual representation of the network. They can navigate through an immersive environment where buildings represent servers and network equipment, and roads represent interconnections between them. This enables them to inspect configuration parameters or performance indicators of each device in the virtual world, making troubleshooting faster, easier, and more efficient [73].

Similarly, with the help of AI and digital twin techniques, the manufacturing industry can benefit from virtual simulations that can provide valuable insights into product design and development, and optimization of manufacturing processes. For example, engineers can collaborate on a design using holographic images, testing various prototypes in a virtual environment, and making changes in real-time. This can save significant time and resources, as well as improve product quality.

In addition, the electric grid or an oil and gas pipeline network can be rendered in a similar manner. Real-time parameters can be obtained from IoT sensors and reported in the virtual model for troubleshooting. Another approach is to combine real-time IoT readings with real images, allowing monitoring and troubleshooting teams to view a 3D version of a live video feed sent by a drone flying over an oil pipeline. In this immersive environment, augmented reality is used to overlay the readings of IoT sensors over the corresponding part of the pipeline, and engineers can see the pressure parameters, temperature, and other relevant data corresponding to each specific section. AI can be used to provide preventive maintenance by analyzing the collected and stored IoT data, identifying potential risks and requesting the drone flights to be directed towards corresponding zones.

2.7 *Public Safety/Military*

The mastery of AI and 6G is expected to lead to remarkable advances in military capabilities. The use of drones and UAVs can fundamentally change law enforcement operations and battlefield tactics. For instance, Figure 6 illustrates an example of how UAV swarms can form flying ad hoc networks (FANETs) to support ground troops equipped with IoT sensors, enabling device-to-device (D2D) communications. The FANETs could also offer 6G connectivity with satellites.

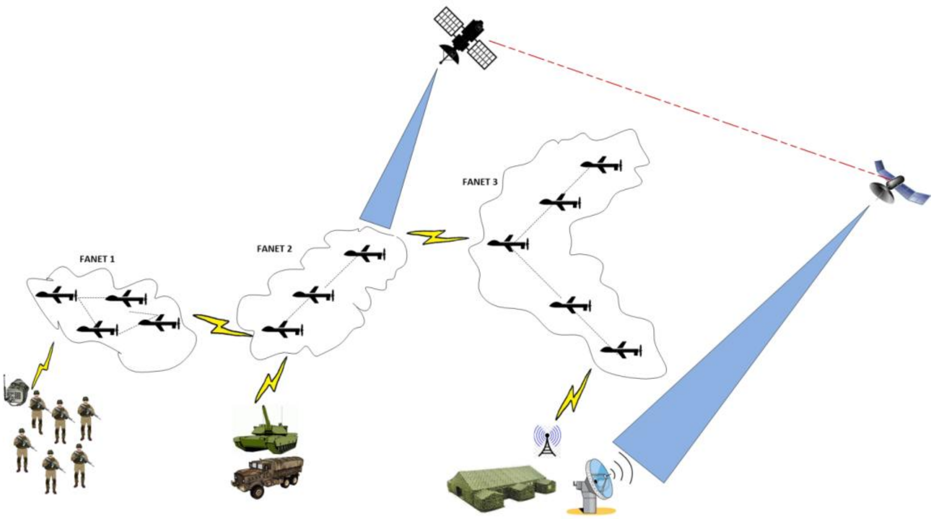

Figure 6. Military scenario with ground, UAV, and satellite communications.

Advances in robotics and AI can lead to the development of robot soldiers, limiting human casualties while inflicting more damage on the enemy. Militaries that use these advanced technologies will have a deterrent force that can tip the balance of power in their favor. On the optimistic side, the mere display of this power can stop unnecessary wars when used responsibly by governments [74]. However, on the pessimistic side, if this technology falls into the wrong hands, it can lead to dramatic consequences. For example, nano-drones in the form of robotic bees or flies can be used to track, find, and assassinate subjects [38]. Additionally, AI-optimized weapons in the hands of international terrorist organizations can cause devastating damage. Several prominent AI scientists and researchers have signed a petition to urge governments to refrain from supporting AI research in the military domain [38,74]. Despite their calls, success is not guaranteed, and even if governments comply, progress in communications and AI in civilian areas can be exploited by malicious groups for military purposes [74].

3. Risks

In Section 2, we analyzed the related literature by considering seven major application areas where the synergy between 6G and AI can open life-changing "Horizons" that could transform the way we live. However, the unprecedented pace at which AI is becoming pervasive, coupled with the connectivity opportunities provided by 6G, could lead to situations with undesirable consequences [38]. Thus, after showing the promising avenues of the synergy between 6G and AI in Section 2, we turn our attention in this section to the risks that accompany the combination of AI and 6G. We discuss the main challenges and threats that might hinder the success of the 6G/AI synergy, and outline potential solutions.

In fact, the opportunities and future horizons discussed in the previous section provide a large target base for a wide range of security attacks and vulnerabilities. While AI techniques can be used to detect and mitigate security vulnerabilities and intrusions, advances in AI can also be utilized to perfect attacks targeting the systems described above. As such, AI can be a double-edged sword that can be used for both offense and defense [75,76].

3.1 *Malware and Attacks*

Traditional malware and attacks are expected to continue to exist even after the proliferation of 6G and AI. Viruses, worms, Trojan horses, denial-of-service (DoS) attacks, distributed DoS (DDoS) attacks, and other similar attacks will remain prevalent. The progress in cybersecurity research and innovative countermeasures will help to limit their occurrence probability. However, if they succeed, their impact and the damage they cause will be devastating and orders of magnitude larger than their current level of damage [75].

For instance, IoNT devices are vulnerable to severe threats, such as a lack of encryption, susceptibility to denial-of-service attacks, malware, and other types of cyber-attacks. Bio-cyber attacks over IoNT networks can be exploited to steal personal health-related information, and viruses can be utilized to hack deployed IoNT to cause serious health risks. Controlling the routers and/or controllers in a medical IoNT network could lead to using them for regulating the nano-sensors/actuators, which could result in network malfunction or communication disruption, and could also impact the life of the patient by altering the operation of these devices in the biological environment [25–27]. This is a form of bio-cyber terrorism that not only steals personal health information but could also result in murder.

Therefore, innovative and efficient methods are required to ensure the confidentiality, integrity, and availability of data. These methods could include:

- Efficient key management and distribution techniques between gateways, nano-controllers, and nano-routers to perform symmetric encryption quickly and efficiently, with reasonable computational overhead. A potential solution could be the use of quantum key distribution between the server and gateway, which would then handle the transmission of the generated keys of Terahertz wireless channels to the controllers and routers.
- Physical layer security techniques to add an extra layer of security. This includes investigating physical layer techniques as an add-on to encryption at the nano-routers and controllers, and as a substitute for encryption at the nano-nodes - router links. In fact, for this latter scenario, the limited capabilities of the node make this approach desirable. However, implementing this technique within a biological propagation environment would be challenging. A more challenging and novel scenario would be to use molecular communications as an additional protection layer, in conjunction with security measures at the terahertz wireless level.
- AI-based techniques for intrusion detection and mitigation of denial-of-service attacks targeting the gateway, controllers, or routers. As mentioned previously, any breach at this level can allow the malicious attacker to control the nano-nodes and cause severe damage.

As another example, hacking the control system of the power grid could lead to system instability [77] and potentially plunge entire nations into darkness. On a smaller and less dramatic scale, hacking smart meters could lead to scenarios where a person's power consumption is billed to their neighbor.

In the self-driving cars scenario, the cars would be expected to be connected to cloud servers (or some remote servers of their manufacturer) for software upgrades, preventive maintenance, etc. A breach in these servers could allow the hacker to remotely control millions of cars at the other end of the world. Imagine a scenario where empty cars are swarming in the streets, closing major road intersections, blocking movement, while being controlled by an unknown malicious user.

The previous examples demonstrate the significance of integrating security measures into the design of AI and 6G systems and providing the option to revert to more primitive techniques in case of a disaster. This could involve, for instance, allowing drivers to return to manual mode by disconnecting the cars (e.g., pressing a special button) or disconnecting the power grid from the telecom network and using manual techniques to route the power through the distribution networks. This necessitates the need to have employees trained in the “old ways” in addition to the more tech savvy ones running the “intelligent” grid.

3.2 *Eavesdropping/Jamming*

These physical layer techniques are expected to become more efficient in the 6G/AI era [78]. However, the strong reliance on small IoT devices presents an obvious weakness [79,80]: Due to their limited capabilities, these devices cannot resist strong jamming attacks. These attacks could, for example, disable the operation of actuators in a medical IoNT network, thus disrupting medicine delivery to patients. Moreover, the reliance of IoT sensors to relay all kinds of measurements makes it possible for an eavesdropper to gain valuable information. It should be noted that eavesdropping in certain scenarios, such as the IoNT nano-sensors, is difficult since the devices have weak power capabilities, and an eavesdropper would have to be physically present near the patient to capture meaningful data.

In general, physical layer techniques could be used to mitigate these attacks, e.g., noise injection to combat eavesdropping or beamforming (whenever supported by the devices) to mitigate jamming, and generation of encryption keys by relying on physical channel parameters, such as channel state information [79]. Moreover, hybrid techniques involving the use of encryption and more traditional security methods, in conjunction with physical layer techniques, can be used to mitigate such attacks. Quantum key distribution, although not supported by small IoT devices, could be used by routers/controllers to provide strong cryptographic keys for IoT devices, as discussed in the next section [81].

3.3 *Quantum Computing*

The progress in quantum computing, while generally beneficial to AI techniques for accelerating computations, also presents a challenge as it provides an advantage to malicious attackers trying to detect encryption keys. Thus, it is crucial to design encryption techniques that can withstand quantum attacks. Unfortunately, the widespread deployment of IoT devices exacerbates this challenge [82,83].

One potential solution is to utilize quantum key distribution (QKD) by the IoT controllers. As more powerful devices, they can establish a fiber optic connection to servers in addition to using traditional radio frequency (RF) wireless connection. They can leverage the optical connection to generate quantum keys using photons, and distribute these keys to IoT devices over the local wireless connection using a secure distribution architecture or protocol. This process should be repeated periodically to avoid the risk of using the keys for too long and compromising the communications [81].

Furthermore, AI techniques can be employed to detect quantum attackers performing man-in-the-middle attacks to intercept the quantum keys being exchanged during QKD [81].

3.4 *Zero Trust*

In the open radio access network (ORAN) of 5G+/6G, a zero-trust architecture is employed. This requires security measures that operate under the assumption that the attacker is already inside the organization or network [78]. Given the billions of connected devices, cloud access, and critical data being circulated, processed, and analyzed in today's and future networks, frequent authentication is essential for users, applications, and infrastructure devices. In addition to confidentiality, integrity, and authentication, this raises the issue of trustworthiness, which must be continuously monitored in real-time according to certain metrics for each device in the network [34,78,84]. Thus, every operation must be logged appropriately for further inspection. This can be done continuously using appropriate AI techniques to detect any threats or through digital forensics techniques after an incident has occurred.

3.5 *Blockchain*

Blockchain has garnered significant interest in privacy and security research, in addition to its role in virtual currencies. As a result, it has been proposed for providing privacy and security in 6G networks [85–87]. Blockchain is being applied in a wide range of 6G-related security research, from securing edge data [86], to securing the 6G access network itself [87], and to vertical sectors such as healthcare, Industry 4.0+, and environment monitoring [85].

However, despite 6G providing the required connectivity for blockchain traffic, several challenges are being either ignored or at least underestimated by most of the literature. For instance, will blockchain's scalability hold up with millions of transactions? Since the blocks are hashed and interconnected, how long would it take to retrieve and decrypt a specific transaction if one had to go all the way back through the chain to reach it? Shorter chains may solve this problem, but they may also reduce the security of the blockchain approach. Additionally, the energy required for transaction validation, similar to bitcoin mining, is significant. The consumption and cost will increase as more nodes are added to the blockchain [88]. In fact, the energy needs of blockchain, coupled with its sensitivity to energy prices and availability, e.g., during the crisis in Kazakhstan at the beginning of 2022 [89], should raise some concerns about the large-scale adoption of blockchain in 6G.

4. Discussion and Future Research Directions

In this paper, the synergy between 6G and AI was investigated, and the related security risks were analyzed. With the proliferation of AI and the abundance of data generated through ubiquitous sensing (see Figure 1(b), as this trend will be exacerbated as 6G nears deployment), the trend for AI algorithms is to become more independent. They have to learn from the environment and adapt dynamically. Therefore, reinforcement learning (RL) techniques, already very popular in research literature, are expected to continue gaining popularity and research interest. Table 1 provided a summary of some recent references using RL for optimizing the performance of 6G networks. However, RL can be used in any of the "Horizons" discussed in Section 2 of this paper. Therefore, Table 3 provides a brief summary of recent papers, e.g., [90–104], using RL in the various application areas studied in this paper.

In addition, it should be noted that each of the application areas discussed in Section 2 of this paper is a hot research area by itself, especially when AI, sensing, and 6G connectivity are used to solve the problems inherent in that area, and thus unlock its future horizons. Moreover, emerging areas that combine one or more of these seven areas are gaining increasing research interest. For example, Metaverse applications are gaining increased popularity. They rely extensively on XR, need stringent QoE requirements that must be provided by 6G networks, are enriched by continuous and ubiquitous sensing (to make the immersive environment more engaging and realistic), and depend heavily on AI. In fact, their high computational requirements necessitate a judicious balance between edge and cloud intelligence, where the 6G/AI synergy discussed in this paper will play a primordial role [105].

Table 3. Summary of Some Recent Papers Using RL Algorithms for various Application Areas.

References	Learning Technique	Application Area/"Horizon"	Summary/Main Topics
[28,90,91]	Federated Learning, Reinforcement learning	Healthcare	Overview of different federating learning types [90]; Survey of attacks on federated learning and potential solutions [91]; investigating stability under Byzantine attack [28].
[29,33,92,93]	Deep Learning, Reinforcement learning	Transportation	Survey of machine learning techniques for Vehicular Ad-hoc Networks (VANETs) [29]; Trajectory prediction [33]; Training to allow self-driving cars to avoid pedestrians [92]; using deep reinforcement learning for self-parking [93].
[35,94,95]	Reinforcement learning	XR	Using RL for adapting the behavior of avatars in the metaverse to the needs of a given user [35]; Using RL for offloading computing resources to mobile edge servers [94]; or for adapting metaverse multimedia traffic to network conditions [95].
[96–98]	Supervised Learning Reinforcement learning	Education	Using RL for enhancing the quality of experience for online educational multimedia traffic [96]; Using regression and other machine learning techniques for detecting relaxation or stress during immersion in virtual environments, with applications to online education [97,98].
[56–66]	Reinforcement learning	6G Resource allocation	Refer to Table 1 for details: 6G Resource allocation, network management, handover
[99–101]	Reinforcement learning	Robotics/Smart Systems	Using RL to train robots for human-robot collaborative tasks [99]; or for other social interactions with humans [100]; Using RL to allow robots to explore unknown environments, e.g., during search and rescue operations in disaster areas [101];
[101–104]	Reinforcement learning	Military/Public Safety	RL for autonomous exploration of unknown areas by autonomous vehicles [101]; RL for decision making by unmanned combat aerial vehicles (UCAVs) [102,103], or for missile strike target assignment [104].

Hence, future research directions are expected to continue using AI to optimize the performance of 6G networks and in the use of 6G-AI synergy to achieve further progress in the various vertical areas discussed in the paper, such as healthcare, transportation, and education. However, a significant barrier to achieving the future horizons discussed in this paper is not technical limitations, which are generally being overcome, but rather the widespread acceptability of the role of AI in our lives. For example, it will be challenging for a patient or a physician to accept a decision made by AI in a healthcare monitoring scenario based only on the data without a convincing reason or demonstration of symptoms. Similarly, psychological barriers (more than technical ones) need to be overcome before seeing the wide adoption of driverless taxis or airplanes. Therefore, more efforts need to be devoted, in addition to the existing ones, to conduct further research on areas such as "explainable AI," "ethical AI," "justifiable AI," in addition to the legal aspects of AI, so that a certain level of maturity is reached in these areas before, or at least in parallel to, the future widespread deployment of 6G [38,106].

5. Conclusions

In this paper, we complemented the existing works on AI and 6G by providing a high-level overview linking the technical concepts with the real-world scenarios and applications that can be unlocked with the successful deployment of 6G and AI. Thus, we provided a unique perspective on the potential applications of the 6G and AI synergy, as well as on the security risks associated with this synergy. First, we analyzed the related literature by grouping the relevant works into seven major application areas, notably: healthcare, transportation, virtual reality, education, resource management, robotics, in addition to public safety and warfare, and discussing how these areas are shaped by the joint use of 6G and AI. Then, after discussing the promising future horizons unlocked by the synergy between 6G and AI, we analyzed the risks accompanying this 6G/AI synergy, and discussed the main challenges and threats, and we proposed potential solutions to mitigate them. Finally, we discussed future research directions, and argued that research in the areas of explainable AI and ethical AI should be given higher priority, in order to balance the permeation of AI into all aspects of human life. This becomes even more important as the Metaverse becomes a reality, and the boundaries between the real and virtual worlds get more blurred.

Acknowledgments

This publication was jointly supported by Qatar University and IS-Wireless - IRCC Grant no. IRCC-2021-003. The findings achieved herein are solely the responsibility of the author.

Conflict of Interest

There is no conflict of interest for this study.

References

[1] Huawei Technologies. 6G: The Next Horizon - From Connected People and Things to Connected Intelligence. White Paper, 2021. Available online: https://www-file.huawei.com/-/media/corp2020/pdf/tech-insights/1/6g-white-paper-en.pdf?la=en (Accessed on 26 May 2023).

[2] Saad, W.; Bennis, M.; Chen, M. A Vision of 6G Wireless Systems: Applications, Trends, Technologies, and Open Research Problems. *IEEE Netw.* **2019**, *34*, 134–142, https://doi.org/10.1109/mnet.001.1900287.

[3] RF Wireless World. 5G vs. 6G: Difference between 5G and 6G. 2020. Available online: https://www.rfwireless-world.com/Terminology/Advantages-and-Disadvantages-of-6G-Wireless-Technology.html (Accessed on 26 May 2023).

[4] Latva-aho, M.; Leppänen, K. Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence. White Paper, 6G Research Visions 1, 6G Flagship. Available online: https://www.6gflagship.com/key-drivers-and-research-challenges-for-6g-ubiquitous-wireless-intelligence/ (Accessed on 26 May 2023).

[5] Giordani, M.; Zorzi, M. Non-Terrestrial Networks in the 6G Era: Challenges and Opportunities. *IEEE Netw.* **2020**, *35*, 244–251, https://doi.org/10.1109/mnet.011.2000493.

[6] Giordani, M.; Zorzi, M. Satellite Communication at Millimeter Waves: A Key Enabler of the 6G Era. In Proceedings of the IEEE International Conference on Computing, Networking and Communications (ICNC), Big Island, HI, USA, 17–20 February 2020, https://doi.org/10.1109/ICNC47757.2020.9049651.

[7] ITU-R M.2083. IMT vision - Framework and overall objectives of the future development of IMT for 2020 and beyond. ITU Recommendation, 2015. Available online: https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf (Accessed on 26 May 2023).

[8] Onireti, O.; Imran, M. A.; Qadir, J.; Sathiaseelan, A. Will 5G see its blind side? Evolving 5G for universal internet access. In Proceedings of the Workshop on Global Access to the Internet for All (GAIA), Florianopolis, Brazil, 26 August 2016, https://doi.org/10.1145/2940157.2940158.

[9] McKinsey & Company, Technology, Media and Telecom Practice. Offline and falling behind: Barriers to internet adoption. October 2014. Available online: https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/offline-and-falling-behind-barriers-to-internet-adoption (Accessed on 26 May 2023).

[10] Mekuria, F.; Mfupe, L. Spectrum sharing & affordable broadband in 5G. In Proceedings of the Global Wireless Summit (GWS), Cape Town, South Africa, 15–18 October 2017, https://doi.org/10.1109/GWS.2017.8300495.

[11] Dixit, S. Realizing wireless internet connectivity for all through B5G leading to 6G Digital Inclusion: The Killer App for 6G. Keynote speech in the 6G Summit, Levi, Finland, March 2019. Available online: http://www.6gsummit.com/wp-content/uploads/2019/04/Day2_Session3_Dixit_IEEE.pdf (Accessed on 26 May 2023).

[12] Yaacoub, E.; Alouini, M.-S. A Key 6G Challenge and Opportunity—Connecting the Base of the Pyramid: A Survey on Rural Connectivity. *Proc. IEEE* **2020**, *108*, 533–582, https://doi.org/10.1109/jproc.2020.2976703.

[13] Dang, S.; Amin, O.; Shihada, B.; Alouini, M.-S. What should 6G be? *Nat. Electron.* **2020**, *3*, 20–29, https://doi.org/10.1038/s41928-019-0355-6.

[14] Zhu, J.; Zhao, M.; Zhang, S.; Zhou, W. Exploring the road to 6G: ABC — foundation for intelligent mobile networks. *China Commun.* **2020**, *17*, 51–67, https://doi.org/10.23919/jcc.2020.06.005.

[15] Jiang, W.; Han, B.; Habibi, M.A.; Schotten, H.D. The Road Towards 6G: A Comprehensive Survey. *IEEE Open J. Commun. Soc.* **2021**, *2*, 334–366, https://doi.org/10.1109/ojcoms.2021.3057679.

[16] Bin Ahammed, T.; Patgiri, R. 6G and AI: The emergence of future forefront technology. In Proceedings of the Advanced Communication Technologies and Signal Processing Conference (ACTS), Silchar, India, 4–6 December 2020, https://doi.org/10.1109/ACTS49415.2020.9350396.

[17] Yaacoub, J.-P.A.; Noura, M.; Noura, H.N.; Salman, O.; Yaacoub, E.; Couturier, R.; Chehab, A. Securing internet of medical things systems: Limitations, issues and recommendations. *Futur. Gener. Comput. Syst.* **2019**, *105*, 581–606, https://doi.org/10.1016/j.future.2019.12.028.

[18] Arias Garcia, D.; Roseman, J. How Digital Twin Technology is Disrupting Healthcare. Plug and Play article, Available online: https://www.plugandplaytechcenter.com/resources/how-digital-twins-technology-disrupting-healthcare/ (Accessed on 26 May 2023).

[19] Sicari, S.; Rizzardi, A.; Piro, G.; Coen-Porisini, A.; Grieco, L. Beyond the smart things: Towards the definition and the performance assessment of a secure architecture for the Internet of Nano-Things. *Comput. Networks* **2019**, *162*, 106856, https://doi.org/10.1016/j.comnet.2019.07.012.

[20] Diamandis, P. Bionauts – Robots in your Body. Tech. Blog, 2021. Available online: https://www.diamandis.com/blog/bionauts-robots-in-the-body (Accessed on 26 May 2023).

[21] Jornet, J.M.; Akyildiz, I.F. Channel Modeling and Capacity Analysis for Electromagnetic Wireless Nanonetworks in the Terahertz Band. *IEEE Trans. Wirel. Commun.* **2011**, *10*, 3211–3221, https://doi.org/10.1109/twc.2011.081011.100545.

[22] Mezaal, Y.S.; Yousif, L.N.; Abdulkareem, Z.J.; Hussein, H.A.; Khaleel, S.K. Review about effects of IoT and Nano-Technology Techniques in the Development of IoNT in Wireless Systems. *Int. J. Eng. Technol.* **2018**, *7*, 3602–3606, https://doi.org/10.14419/ijet.v7i4.19615.

[23] Yaacoub, E.; Abualsaud, K.; Khattab, T.; Guizani, M.; Chehab, A. Secure mHealth IoT Data Transfer from the Patient to the Hospital: A Three-Tier Approach. *IEEE Wirel. Commun.* **2019**, *26*, 70–76, https://doi.org/10.1109/mwc.2019.1800590.

[24] Yaacoub, E.; Abualsaud, K.; Khattab, T.; Chehab, A. Secure Transmission of IoT mHealth Patient Monitoring Data from Remote Areas Using DTN. *IEEE Netw.* **2020**, *34*, 226–231, https://doi.org/10.1109/mnet.011.1900627.

[25] Akyildiz, I.F.; Pierobon, M.; Balasubramaniam, S.; Koucheryavy, Y. The internet of Bio-Nano things. *IEEE Commun. Mag.* **2015**, *53*, 32–40, https://doi.org/10.1109/mcom.2015.7060516.

[26] Atlam, H.F.; Walters, R.J.; Wills, G.B. Internet of Nano Things: Security Issues and Applications. In Proceedings of the International Conference on Cloud and Big Data Computing, Barcelona, Spain, 3–5 August 2018, https://doi.org/10.1145/3264560.3264570.

[27] Akhtar, N.; Perwej, Y. The internet of nano things (IoNT) existing state and future Prospects. *GSC Adv. Res. Rev.* **2020**, *5*, 131–150, https://doi.org/10.30574/gscarr.2020.5.2.0110.

[28] Gouissem, A.; Abualsaud, K.; Yaacoub, E.; Khattab, T. Federated Learning Stability Under Byzantine Attacks. In Proceedings of the Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022, https://doi.org/10.1109/WCNC51071.2022.9771594.

[29] Mchergui, A.; Moulahi, T.; Zeadally, S. Survey on Artificial Intelligence (AI) techniques for Vehicular A d-hoc Networks (VANETs). *Veh. Commun.* **2021**, *34*, 100403, https://doi.org/10.1016/j.vehcom.2021.100 403.

[30] Marr, B. The 5 biggest connected and autonomous vehicle trends in 2022. Forbes, 2021, Available online: https://www.forbes.com/sites/bernardmarr/2021/12/20/the-5-biggest-connected-and-autonomous-vehicle-trends-in-2022/ (Accessed on 26 May 2023).

[31] Pao, W. Intelligent transportation trends to watch for in 2021. asmag.com Security and IoT, 2021, Available online: https://www.asmag.com/showpost/32201.aspx2 (Accessed on 26 May 2023).

[32] Muoio, D. 4 ways driverless cars will change how we live. Business Insider, 2016, Available online: https://www.businessinsider.com/peter-diamandis-how-driverless-cars-will-change-how-we-live-2016-8 (Accessed on 26 May 2023).

[33] Liu, R.W.; Liang, M.; Nie, J.; Lim, W.Y.B.; Zhang, Y.; Guizani, M. Deep Learning-Powered Vessel Trajectory Prediction for Improving Smart Traffic Services in Maritime Internet of Things. *IEEE Trans. Netw. Sci. Eng.* **2022**, *9*, 3080–3094, https://doi.org/10.1109/tnse.2022.3140529.

[34] Tong, W.; Zhu, P. *6G: The Next Horizon - From Connected People and Things to Connected Intelligence*, 1st ed.; Cambridge University Press: Cambridge, UK, 2021; ISBN: 9781108839327.

[35] Banham, R. The Departed: Communicating with Lost Loved Ones Through AI and VR. Dell Technologie s, 2019, Available online: https://www.delltechnologies.com/en-us/perspectives/the-departed-communicat ing-with-lost-loved-ones-through-ai-and-vr/ (Accessed on 26 May 2023).

[36] Messier, D. "In Lieu of Actual Trips to Space, Try Virtual Reality", Parabolic Arc, 2016, Available online: http://www.parabolicarc.com/2016/02/27/diamandis-lieu-actual-trips-space-try-virtual-reality/ (Accessed on 26 May 2023).

[37] Diamandis, P. Artificial Intelligence and Shopping - A New Retail Era. Tech. Blog, 2019, Available online: https://www.diamandis.com/blog/future-of-retail-part-1 (Accessed on 26 May 2023).

[38] Tegmark, M. *Life 3.0: Being Human in the Age of Artificial Intelligence*, 1st ed.; Vintage Books: New York, USA, 2017; ISBN 978-1-101-97031-7.

[39] Deloitte. National transformation in the Middle East: A digital journey. Tech. Rep., Deloitte, 2017. Availa ble online: https://www2.deloitte.com/xe/en/pages/technology-media-and-telecommunications/articles/dt me_tmt_national-transformation-in-the-middleeast-a-digital-journey.html (Accessed on 26 May 2023).

[40] DSI VR 300. Available online: https://wearablesensing.com/products/vr300/ (Accessed on 26 May 2023).

[41] Hashash, O.; Sharafeddine, S.; Dawy, Z.; Mohamed, A.; Yaacoub, E. Energy-Aware Distributed Edge ML for mHealth Applications with Strict Latency Requirements. *IEEE Wirel. Commun. Lett.* **2021**, *10*, 2791–2794, https://doi.org/10.1109/lwc.2021.3117876.

[42] Marzbani, H.; Marateb, H.R.; Mansourian, M. Methodological Note: Neurofeedback: A Comprehensive Review on System Design, Methodology and Clinical Applications. *Basic Clin. Neurosci. J.* **2016**, *7*, 143–158, https://doi.org/10.15412/j.bcn.03070208.

[43] Healey, J.; Picard, R. Detecting Stress During Real-World Driving Tasks Using Physiological Sensors. *IEEE Trans. Intell. Transp. Syst.* **2005**, *6*, 156–166, https://doi.org/10.1109/tits.2005.848368.

[44] Jensen, J.N.; Hannmose, M. Camera-based heart rate monitoring. B.Sc. Thesis, Department of Applied Mathematics and Computer Science, Technical University of Denmark, 2014.

[45] The 11 Best Heart Rate Monitor Watches for 2023. Available online: https://www.healthline.com/nutritio n/best-heart-rate-monitoring-watch (Accessed on 26 May 2023).

[46] Oura Ring, Accurate health information accessible to everyone. Available online: https://ouraring.com/ (Accessed on 26 May 2023).

[47] MUSE. Available online: http://www.choosemuse.com/ (Accessed on 26 May 2023).

[48] Jamil, S.U.; Khan, M.A.; Rehman, S. Intelligent Task Off-Loading and Resource Allocation for 6G Smart City Environment. In Proceedings of the IEEE 45th Conference on Local Computer Networks (LCN), Sydney, NSW, Australia, 16–19 November 2020, https://doi.org/10.1109/LCN48667.2020.9314819.

[49] Du, J.; Jiang, C.; Wang, J.; Ren, Y.; Debbah, M. Machine Learning for 6G Wireless Networks: Carrying Forward Enhanced Bandwidth, Massive Access, and Ultrareliable/Low-Latency Service. *IEEE Veh. Technol. Mag.* **2020**, *15*, 122–134, https://doi.org/10.1109/mvt.2020.3019650.

[50] Lee, H.; Jang, Y.; Song, J.; Yeon, H. O-RAN AI/ML Workflow Implementation of Personalized Network Optimization via Reinforcement Learning. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021, https://doi.org/10.1109/GCWkshps52748.2021.9681936.

[51] Manogaran, G.; Baabdullah, T.; Rawat, D.B.; Shakeel, P.M. AI-Assisted Service Virtualization and Flow Management Framework for 6G-Enabled Cloud-Software-Defined Network-Based IoT. *IEEE Internet Things J.* **2021**, *9*, 14644–14654, https://doi.org/10.1109/jiot.2021.3077895.

[52] Zeb, S.; Rathore, M. A.; Mahmood, A.; Hassan, S. A.; Kim, J. W.; Gidlund, M. Edge Intelligence in Soft warized 6G: Deep Learning-enabled Network Traffic Predictions. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021, https://doi.org/10.1109/GCWkshps5274 8.2021.9682131.

[53] Ren, J.; Wang, Z.; Xu, M.; Fang, F.; Ding, Z. An EM-Based User Clustering Method in Non-Orthogonal Multiple Access. *IEEE Trans. Commun.* **2019**, *67*, 8422–8434, https://doi.org/10.1109/tcomm.2019.29453 34.

[54] Jamshed, M.A.; Heliot, F.; Brown, T.W.C. Unsupervised Learning Based Emission-Aware Uplink Resource Allocation Scheme for Non-Orthogonal Multiple Access Systems. *IEEE Trans. Veh. Technol.* **2021**, *70*, 7681–7691, https://doi.org/10.1109/tvt.2021.3089898.

[55] Chi, N.; Zhou, Y.; Wei, Y.; Hu, F. Visible Light Communication in 6G: Advances, Challenges, and Prospects. *IEEE Veh. Technol. Mag.* **2020**, *15*, 93–102, https://doi.org/10.1109/mvt.2020.3017153.

[56] Sritharan, S.; Weligampola, H.; Gacanin, H. A Study on Deep Learning for Latency Constraint Applicatio ns in Beyond 5G Wireless Systems. *IEEE Access* **2020**, *8*, 218037–218061, https://doi.org/10.1109/access. 2020.3040133.

[57] Salh, A.; Audah, L.; Shah, N.S.M.; Alhammadi, A.; Abdullah, Q.; Kim, Y.H.; Al-Gailani, S.A.; Hamzah, S.A.; Esmail, B.A.F.; Almohammedi, A.A. A Survey on Deep Learning for Ultra-Reliable and Low-Latency Communications Challenges on 6G Wireless Systems. *IEEE Access* **2021**, *9*, 55098–55131, https://doi.org/10.1109/access.2021.3069707.

[58] She, C.; Sun, C.; Gu, Z.; Li, Y.; Yang, C.; Poor, H.V.; Vucetic, B. A Tutorial on Ultrareliable and Low-Latency Communications in 6G: Integrating Domain Knowledge Into Deep Learning. *Proc. IEEE* **2021**, *109*, 204–246, https://doi.org/10.1109/jproc.2021.3053601.

[59] Kim, Y.; Ahn, S.; You, C.; and Cho, S. A Survey on Machine Learning-based Medium Access Control Technology for 6G Requirements. In Proceedings of the IEEE Region 10 Symposium, Jeju, South Korea, 23–25 August 2021, https://doi.org/10.1109/TENSYMP52854.2021.9550841.

[60] Sami, H.; Otrok, H.; Bentahar, J.; Mourad, A. AI-Based Resource Provisioning of IoE Services in 6G: A Deep Reinforcement Learning Approach. *IEEE Trans. Netw. Serv. Manag.* **2021**, *18*, 3527–3540, https://doi.org/10.1109/tnsm.2021.3066625.

[61] Wang, L.; Han, D.; Zhang, M.; Wang, D.; Zhang, Z. Deep Reinforcement Learning-Based Adaptive Handover Mechanism for VLC in a Hybrid 6G Network Architecture. *IEEE Access* **2021**, *9*, 87241–87250, https://doi.org/10.1109/access.2021.3089521.

[62] Wu, T. Reinforcement Learning Based Proactive Monitor Channel Allocation. In Proceedings of the IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), Chongqing, China, 12–14 March 2021, https://doi.org/10.1109/IAEAC50856.2021.9391117.

[63] Shah, H.A.; Zhao, L.; Kim, I.-M. Joint Network Control and Resource Allocation for Space-Terrestrial Integrated Network Through Hierarchal Deep Actor-Critic Reinforcement Learning. *IEEE Trans. Veh. Technol.* **2021**, *70*, 4943–4954, https://doi.org/10.1109/TVT.2021.3071983.

[64] Zhao, Q.; Paris, S.; Veijalainen, T.; Ali, S. Hierarchical Multi-Objective Deep Reinforcement Learning fo r Packet Duplication in Multi-Connectivity for URLLC. In Proceedings of the Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit): Wireless, Optical and Satellite N etworks (WOS), Porto, Portugal, 8–11 June 2021, https://doi.org/10.1109/EuCNC/6GSummit51104.2021. 9482453.

[65] Mei, J.; Wang, X.; Zheng, K.; Boudreau, G.; Bin Sediq, A.; Abou-Zeid, H. Intelligent Radio Access Network Slicing for Service Provisioning in 6G: A Hierarchical Deep Reinforcement Learning Approach. *IEEE Trans. Commun.* **2021**, *69*, 6063–6078, https://doi.org/10.1109/tcomm.2021.3090423.

[66] Cao, Y.; Lieny, S.-Y.; Liang, Y.-C.; Chen, K.-C. Federated Deep Reinforcement Learning for User Acces s Control in Open Radio Access Networks. In Proceedings of the IEEE International Conference on Com munications (ICC), Montreal, QC, Canada, 14–23 June 2021, https://doi.org/ 10.1109/ICC42927.2021.95 00603.

[67] Esenogho, E.; Djouani, K.; Kurien, A.M. Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect. *IEEE Access* **2022**, *10*, 4794–4831, https://doi.org/10.1109/access.2022.3140595.

[68] Usman, M.; Ansari, S.; Taha, A.; Zahid, A.; Abbasi, Q.H.; Imran, M.A. Terahertz-Based Joint Communication and Sensing for Precision Agriculture: A 6G Use-Case. *Front. Commun. Networks* **2022**, *3*, https://doi.org/10.3389/frcmn.2022.836506.

[69] Lovén, L.; Leppänen, T.; Peltonen, E.; Partala, J.; Harjula, E.; Porambage, P.; Ylianttila, M.; Riekki, J. Edge AI: A vision for distributed, edge-native artificial intelligence in future 6G networks. In Proceedings of the 6G Wireless Summit, Levi, Finland, 24–26 March 2019.

[70] Xiao, Y.; Shi, G.; Li, Y.; Saad, W.; Poor, H.V. Toward Self-Learning Edge Intelligence in 6G. *IEEE Commun. Mag.* **2020**, *58*, 34–40, https://doi.org/10.1109/mcom.001.2000388.

[71] Dupont, P.E.; Nelson, B.J.; Goldfarb, M.; Hannaford, B.; Menciassi, A.; O'malley, M.K.; Simaan, N.; Valdastri, P.; Yang, G.-Z. A decade retrospective of medical robotics research from 2010 to 2020. *Sci. Robot.* **2021**, *6*, https://doi.org/10.1126/scirobotics.abi8017.

[72] Murphy, R.R. Robot intelligence and applications are as varied as animal intelligence, so why not treat them the same way? *Sci. Robot.* **2021**, *6*, https://doi.org/10.1126/scirobotics.abn0877.

[73] Ryan, K. This Startup Recruited a Hollywood Designer to Create the Coolest Cybersecurity Software You've Ever Seen. Inc., 2017. Available online: https://www.inc.com/kevin-j-ryan/protectwise-futuristic-cybersecurity-startup.html (Accessed on 26 May 2023).

[74] Reese, B. *The Fourth Age: Smart Robots, Conscious Computers, and the Future of Humanity*, 1st ed.; Atria International, New York, USA, 2018; ISBN 978-1-5011-9162-6.

[75] Siriwardhana, Y.; Porambage, P.; Liyanage, M.; Ylianttila, M. AI and 6G security: Opportunities and chal lenges. In Proceedings of the Joint European Conference on Networks and Communications & 6G Summi t, EuCNC/6G Summi, Porto, Portugal, 8–11 June 2021, https://doi.org/10.1109/EuCNC/6GSummit51104. 2021.9482503.

[76] Buchholz, S.; Bechtel, M.; Briggs, B. Deloitte Insights - Tech Trends 2022. Available online: https://www2.deloitte.com/us/en/insights/focus/tech-trends.html (Accessed on 26 May 2023).

[77] Tariq, M.; Ali, M.; Naeem, F.; Poor, H.V. Vulnerability Assessment of 6G-Enabled Smart Grid Cyber–Physical Systems. *IEEE Internet Things J.* **2020**, *8*, 5468–5475, https://doi.org/10.1109/jiot.2020.3042090.

[78] Nguyen, V.-L.; Lin, P.-C.; Cheng, B.-C.; Hwang, R.-H.; Lin, Y.-D. Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges. *IEEE Commun. Surv. Tutorials* **2021**, *23*, 2384–2428, https://doi.org/10.1109/comst.2021.3108618.

[79] Dastjerdi, A.V.; Buyya, R. Fog Computing: Helping the Internet of Things Realize Its Potential. *Computer* **2016**, *49*, 112–116, https://doi.org/10.1109/mc.2016.245.

[80] Al-Garadi, M.A.; Mohamed, A.; Al-Ali, A.K.; Du, X.; Ali, I.; Guizani, M. A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security. *IEEE Commun. Surv. Tutor.* **2018***, 22,* 1646–1685, https://doi.org/10.1109/COMST.2020.2988293.

[81] Al-Mohammed, H.A.; Al-Ali, A.; Yaacoub, E.; Qidwai, U.; Abualsaud, K.; Rzewuski, S.; Flizikowski, A. Machine Learning Techniques for Detecting Attackers During Quantum Key Distribution in IoT Networ ks with Application to Railway Scenarios. *IEEE Access* **2021**, *9*, 136994–137004, https://doi.org/10.1109/ access.2021.3117405.

[82] Lohachab, A.; Jangra, A. A comprehensive survey of prominent cryptographic aspects for securing comm unication in post-quantum IoT networks. *Internet Things* **2020**, *9*, 100174, https://doi.org/10.1016/j.iot.20 20.100174.

[83] Fernandez-Carames, T.M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet Things J.* **2019**, *7*, 6457–6480, https://doi.org/10.1109/jiot.2019.2958788.

[84] Ziegler, V.; Schneider, P.; Viswanathan, H.; Montag, M.; Kanugovi, S.; Rezaki, A. Security and Trust in the 6G Era. *IEEE Access* **2021**, *9*, 142314–142327, https://doi.org/10.1109/access.2021.3120143.

[85] Hewa, T.; Gür, G.; Kalla, A.; Ylianttila, M.; Bracken, A.; Liyanage, M. The Role of Blockchain in 6G: Challenges, Opportunities and Research Directions. In Proceedings of the second 6G Wireless Summit, Levi, Finland, 17–20 March 2020, https://doi.org/10.1109/6GSUMMIT49458.2020.9083784.

[86] Sun, W.; Li, S.; Zhang, Y. Edge caching in blockchain empowered 6G. *China Commun.* **2021**, *18*, 1–17, https://doi.org/10.23919/jcc.2021.01.001.

[87] Velliangiri, S.; Manoharn, R.; Ramachandran, S.; Rajasekar, V.R. Blockchain Based Privacy Preserving Framework for Emerging 6G Wireless Communications. *IEEE Trans. Ind. Informatics* **2022**, *18*, 4868 – 4874, https://doi.org/10.1109/tii.2021.3107556.

[88] Ali, F. The Top 5 Problems with Blockchain Technology. MakeUseOf.com, July 16, 2021; Available online: https://www.makeuseof.com/problems-with-blockchain-technology/ (Accessed on 26 May 2023).

[89] Nahar, P. After Kazakh crisis, here's what can push Bitcoin to $30,000. The Economic Times, January 11, 2022; Available online: https://economictimes.indiatimes.com/markets/cryptocurrency/after-kazakh-crisis-heres-what-can-push-bitcoin-to-30000/articleshow/88808284.cms (Accessed on 26 May 2023).

[90] Elahi, M.; Cui, H.; Kaosar, M. Survey: An Overview on Privacy Preserving Federated Learning in Health Data. *Comput. Netw. Commun*. **2023**, *1,* 147–161.

[91] Ali, M.; Naeem, F.; Tariq, M.; Kaddoum, G. Federated Learning for Privacy Preservation in Smart Healthcare Systems: A Comprehensive Survey. *IEEE J. Biomed. Heal. Informatics* **2022**, *27*, 778–789, https://doi.org/10.1109/jbhi.2022.3181823.

[92] Haklidir, M.; Temeltas, H. Autonomous Driving Systems for Decision-Making Under Uncertainty Using Deep Reinforcement Learning. In Proceedings of the Signal Processing and Communications Application s Conference (SIU), Safranbolu, Turkey, 15–18 May 2022, https://doi.org/ 10.1109/SIU55565.2022.9864 806.

[93] Thunyapoo, B.; Ratchadakorntham, C.; Siricharoen, P.; Susutti, W. Self-Parking Car Simulation using Reinforcement Learning Approach for Moderate Complexity Parking Scenario. In Proceedings of the International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), Phuket, Thailand, 24–27 June 2020, https://doi.org/10.1109/ECTI-CON49241.2020.9158298.

[94] Trinh, B.; Muntean, G.-M. A Deep Reinforcement Learning-Based Offloading Scheme for Multi-Access Edge Computing-Supported eXtended Reality Systems. *IEEE Trans. Veh. Technol.* **2022**, *72*, 1254–1264, https://doi.org/10.1109/tvt.2022.3207692.

[95] Dong H.; Lee, J. S. A. The Metaverse from a Multimedia Communications Perspective. *IEEE MultiMedia* **2022**, *29*, 123–127, https://doi.org/10.1109/MMUL.2022.3217627.

[96] Sa, I.-S.C.; Molnar, A.; Tal, I.; Imhof, C.; Bergamin, P.; Muntean, G.-M.; Muntean, C.H.; Trestian, R. Improved Quality of Online Education Using Prioritized Multi-Agent Reinforcement Learning for Video Traffic Scheduling. **2023**, *PP*, 1–19, https://doi.org/10.1109/tbc.2023.3246815.

[97] Perez-Valero, E.; Vaquero-Blasco, M.A.; Lopez-Gordo, M.A.; Morillas, C. Quantitative Assessment of Stress Through EEG During a Virtual Reality Stress-Relax Session. *Front. Comput. Neurosci.* **2021**, *15*, 684423, https://doi.org/10.3389/fncom.2021.684423.

[98] Zhang, Y.; Zhang, L.; Hua, H.; Jin, J.; Zhu, L.; Shu, L.; Xu, X.; Kuang, F.; Liu, Y. Relaxation Degree Analysis Using Frontal Electroencephalogram Under Virtual Reality Relaxation Scenes. *Front. Neurosci.* **2021**, *15*,719869, https://doi.org/10.3389/fnins.2021.719869.

[99] Ghadirzadeh, A.; Chen, X.; Yin, W.; Yi, Z.; Bjorkman, M.; Kragic, D. Human-Centered Collaborative Ro bots with Deep Reinforcement Learning. *IEEE Robot. Autom. Lett.* **2020**, *6*, 566–571, https://doi.org/10.1 109/lra.2020.3047730.

[100] Chen, Z.; Nakamura, Y.; Ishiguro, H. Outperformance of Mall-Receptionist Android as Inverse Reinforcement Learning is Transitioned to Reinforcement Learning. *IEEE Robot. Autom. Lett.* **2023**, *8*, 3350–3357, https://doi.org/10.1109/lra.2023.3267385.

[101] Ali, A.; Gul, S.; Mahmood, T.; Ullah, A. Exploration of Unknown Environment using Deep Reinforceme nt Learning. In Proceedings of the International Conference on Robotics and Automation in Industry (ICR AI), Peshawar, Pakistan, 3–5 March 2023, https://doi.org/10.1109/ICRAI57502.2023.10089589.

[102] Li, W.; Wu, J.; Chen, J.; Lia, K.; Cai, X.; Wang, C.; Guo, Y.; Jia, S.; Chen, W.; Luo, F.; Wang, W. UAV countermeasure maneuver decision based on deep reinforcement learning. In Proceedings of the Youth Academic Annual Conference of Chinese Association of Automation (YAC), Beijing, China, 19–20 November 2022, https://doi.org/10.1109/YAC57282.2022.10023761.

[103] Wang, L.; Wei, H. Research on Autonomous Decision-Making of UCAV Based on Deep Reinforcement Learning. In Proceedings of the Information Communication Technologies Conference (ICTC), Nanjing, China, 6–8 May 2022, https://doi.org/10.1109/ICTC55111.2022.9778652.

[104] Bian, W.; Wang, C.; Huang, K.; Jia, Y.; Liu, C.; Mi, Y. Cooperative Strike Target Assignment Algorithm Based on Deep Reinforcement Learning. In Proceedings of the International Conference on Cyber-Physic al Social Intelligence (ICCSI), Nanjing, China, 18–21 November 2022, https://doi.org/ 10.1109/ICCSI555 36.2022.9970699.

[105] Lim, W.Y.B.; Xiong, Z.; Niyato, D.; Cao, X.; Miao, C.; Sun, S.; Yang, Q. Realizing the Metaverse with E dge Intelligence: A Match Made in Heaven. *IEEE Wirel. Commun.* **2022**, *PP*, 1–9, https://doi.org/10.1109 /mwc.018.2100716.

[106] McDermid, J.A.; Jia, Y.; Porter, Z.; Habli, I. Artificial intelligence explainability: the technical and ethical dimensions. *Philos. Trans. R. Soc. A: Math. Phys. Eng. Sci.* **2021**, *379*, 20200363, https://doi.org/10.1098 /rsta.2020.0363.