Finabel

Food for thought 03-2025

The Light Advantage: Exploring Li-Fi as the Next Frontier in Military Data Transmission

FINABEL
European Land Force Commanders Organisation

WRITTEN BY:

Antonio Sorbino is an expert in European foreign policy, transatlantic affairs, defence and international relations. He focuses on strategic autonomy, aiming to analyse how the EU can develop a securitarian framework that promotes more cohesive defence integration among its member states.

Berk Büyükarslan is a research trainee at Finabel, specialising in post-Soviet politics, psychological warfare and discourse analysis. He focuses on the sociopolitical developments and defence policies in Central/Eastern Europe and Central Asia, where hybrid threats continue to evolve.

Petar Petrović is an expert in defence, security, and international relations, focusing on strategic analysis, hybrid warfare, and policy development. He specialises in producing in-depth research and insightful publications addressing complex geopolitical challenges and emerging security threats.

This paper was commissioned by **Mario Blokken**, supervised by **Victoriano Vicente Botella Berenguer** and edited by **Riccardo Cernigliaro**. The authors would also like to express their gratitude to **Jeroen van Gils (CEO of Li-Fi Co)** and **Günter Boomgarden** for their valuable contributions to the research process, providing insights and expertise that greatly enhanced the study.

DIRECTOR'S EDITORIAL

In an era where military operations are increasingly dependent on secure, high-speed communication networks, the exploration of Light Fidelity (Li-Fi) represents a significant leap forward. Traditional radio frequency (RF)-based systems have long served as the backbone of military communications, but they are becoming increasingly susceptible to spectrum congestion, cyber vulnerabilities, and electromagnetic interference. This reality demands innovative solutions to maintain operational superiority in modern warfare.

Li-Fi, an emerging optical communication technology that leverages visible light for data transmission, presents a promising alternative. Its unique attributes – including enhanced security, high bandwidth capacity, and immunity to electromagnetic disturbances – offer a transformational opportunity for military applications. This Food for Thought paper delves into the technical potential, strategic advantages, and practical limitations of integrating Li-Fi into command-and-control operations, naval communications, and crisis management scenarios.

The ability to transmit data through light waves, imperceptible to external adversaries, provides an unparalleled layer of security in sensitive military operations. Additionally, Li-Fi's resilience against jamming and interception, coupled with its potential to integrate with quantum encryption, highlights its role in shaping the future of military data transmission. However, challenges remain, including line-of-sight dependence, environmental sensitivity, and the necessity for hybrid integration with existing RF infrastructures.

This paper does not aim to provide definitive answers but rather to stimulate discussion and inform strategic thinking on the next frontier of military communication. As defence organisations worldwide assess new technologies to maintain strategic advantages, Li-Fi deserves serious consideration as part of a broader multi-domain operational strategy.

We encourage policymakers, military planners, and defence industry leaders to explore Li-Fi's potential applications and contribute to the ongoing dialogue on its viability. As with any disruptive innovation, its true impact will depend on collaborative research, cross-sector cooperation, and deliberate implementation strategies.

Mario Blokken
Director

ABSTRACT

Light Fidelity (Li-Fi) is an emerging technology that revolutionises wireless communication by leveraging the visible light spectrum for data transmission. Addressing the limitations of traditional radio frequency (RF)-based systems, Li-Fi offers unparalleled advantages in bandwidth, security, and energy efficiency. This paper examines Li-Fi's transformative potential, particularly in military contexts where secure and resilient communication is paramount. From enhancing command and control operations to facilitating naval coordination and disaster response, Li-Fi's unique attributes, such as immunity to electromagnetic interference and high-speed transmission, make it a compelling alternative to RF technologies.

However, issues like line-of-sight reliance and environmental sensitivity must be addressed before widespread use occurs. The integration of Li-Fi with existing RF systems via hybrid techniques, as well as the new IEEE 802.11bb standardisation, point to a route towards practical feasibility. The paper also explores prospects, including Li-Fi's role in multi-domain operations and its potential synergy with quantum encryption technologies.

The study's extensive research highlights Li-Fi's importance in tackling current communication difficulties, as well as its ability to reinvent connection in military and civilian applications. The adoption of Li-Fi might signal a watershed moment in the transition to more secure, efficient, and adaptive wireless communication networks for an increasingly linked world by encouraging collaboration among governments, academics, and businesses.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Acronym	Full Form
AR	Augmented reality
AUVs	Autonomous Underwater Vehicles
BFT	Blue Force Tracking
C2	Command and Control
COP	Common Operational Picture
DD	Direct Detection
EM	Electromagnetic
FBCB2	Force XXI Battle Command Brigade and Below
Gbps	Gigabits per second
GCCS-M	Global Command and Control System-Maritime
GPS	Global Positioning System
HF	High-Frequency
IEEE	Institute of Electrical and Electronics Engineers
IM	Intensity Modulation
JBC-P	Joint Battle Command-Platform
JTRS	Joint Tactical Radio System
LED	Light Emitting Diode
Li-FI	Light Fidelity
LOS	Line of sight

Mbps	Megabits per second
MUOS	Mobile User Objective System
NMT	Navy Multiband Terminal
OFDM	Orthogonal Frequency Division Multiplexing
OOK	On-Off Keying
QAM	Quadrature Amplitude Modulation
QKD	Quantum key distribution
RF	Radio frequencies
SATCOM	Satellite communications
THz	Terahertz
U.S	United States
UAVs	Unmanned Aerial Vehicles
UHF	Ultra-High Frequency
VHF	Very High Frequency
VLC	Visible Light Communication
Wi-Fi	Wireless Fidelity

INTRODUCTION

The emergence of wireless communication technology has played a critical role in creating modern connectedness, propelling improvements in areas ranging from commerce to the military. However, the limits of classic radio frequency (RF)-based systems are becoming more apparent in today's data-intensive, security-conscious society. Spectrum congestion, vulnerability to cyberattacks, and environmental inefficiencies highlight the critical need for creative solutions. Within this setting, Light Fidelity (Li-Fi) appears as a ground-breaking technology that uses visible light to revolutionise data transport.

Introduced in 2011, Li-Fi uses visible light communication (VLC) technology to send data at high rates through LED light bulbs. This breakthrough not only tackles RF systems' bandwidth limits, but also provides unique benefits in terms of security, efficiency, and adaptability. Li-Fi's capacity to transfer data via light waves, which do not penetrate walls, makes it intrinsically secure against external eavesdropping, while its connection with existing LED infrastructure assures both energy efficiency and wider application. As a supplement to or substitute for standard wireless systems, Li-Fi has the potential to revolutionise a wide range of sectors, with particularly interesting military applications.

To achieve mission effectiveness in varied and frequently hostile circumstances, military operations require strong, secure, and high-speed communication networks. From subterranean bunkers to large-scale naval operations, the ability to maintain continuous and secure communication can spell the difference between mission success and failure. Current military communication systems mostly rely on radio frequency (RF) technology such as satellite communications (SATCOM), GPS, and tactical radio networks. While effective, these systems are becoming increasingly vulnerable to jamming, interception, and interference, particularly in the context of contemporary electronic warfare. Li-Fi's unique qualities, such as its tolerance to electromagnetic interference and high bandwidth capacity, make it a transformational solution for tackling these problems.

This paper explores the potential of Li-Fi technology in military contexts, delving into its structural innovations, operational advantages, and comparative benefits over traditional systems. It examines the conceptual framework of Li-Fi, highlighting its superior speed, security, and eco-friendly attributes, and analyses its applications in land-based command and control centres, naval operations, and crisis management scenarios. By incorporating real-world case studies and addressing the technical and operational challenges of Li-Fi integration, this work underscores the critical role that light-based communication systems could play in enhancing military communication networks.

The analysis begins with a comprehensive overview of the advantages and structure of Li-Fi technology, followed by an examination of its standardisation and readiness for large-scale deployment. Subsequent sections investigate the transformative potential of Li-Fi in military command centres, naval fleets, and disaster management scenarios, illustrating

its capacity to operate securely and effectively in environments where RF-based systems fall short. The paper also explores the limitations of Li-Fi, such as its reliance on line-of-sight communication and susceptibility to environmental factors, while proposing hybrid solutions and future advancements to overcome these obstacles.

As the global security landscape evolves, the need for resilient, adaptive, and secure communication systems becomes ever more pressing. By harnessing the untapped potential of the visible light spectrum, Li-Fi represents a paradigm shift in wireless communication, offering a secure, high-speed, and scalable solution to the challenges faced by modern military forces. This exploration aims to provide a nuanced understanding of Li-Fi's capabilities, limitations, and prospects, positioning it as a cornerstone of next-generation military communication strategies.

CONCEPTUALISING LI-FI TECHNOLOGY

Defining Light Fidelity

In the digital age, data transmission assumes a crucial role, especially in the context of ever more extensive and global connectivity. This scenario poses significant challenges but also unprecedented opportunities for technological and social progress. In this respect, Wi-Fi (Wireless Fidelity) represented a breakthrough in wireless communication, as, relying on Radio frequencies (RF), it enabled the transmission of data over relatively large distances without the need for physical cables. However, as internet user numbers continue to rise, the current RF spectrum is becoming inadequate and insufficient to handle this high demand (Fabiyi, 2016). This deficiency leads to a scarcity of RF resources, which may cause significant connectivity disruptions and deteriorate service quality (Sharma et al., 2013). Furthermore, problems of congestion and security emerge, with transmissions potentially vulnerable to interceptions and interference, highlighting the urgent need for addressing these vulnerabilities in wireless communication systems (Sharma et al., 2013).

In response to these existing challenges, Li-Fi technology presents a valid alternative. Unlike traditional methods that rely on radio waves, Li-Fi transmits data using light, offering a promising solution to the limitations of current wireless communication systems. First introduced in 2011 by Professor Harald Hass, Li-Fi relies on a VLC system, which is a "data communication medium, which uses visible light between 400 THz (780 nm) and 800 THz (375 nm) as optical carrier for data transmission and illumination" (Sharma et al., p. 151, 2013). Therefore, Li-Fi transmits data by using LED light bulbs that modulate the light at speeds imperceptible to the human eye. These LEDs serve both as illumination sources and data transmission devices, which encode data by varying the rate of light flickering (Guan & Hina, 2024).

Having said that, Li-Fi offers multiple advantages and benefits that improve the performance and utility of wireless networks. One of the most important is the enhanced security aspect that this technology could offer: data transmitted via Li-Fi remains confined with-

in light-illuminated areas, creating a natural barrier to data breaches (pureLiFi, n.d). Since light waves cannot penetrate walls, they cannot be perceived and detected, thus ensuring that data partitioning takes place safely and without external interference and in this way offering a level of privacy that radio frequency-based systems struggle to match (Sharma et al., 2013).

In addition to its security benefits, Li-Fi offers unprecedented speed and bandwidth, far exceeding the capabilities of traditional Wi-Fi. This makes it suitable for applications that require high bandwidth, enabling faster downloads and more reliable connections in dense and populated digital environments, thus ensuring a clear and reliable communication channel (pureLiFi, n.d). Moreover, Li-Fi constitutes a step forward in promoting eco-friendly technology alternatives. By integrating data transmission capabilities with LED lighting, Li-Fi contributes to significant energy savings and reduced environmental impact (Fabiyi, 2016). This synergy not only optimises energy use but also extends the lifecycle of lighting infrastructure while adding functional value. This dual functionality (illumination and transmission) makes Li-Fi not only an efficient means of communication but also an energy-efficient lighting solution.

In terms of stability, Li-Fi offers consistent connectivity that is not susceptible to radio frequency interference, making it effective in industrial environments where other wireless signals may cause disruptions (pureLiFi, n.d). Additionally, the issue of availability is efficiently addressed with Li-Fi, given the ubiquity of light sources. Globally, billions of light bulbs are in use, and these can simply be replaced with LED bulbs to enable effective data transmission. This widespread availability, combined with robust performance, ensures that Li-Fi can underpin critical communications without the risk of interruption (pureLiFi, n.d). Considering these advantages, Li-Fi has the potential to revolutionise the way we think about and use wireless communication, promising enhanced security, faster speeds, environmental benefits, and greater reliability. Therefore, "Li-Fi offers a relatively easier, cheaper, faster and more secure means of data transfer. In other words, Li-Fi is a cutting-edge technology that has given wireless communication a broad edge over its wired counterpart" (Fabiyi, 1033, 2016).

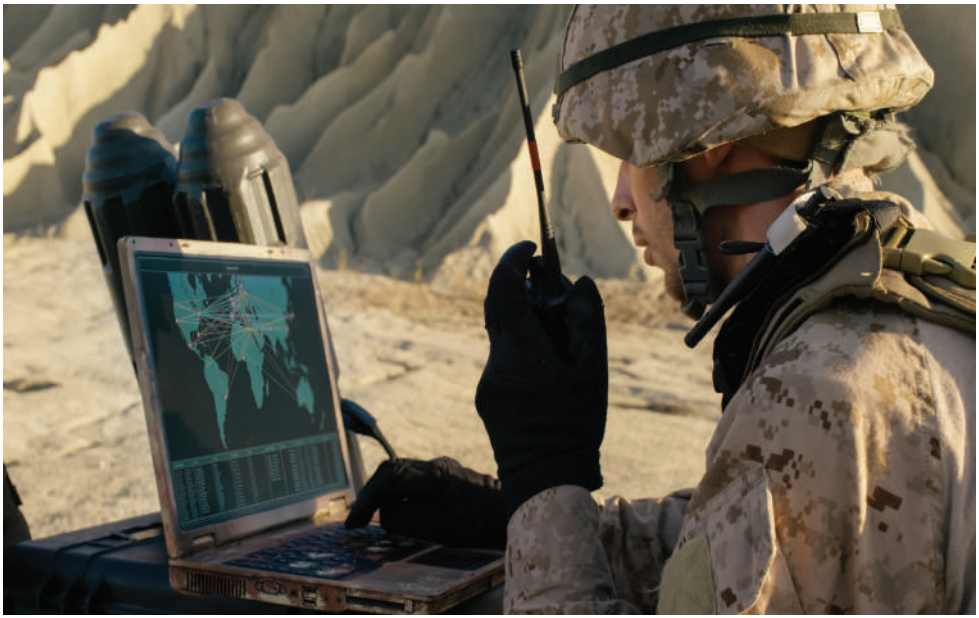
Current Military Communications in the Land and Naval Domains

In the military, communication assumes a major role in coordinating operations as decision-making capabilities and tactical response is highly dependent on the speed and accuracy with which information is transmitted between units and commands. Therefore, "military communications must be characterised by having flexibility, adaptability, and controllability of characteristics such as frequency, bandwidths, speed of transmission of information, and response times and guarantee the continuity of communications despite variant environments that may arise" (Velastegui et al., p.62, 2022). In this regard, the use of precise communication technology can determine the success of a military mission, thereby improving overall operational effectiveness (Oledcomm, n.d-b).

From a technological and communicative

point of view, the common denominator in the land and naval domains is the use of advanced radio systems that leverage electromagnetic waves to transmit information, mainly operating through wireless communications (Velastegui et al., 2022). Therefore, radio waves represent one of the main vectors for military communications as they use different frequencies—High-Frequency (HF), Very High Frequency (VHF) and Ultra-High Frequency (UHF)—for tactical and naval communication. In this regard, there are several instruments employed in the military that rely on radio waves, such as SATCOM, antennas, GPS, transponders and receivers, which are integral for maintaining stable communication lines.

For instance, one example is represented by the Joint Tactical Radio System (JTRS) employed by the US Army (Maher, 2007). The JTRS is an innovative set of software-defined radios that can use multiple radio frequencies and can be easily upgraded through software updates. This system allows US forces to communicate across all services, providing interoperable communication among Army, Navy, Air Force, and Marines (Maher, 2007). By supporting multiple frequency bands and communication modes, this system offers an interoperable, high-capacity solution for the diverse needs of the armed forces (Maher, 2007). From a more tactical perspective, the most modern tool used by the US military is the Joint Battle Command-Platform (JBC-P), which is used to track friendly forces and deliver to soldiers enhanced satellite connectivity and superior logistical capabilities (PEO C3N, n.d.). This platform is committed to enhancing the capabilities of the earlier Force XXI Battle Command Brigade and Below/ Blue Force Tracking (FBCB2/BFT) system (PEO C3N, n.d.). This foundational system



is not only widely implemented across every brigade combat team in the Army, but it is also integrated into thousands of platforms, serving as a critical component in maintaining situational awareness and operational coordination (PEO C3N, n.d.).

For the naval communication system in the military, there are many projects, especially in the US, like the Global Command and Control System-Maritime (GCCS-M), the Mobile User Objective System (MUOS) and the Navy Multiband Terminal (NMT). All of these rely on satellite communications to ensure that naval forces remain connected across vast oceanic expanses (Hu et al., 2018). Designed to provide robust and high-capacity channels for transmitting data and information, these systems are key components of the US naval communication system as they foster communication in diverse and challenging environments, from peacetime deployments to high-intensity conflicts.

Considering the aforementioned, most of the military communications channels for land and naval operations rely on radio waves and satellite technology to provide connections that are critical for coordinating and executing military operations.

STRUCTURE AND STANDARDISATION: OPERATIONAL ABILITIES OF LI-FI

Structure of the Technology

At its core, Li-Fi is a bidirectional, high-speed, and fully networked wireless communication technology that uses light to transmit and receive information. The name itself, 'Light Fidelity,' encapsulates the essence of this technology: fidelity, or accuracy, in data transmission using light (Bao et al., 2015). As mentioned, the term was coined by Professor Haas in 2011 when he brought out the use of wireless communication technology that transmits data using light waves, typically from LEDs (Haas, 2011). This data transmission happens in a manner invisible to the human eye, using a portion of the electromagnetic spectrum not traditionally associated with internet connectivity—the visible light spectrum (LiFi.Co, n.d-b). The visible light spectrum, the portion of the electromagnetic spectrum that is detectable by the human eye, is approximately 10,000 times larger than the entire radio frequency spectrum. This abundant, unused spectrum offers an untapped resource for data transmission, enabling speeds far beyond those currently achievable with traditional radio frequencies. Thus, Li-Fi has the potential to loosen the constraints of the traditional, congested radio frequency spectrum and bring us into a new era of high-speed, high-density wireless data communication (Kuttan et al., 2021).

According to one of the pioneering companies in the field (LiFi.Co, n.d-a), crucial components of the technology are:

Light Source (Transmitter): Modern Li-Fi systems primarily use LED bulbs. When an electrical current is applied to an LED, it emits light, thereby by adjusting this current, the light emission is modulated to transmit data.

Photodetector (Receiver): The photodetector captures the light signals and converts them back into electrical signals. These are then transformed back into binary data. Com-

mon photodetectors in Li-Fi systems include photodiodes or avalanche photodiodes and they're chosen based on sensitivity and speed requirements.

Signal Processing Unit: This unit transforms the received electrical signals from the photodetector into a format that digital devices can understand. Sometimes, the signals might be weak, especially if the receiver is far from the light source and in these cases, the processing unit amplifies these signals to ensure data integrity.

Modulation & Demodulation Circuits: Before sending, the input data is modulated to be encoded onto the light signal. Different modulation schemes, like On-Off Keying (OOK) or Quadrature Amplitude Modulation (QAM), can be used based on data rate requirements. At the receiving end, this circuitry decodes the data from the light signal, turning it back into its original form.

Optical Components: Lenses can be used to focus the light onto the photodetector, ensuring maximum data capture. Another type of optical component, filters, help in eliminating unwanted ambient light, ensuring that only the desired Li-Fi signal reaches the photodetector.

Power Source & Management: LEDs require a power source, and this can be direct electricity or even battery-operated in portable setups. In that manner, efficient power management ensures the LED operates optimally without overheating or wasting energy.

Interface with Digital Devices.

In summary, at a basic level, a Li-Fi system involves two primary components: a high-brightness white LED that acts as a transmitter and a silicon photodiode that is sensitive to visible wavelength range, functioning as a receiver. This pair of components communicate with each other via rapid, invisible fluctuations in LED light intensity, allowing data to be transmitted wirelessly at high speeds (Karthika & Balakrishan, 2015). LEDs can be switched on and off to generate digital strings of 1s and 0s. To be clearer, by modulating the LED light with the data signal, the LED illumination can be used as a communication source (Bhad & Chavam, 2015). It is noteworthy that Li-Fi can function in both the visible light spectrum and the invisible spectra, such as infrared and ultraviolet. This versatility enhances its potential applications across various environmental conditions (Karthika & Balakrishan, 2015). In this sense, Li-Fi is a fast optical variant of Wi-Fi, a system based on VLC that employs fast light pulses to transport information wirelessly (Bhad & Chavam, 2015).

Li-Fi Standardisation

Before digging into the complexities of the 802.11bb standard, it is important to note that standardisation remains in a competitive setting, with three major standards being created for optical communications (Boomgaarden, 2024). Aside from the 802.11bb, there is the 802.15.13 and the ITU T.G9991. While the former is still not being implemented, the latter is likely the most widely used nowadays due to the unique qualities of its chip (Boomgaarden, 2024). However, the article will examine the 802.11bb standard because of its future potential, as many experts in the field have referred to it as a foundation for op-

tical communications on a worldwide scale. Furthermore, this standard has been widely regarded as a big step towards commercial usage of the Light Fidelity (Choi, 2023).

The Institute of Electrical and Electronics Engineers (IEEE) approved the standard for mass, commercial use of Light Fidelity in June 2023, thereby providing the framework for its use on a global scale (Halper, 2023). Li-Fi distinguishes itself by using the optical spectrum for data transmission, a less congested area than the radio frequencies utilised in Wi-Fi. As we navigate the changing environment of wireless communication technologies, Light Fidelity stands out as a paradigm-shifting challenger. The recent certification of the IEEE 802.11bb standard is regarded as a watershed moment that will catapult Li-Fi from academic curiosity to industry-accepted technology (Van Gils, 2023). The ratification of the IEEE 802.11bb standard in June 2023 marked a crucial point in Li-Fi technology as it defined the physical layer specifications and system topologies, laying the groundwork for Li-Fi's widespread use. According to Rebecca Pool (2023), with an 802.11 specification, Li-Fi is poised to join Wi-Fi and accelerate the transmission of information to new levels.

Li-Fi formalises data rates ranging from as low as 10 Mbps up to a staggering 9.6 Gbps using invisible infrared light (Van Gils, 2023). The 802.11bb standard promises to revolutionise sectors ranging from general connectivity to high-security data transmission and smart home technologies (Van Gils, 2023). With the release of the IEEE 802.11bb standard, pureLiFi, a leading company in the field, believes that Li-Fi is now poised to take its place in the wireless communication market, offering unprecedented speed, security, and reliability to users around the world (Scace, 2021). The IEEE's adoption of the 802.11bb standard meant that Li-Fi is ready to address the mass-market requirements, such as low cost, low energy and high volumes. In the manner of institutional and operational capabilities, the industry can fully reuse Wi-Fi protocols over the light medium. This will bring traffic offloading, security and navigation capabilities of Wi-Fi to the next level (Scace, 2021). Li-Fi provides better bandwidth, efficiency, availability and security than Wi-Fi and has already achieved blisteringly high speed in the lab. By leveraging the low-cost nature of LEDs and lighting units, there are many opportunities to exploit this medium (Karthika & Balakrishnan, 2015). Examples of its usability are various and ranging from public internet access through streetlamps to auto-piloted cars that can communicate through their headlights.

Volker Jungnickel, technical editor of the task group on Li-Fi, from Fraunhofer HHI, referred to the IEEE 802.11bb standard as a critical step in enabling interoperability between multiple vendors, hence further enhancing Li-Fi's operational use. He praised the standard as it allows, for the first time, Li-Fi solutions inside the Wi-Fi ecosystem labelling this as essential for the development of new and innovative applications of the technology (Muller, 2023). PureLiFi CEO, Alistair Benham, used the standardisation of this technology to amplify his belief that Li-Fi can replace cables with short-range optical wireless links and connect numerous sensors and actuators to the Internet (Scace, 2021), hence revolu-

tionising the data transfer field and enhancing the decision-making on the battlefield.

Essentially, the structure developed in the aftermath of standardisation placed Li-Fi technology at the centre of future data transfer due to its exceptional speed, which can exceed 10 Gbps (Alleven, 2023). However, it is important to note that neither of the current standardisations are military-applicable or useful. As technology advances and its military potential becomes apparent, a new, military-specific standardisation will be required.

ANALYSIS OF LI-FI FOR MILITARY USE - OPTICAL TRANSFORMATION

Military operations take place in a variety of challenging environments, ranging from metropolitan landscapes to isolated battlefields and marine territories. This can be difficult for a secure wireless connection, as communication solutions that can work well in these harsh settings are critical. Traditional electromagnetic (EM) spectrum-based data networks are vulnerable to attack. Because of the nature of EM-spectrum technology, communications travel in all directions, providing enough opportunity for anyone with malicious intent to hijack these signals and gain access to networks. As a result, Li-Fi can be an effective solution to this vulnerability for a variety of important reasons (Lt. Lowry III & Second Lt. Suarez, 2019). As Boomgaarden aptly noted (2024), the whole area of critical communications in the warfare context must transform into an end-to-end light-based system. Li-Fi communication offers inherent resilience to environmental challenges, as demonstrated in a study conducted by the US Army Research Laboratory (Benson, 2018). The study found that Li-Fi systems can maintain reliable connectivity in underground bunkers, submarines, and other environments where radio signals struggle to penetrate. Furthermore, Li-Fi can be deployed in conjunction with existing infrastructure or portable setups, enabling rapid deployment in temporary or mobile command posts (Lifimax, 2024).

Li-Fi in Command-and-Control Centres

When talking about the most important aspects of Li-Fi technology, the first one to be mentioned must be its unique security characteristics, making it one of the safest ways to transfer data and communicate. Because light cannot penetrate through walls like radio waves, Li-Fi signals remain confined within a specific space. This characteristic, as well as advanced encryption methods, makes it extremely difficult for unsanctioned interception of sensitive data by outside parties (Boomgaarden, 2024). In military command and control (C2) operations, every second counts, and in that manner, Li-Fi communication offers exceptionally low latency to the military internet, ensuring that critical data reaches its destination with minimal delay. This near-instantaneous transmission is crucial for real-time decision-making, allowing personnel to respond swiftly to changing situations (Oledcomm, n.d.-d). On the one hand, traditional Wi-Fi networks are susceptible to cybersecurity breaches and electromagnetic interference from various sources, including electronic devices and other wireless signals.

Li-Fi, on the other hand, operates in the optical light spectrum, making it immune to such interference (Boomgaarden, 2024).

In highly secure environments such as military command centres or government agencies, the use of radio frequency-based communication technologies may be restricted due to potential security risks. The role of Li-Fi security is to provide a safe alternative that operates on light waves that do not propagate beyond the designated area (Lifimax, 2024). The fact that Li-Fi offers a high bandwidth of data exchange makes it an ideal tool for C2 centres on the battlefield, as the high bandwidth would ensure gaining a common operational picture (COP) in a faster and safer way.

Li-Fi's resistance to electromagnetic interference and its customisable structure make it a solution particularly suitable for communication systems in aircraft and naval vessels. Radio frequency-based communication technologies can be susceptible to interference from onboard electronics or external sources, potentially compromising communication reliability (Boomgaarden, 2024). Li-Fi communication systems installed on aircraft or naval platforms defy boundaries for connection and provide local and secure data transmission capabilities (Dinodia, 2024). In that manner, transformation to an end-to-end optical communication would mean the employment of lasers in long-range, e.g. ground-space, medium-range, e.g. ground-ground/air and short, individual communication ranges. The long-distance communication is mostly based on directed lasers, and that could prove to be the pillar of future laser-based communication. Boomgaarden (2024) states that current lasers are capable of ensuring secure and efficient medium and short-range communication systems, although systematic development efforts are needed to repurpose lasers and make them military-usable.

Li-Fi Technology in Naval Operations

When addressing naval operations, it is vital to emphasise that we mean any actions carried out at sea or connected to the maritime domain, which includes oceans, coastal areas, rivers, and ports (Vego, 2008). Naval operations frequently take place in a highly dynamic environment spanning numerous domains, necessitating seamless, high-speed, and secure communication under a variety of limitations. These activities cover a wide range, from fleet manoeuvring to submarine surveillance. As a result, communication systems must be strong enough to withstand cyber and physical attacks while remaining operationally efficient (Vego, 2008).

In the event of a 'dark' battlespace, with traditional RF-based communication systems vulnerable and non-usable, the Navy is left to operate similarly to the ships of sail, with no direct communication with the mainland, sticking to the broad, formerly established plan of action. In that sense, communication between fleet commanders to ship captains or fleet commanders and the mainland will no longer be a viable option. As the paper already touched upon, streamlined communication in the chain of command is of utmost importance for the success of maritime operations. Li-Fi technology could prove to be the difference maker in these situations, as it can allow fast and secure data transmission, enabling

fleet commanders to retain control and ensure mission success (Lt. Lowry III & Second Lt. Suarez, 2019).

Li-Fi's unique characteristics make it suitable for a wide range of applications for maritime operations. It can be used to ensure secure, high-speed data transmission between ships operating within a fleet. This is key for both Fleet Manoeuvres and Stealth Operations. Ships can maintain unhindered communication with each other by using visible/infrared light beams, eliminating the risk of detection. This will ensure secure transmission between ships, and the risk of being compromised by any RF interference or interception is low (Kumar, 2024). The reliance on LOS transmission between two Li-Fi systems onboard different platforms makes it harder for adversaries to intercept signals, thereby providing a secure alternative during hostile periods. Moreover, the Logistics and Maintenance aspect of naval missions could prove to be another field where this technology can have a major impact, especially considering the importance of managing multiple naval assets, as Li-Fi can be used to streamline communication between ships, bases and ports. Ships can use Li-Fi to communicate their maintenance status, supply needs or mission readiness without relying on vulnerable RF systems (Sullivan et al., 2021).

Underwater Operations

The underwater domain is of special interest when discussing battlefield communication, as the only current way of exchanging information and data is the acoustic method, considering that traditional RF-based communication does not work. This domain's importance lies in the existent critical infrastructure, pipelines and cables, which are unprotected. In that sense, underwater warfare will become more and more important to gain tactical advantage, hence, developing effective ways of conducting underwater communication between the ships, submarines, and platforms would ensure battlefield advantage (Boomgaarden, 2024). The communication networks between submarines and surface ships have been of utmost importance, as maintaining secure and undetectable communication in submarine warfare is crucial (Sullivan et al., 2021). Li-Fi can be used for both Submarine-to-Submarine and Ships-to-Submarine communications. If discussing the former, submarines could use blue-green light waves to communicate while submerged, hence ensuring safe and secure communications while maintaining the stealth component. In the latter case, Li-Fi would help submarines to stay connected with surface platforms without surfacing, keeping them safe from detection. This would significantly enhance safety, security and secrecy during naval operations (Kumar, 2024).

As Unmanned Aerial Vehicles (UAVs) and Autonomous Underwater Vehicles (AUVs) transform the future battlefields, having secure communication between these systems and their human operators is vital. Li-Fi technology could offer a significant breakthrough and change the landscape regarding Drone-to-Ship and AUV-to-Ship/Submarine communication. Drones could use light-based communication to relay ISR data to ships without relying on RF channels that could be intercepted or jammed, while AUVs conducting underwater missions could use this tech-

nology to send data to nearby vessels, creating an efficient network of underwater sensors (Kumar, 2024).

China is, without a doubt, the world leader in underwater communication development, as it is the only country having its own undersea optical communication test field. China appears to be a pioneering power in this sector, having transformed certain university facilities into optical underwater communication institutes (Boomgaarden, 2024). While we cannot be positive about the Chinese side's progress in this area, Europe and the United States are far behind. As Boomgaarden (2024) eloquently notes, optical underwater communication will play a crucial role in future wars, with so much essential infrastructure resting unguarded beneath the sea. It is worth noting that the trend of damaging this infrastructure has already caught on, and countries are struggling to find a way to stop it, mostly because of the inability to communicate safely and effectively.

Li-Fi Use in Crisis Management

Li-Fi's unique capabilities make it a promising solution for crisis and disaster management, where quick deployment, reliable communication, and security are critical. Its ability to deliver high-speed, localised data transmission can play a crucial role in enhancing communication infrastructure in scenarios where traditional wireless technologies might fail or be unavailable.

During natural disasters such as earthquakes, floods, or hurricanes, infrastructure damage often disrupts communication networks. Li-Fi systems, which can be deployed using portable LED lighting and photodetectors, offer a viable alternative (Priyadharsini et al., 2020). For example, emergency shelters or command centres can use Li-Fi to establish secure and high-speed local networks for coordinating relief operations (Oledcomm, n.d-a). Unlike Wi-Fi, Li-Fi is immune to electromagnetic interference, ensuring stable communication in environments saturated with electronic devices or competing signals (Haas et al., 2015).

Military units often assist in disaster relief efforts, providing logistics, medical aid, and security. In such scenarios, Li-Fi can facilitate

seamless communication between military personnel and first responders. Secure Li-Fi networks can be set up on a temporary basis to enable data sharing, real-time updates, and resource tracking, ensuring coordinated efforts across multiple agencies (Priyadharsini et al., 2020). Moreover, its localised nature enhances data security, reducing the risk of intercepted communications in conflict-prone areas during disaster response.

One proposed method is using Li-Fi balloons that contain the necessary communication equipment and the power source (Surampudi, 2017). Through a network system called LibNet, Li-Fi balloons can provide a secure and instant network between the disaster area (alerted by the victims) and the first responders (Surampudi, 2017). Traditional RF-based systems often face performance issues in densely populated disaster zones due to signal congestion, showing Wi-Fi's vulnerability (Van Wyk et al, 2023). Li-Fi on the other hand operates on the visible light spectrum, bypassing such limitations and providing a stable alternative (Oledcomm, n.d.-a). In disaster scenarios such as earthquakes or floods, Li-Fi can offer high-speed, interference-free communication for managing aid distribution, medical services, and public safety (Surampudi, 2018).

Case Study - Quantum-based Infrastructure Networks for Safety-Critical Wireless Data Communication (QuINSiDa) & Li-Fi

Quantum technology opens up many new areas of application, however, it also harbours risks. Due to their enormous computing power, quantum computers could undermine even the most modern encryption methods (AWC, 2024). The quantum key distribution (QKD) mechanism, while one of the most secure means of sending data, is nonetheless susceptible to jamming or disruption. Despite QKD's unique properties, the system remains insecure since it employs standard, frequency-based data transmissions. Connections are frequently vulnerable to assault at the last step, right before they reach the end user (BMBF, 2022). Optical communication would offer a much-needed safety net, rendering QKD resistant to external influences. Enabling optical communication in this context might provide a huge edge in cyber warfare by ensuring critical battlefield advantages in both encryption and decryption.

The QuINSiDa project should create a novel way to secure optical data transfer in wireless networks. This demonstrates how quantum keys created by photonic devices may be sent directly via LiFi networks (Flaherty, 2023). The project's goal is to demonstrate a quantum-based data communication network that wirelessly and flexibly links many end users to a secure backbone infrastructure or may be deployed independently as a secure campus network (Flaherty, 2023). This allows QKD, which was previously thought of as a building-to-building situation, to be carried to the end user.

TECHNICAL AND OPERATIONAL CHALLENGES OF LI-FI INTEGRATION

One of the primary technical challenges of Li-Fi technology is its dependence on line-of-sight (LOS) communication (Oledcomm, n.d-a). Unlike RF-based systems like Wi-Fi, which can transmit signals through walls and other obstacles, Li-Fi requires a direct or semi-direct path between the transmitter (light source) and receiver (Li-Fi Co, 2024a). This limitation makes the technology less effective in dynamic military environments, such as battlefields, where obstacles are common and rapid mobility is essential. While solutions like reflective surfaces and hybrid RF-Li-Fi systems have been proposed, these require further development to ensure reliable performance in such scenarios (Haigh, 2020; Noshad & Brandt-Pearce, 2014).

Li-Fi's effective range presents a notable limitation that hampers its practical usability, particularly in large-scale deployments (Singh and Sharma, 2020). The technology relies heavily on the strength of the light source and the sensitivity of the photodetector, confining its effective range to only a few metres under optimal conditions (Kuehner-Hebert, 2023). This limitation becomes even more pronounced in environments where the light source is obstructed or where ambient light interference reduces signal quality (Singh and Sharma, 2020). In comparison, Wi-Fi, which operates on RF signals, can deliver reliable connectivity over tens of metres indoors and even greater distances outdoors (Haiston, 2023). This scalability makes Wi-Fi far more suited for extensive military operations, such as establishing base-wide communication networks or ensuring connectivity in open combat zones, albeit the connectivity is limited in certain military settings due to security.

For example, military units requiring mobility or distributed operations would find Li-Fi's range a significant bottleneck, as it necessitates a dense network of light sources to cover even a moderately sized area. Additionally, the effectiveness of Li-Fi diminishes as distance increases, often requiring high-powered LEDs or advanced photodetectors to extend coverage, which adds to both energy demands and equipment costs (Sangikyo, 2021; Versa Technology, 2020). Unlike Wi-Fi, which can seamlessly penetrate walls and physical barriers, Li-Fi's dependence on direct or semi-direct line-of-sight further exacerbates its range limitations, hence making it impractical for scenarios that require long-distance communication or operations across multiple terrains (Haas et al., 2015).

Environmental factors pose yet another challenge for Li-Fi. Sunlight, for instance, can saturate photodetectors, while weather conditions like fog, rain, or dust can scatter light beams, significantly degrading signal quality (Kumar, 2024). These limitations make Li-Fi unsuitable for outdoor and all-weather military operations where RF-based technologies remain more robust (Rajagopal et al., 2012). Overcoming such challenges requires advancements in adaptive optics and environmental shielding to ensure consistent performance in diverse conditions (Li-Fi Co, 2024b).

Although Li-Fi offers higher theoretical bandwidth compared to RF systems, achieving this potential comes with substantial tech-

nical hurdles (Haiston, 2023). Sophisticated modulation techniques, such as Orthogonal Frequency Division Multiplexing (OFDM) and Intensity Modulation/Direct Detection (IM/DD), are required to maximise data rates and channel efficiency (Mohsin and Murdas, 2023; Tan et al, 2019). While these methods enable high-speed data transfer, they also increase the system's complexity and may introduce additional latency during data encoding and decoding. Such latency can pose challenges in mission-critical military operations, where even milliseconds can impact outcomes. For example, augmented reality (AR) systems used by soldiers for battlefield visualisation demand seamless and real-time data transfer to ensure accuracy and situational awareness (Kirrbach et al., 2019). Any lag or interruption caused by Li-Fi's modulation constraints could jeopardise the mission's success. Similarly, autonomous drones and robotics, which depend on continuous, high-bandwidth data streams for navigation and coordination, could suffer from performance degradation in environments where Li-Fi's theoretical advantages cannot be fully realised (Kumar, 2024).

Moreover, the high data rates achievable with Li-Fi necessitate optimal alignment between the light source and the receiver, which is often challenging in dynamic or mobile scenarios (Alshaer et al., 2021). Military applications often require robust communication systems that can adapt to rapid movements, sudden changes in positioning, or environmental disruptions (Lowry III, 2019). These scenarios further complicate the integration of advanced modulation techniques into Li-Fi systems. Research is ongoing to develop more adaptive and low-latency modulation protocols, but until these technologies mature, Li-Fi will remain less reliable for applications requiring instantaneous responses or constant high-speed connectivity (Linnartz et al., 2022).

Power consumption presents another critical concern when considering Li-Fi for military applications. While Li-Fi technology can leverage existing LED lighting systems for dual purposes—providing illumination and enabling data transmission—this dual functionality can result in increased energy demands. In scenarios requiring 24/7 communication, such as surveillance operations or secure data links in command centres, the continuous operation of LEDs for both lighting and communication significantly raises power requirements. This issue is particularly pressing in energy-constrained environments like remote military outposts, where access to power supplies is limited, or submarines, where operational efficiency hinges on conserving every watt of energy (Bennett, 2016).

Additionally, the increasing energy demands could lead to logistical complications in deployment. One advantage of Li-Fi in contrast to Wi-Fi is the low price and energy consumption (Pothanaicker, 2016). For example, power generators or energy storage systems in remote locations may need to be upgraded to accommodate the increased load, diverting resources from other mission-critical functions. Even in scenarios where solar or alternative energy sources are available, maintaining uninterrupted Li-Fi communication could place undue strain on the energy infrastructure (Chatterjee et al., 2015). Developing energy-efficient Li-Fi systems, such as low-power

LEDs or adaptive dimming techniques, is a potential solution. However, these advancements may come at the expense of signal quality or range, necessitating trade-offs that could limit Li-Fi's applicability in high-stakes military operations.

Finally, hardware compatibility significantly impacts Li-Fi adoption in military settings. The technology requires specialised photodetectors and transmitters, increasing costs and complicating logistics (GreyB, n.d.). Retrofitting existing military communication infrastructure to support Li-Fi would demand considerable investment in both hardware and training. Additionally, the lack of universal standards and cross-vendor interoperability further complicates integration with existing communication systems (Pathak et al., 2015).

Operational Challenges

In operational contexts, the deployment of Li-Fi in dynamic environments is a notable challenge. Combat zones or mobile command centres often require highly adaptable communication systems capable of functioning under constant movement (Faster Capital, 2024). Li-Fi's reliance on stationary light sources limits its application in such scenarios, particularly for troops or vehicles in transit. In these cases, RF-based systems remain more practical due to their inherent flexibility (Komine & Nakagawa, 2004).

Signal security is a double-edged sword for Li-Fi. On the one hand, its confined spatial range and the inability of light signals to penetrate walls make it inherently more secure against long-range interception compared to RF systems (To Be, n.d.). However, visible light beams could inadvertently expose the location of sensitive operations, posing risks for stealth missions. Enhancements like narrow-beam optics and encrypted communication can address this issue but add complexity to the system (Haas and Cogalan, 2019).

The cost and maintenance of Li-Fi systems also present substantial barriers to adoption. The high initial investment required for specialised LEDs, photodetectors, and network management systems can deter widespread use (Oledcomm, n.d-b.). Furthermore, maintaining these systems in harsh environments such as deserts or maritime settings introduces additional operational costs. For example, it is reported that the application of Li-Fi is challenged significantly in deep water due to environmental sensitivity and high costs (Das, n.d.). Environmental factors like heat, moisture, and physical wear can accelerate hardware degradation, reducing the technology's reliability and lifespan (Burchardt et al., 2014).

Interoperability is another significant operational hurdle. Military operations often rely on seamless communication across multiple platforms and units with advanced encryption methods (Oledcomm, n.d.-a). This is a requirement that Li-Fi struggles to meet due to its lack of universal standards (Livinus, 2023). This limitation can result in inefficiencies or vulnerabilities in joint operations, especially when attempting to integrate Li-Fi into existing RF-based networks (Badeel et. al, 2021). Addressing this challenge will require the development of standardised protocols and hybrid systems that leverage the strengths of both Li-Fi and RF technologies.

COMPARATIVE ANALYSIS WITH TRADITIONAL WIRELESS TECHNOLOGIES

Wireless communication systems have evolved significantly, with technologies like Wi-Fi and Bluetooth dominating the landscape due to their robustness, scalability, and widespread adoption. In contrast, Li-Fi, while a promising innovation, remains in its nascent stages. This section provides a detailed comparative analysis of Li-Fi and traditional wireless technologies, focusing on their capabilities, limitations, and suitability for various military applications.

Bandwidth and Speed

One of Li-Fi's most significant advantages over traditional wireless systems is its potential to deliver high-speed data transmission, leveraging the visible light spectrum. The visible spectrum offers bandwidths thousands of times greater than the RF spectrum, theoretically allowing Li-Fi to achieve data rates up to 224 Gbps (Haas et al., 2015). In comparison, Wi-Fi systems operating on RF bands are limited to a maximum theoretical speed of 9.6 Gbps under the latest Wi-Fi 6 standard (IEEE, 2021).

This bandwidth advantage positions Li-Fi as a viable option for data-heavy applications in military settings, such as real-time analytics, augmented reality (AR) systems for soldiers, and high-resolution video streaming for reconnaissance (Kirrbach et al., 2019). However, achieving these speeds in practical scenarios is contingent on ideal conditions, including a direct LOS, absence of ambient light interference, and proximity to the light source. In contrast, Wi-Fi and other RF-based technologies maintain consistent performance over greater distances and in environments where physical obstacles or adverse weather conditions are present (Rajagopal et al., 2012).

Range and Scalability

Wi-Fi's ability to operate over tens of meters indoors and even longer ranges outdoors provides a significant edge in terms of scalability. Its signals can penetrate walls, making it ideal for large-scale deployments, such as securing communication across an entire military base or in combat zones. In contrast, Li-Fi's effective range is typically limited to a few meters due to the reliance on visible light and photodetectors. This constraint necessitates a dense network of Li-Fi-enabled light sources to achieve the same level of coverage, increasing the infrastructure requirements and costs (Haas et al., 2015).

Furthermore, while Wi-Fi enables seamless connectivity in dynamic environments, such as mobile command centres or moving vehicles, Li-Fi struggles in these scenarios due to its need for a stable LOS. For example, in battlefield operations requiring constant movement, RF-based systems remain more practical and reliable. Although hybrid systems combining RF and Li-Fi technologies are being explored to address these limitations, they are not yet mature enough for widespread military adoption (Komine & Nakagawa, 2004).

Interference and Environmental Factors

Traditional wireless technologies face interference from other RF systems, which can degrade signal quality in environments saturated with electronic devices. Li-Fi, on the other

hand, is immune to electromagnetic interference, making it particularly attractive for sensitive military operations where electronic warfare or jamming is a concern (Burchardt et al., 2014).

However, Li-Fi is highly susceptible to environmental factors that do not impact RF technologies. For instance, sunlight can saturate photodetectors, and weather conditions like fog, rain, or dust can scatter visible light beams, significantly reducing signal quality. These vulnerabilities make Li-Fi unsuitable for outdoor or all-weather operations where traditional RF systems remain the preferred choice (Rajagopal et al., 2012). Advances in adaptive optics and environmental shielding could potentially mitigate these challenges, but such solutions are still under development.

Security Considerations

Li-Fi offers inherent security advantages due to the confined nature of light signals, which do not penetrate walls. This makes Li-Fi communication less susceptible to long-range interception or eavesdropping compared to RF-based systems. For military applications involving classified or sensitive information, this feature provides an added layer of protection (Badeel et al., 2021).

However, this security advantage is not without its caveats. The visible nature of Li-Fi signals can inadvertently expose the location of a light source, posing risks in stealth operations. In contrast, Wi-Fi and other RF systems, while more vulnerable to interception, do not have a physical signal footprint that can be easily detected. Implementing narrow-beam optics and encrypted communication protocols can enhance Li-Fi's security, but these measures increase system complexity and cost (Haas et al., 2015).

Power Efficiency

Energy efficiency is a critical consideration for both Li-Fi and traditional wireless technologies, especially in military contexts where power resources are often limited. Li-Fi systems can utilise existing LED lighting infrastructure, providing dual functionality for illumination and data transmission. This integration theoretically reduces energy consumption compared to deploying separate lighting and communication systems.

However, the continuous operation of LEDs for both lighting and data transmission can increase overall power requirements, particularly in scenarios demanding 24/7 connectivity. Wi-Fi systems, while not inherently more energy-efficient, do not require constant illumination and thus may prove more adaptable in power-constrained environments such as remote military outposts or submarines (Baeza and Garcia, 2023).

Hardware and Infrastructure

The widespread adoption of Wi-Fi and other RF-based systems has resulted in the development of standardised hardware and protocols, enabling seamless integration across multiple platforms. In contrast, Li-Fi requires specialised photodetectors, LEDs, and modems, which complicates its deployment and increases costs (Pathak et al., 2015). Additionally, retrofitting existing military infrastructure to accommodate Li-Fi would require significant investment in both hardware and personnel training.

Moreover, the lack of universal standards for Li-Fi further hampers its interoperability with existing communication systems. For joint operations involving multiple military units or allied nations, this lack of standardisation could result in inefficiencies or vulnerabilities. Wi-Fi, with its established ecosystem and cross-vendor compatibility, remains the more practical choice for such scenarios (The WiFi Specialist, n.d.).

Application Suitability

The choice between Li-Fi and traditional wireless technologies ultimately depends on the specific requirements of the application. For indoor environments where high-speed data transfer and enhanced security are priorities, such as command centres or secure communication hubs, Li-Fi offers distinct advantages. In contrast, Wi-Fi and RF-based systems are better suited for outdoor, large-scale, or mobile deployments, where range, scalability, and environmental resilience are critical factors.

Hybrid systems combining the strengths of Li-Fi and RF technologies represent a promising avenue for future development. By leveraging Li-Fi for high-speed, secure data transfer in localised environments and using RF systems for long-range communication, such solutions could offer a balanced approach to military communication challenges. However, realising this vision will require advancements in hardware, standardisation, and integration protocols (Komine & Nakagawa, 2004).

CONCLUDING REMARKS

The exploration of Li-Fi as a cutting-edge communication technology underscores its transformative potential in addressing the limitations of traditional RF-based systems. With its unprecedented bandwidth, inherent security advantages, and energy-efficient design, Li-Fi stands poised to redefine wireless communication across a spectrum of applications, particularly in the military domain. As military operations grow increasingly complex and technology-dependent, the need for secure, high-speed, and reliable communication systems becomes paramount. Li-Fi's ability to deliver on these fronts positions it as a critical asset for modern defence strategies.

In military command and control centres, Li-Fi's high-speed data transmission and resistance to electromagnetic interference offer significant operational advantages. By enabling real-time decision-making and ensuring secure data exchange, Li-Fi can enhance situational awareness and streamline mission coordination. Its localised nature reduces the risk of interception, providing a robust communication solution for sensitive operations. Similarly, in naval operations, Li-Fi's capacity for secure and interference-free communication can revolutionise fleet coordination and underwater communication, addressing long-standing challenges associated with traditional RF systems.

The unique attributes of Li-Fi also make it an invaluable tool for crisis management and disaster response. Its ability to establish localised, high-speed networks in the absence of traditional infrastructure can facilitate seamless coordination among first responders and military personnel, enhancing the effective-

ness of relief efforts. The development of innovative deployment methods, such as Li-Fi-equipped balloons or portable LED systems, further expands its applicability in emergency scenarios.

However, the integration of Li-Fi into military communication networks is not without challenges. Its reliance on LOS communication and its limited range necessitate further advancements in technology and infrastructure. Environmental factors, such as sunlight and weather conditions, pose additional hurdles that must be addressed through adaptive optics and shielding solutions. Moreover, the high initial costs and the need for specialised hardware highlight the importance of strategic investment and phased implementation.

To fully realise the potential of Li-Fi, a hybrid approach that combines its strengths with those of RF-based systems offers a promising path forward. By leveraging Li-Fi for secure, high-speed, and localised communication and utilising RF technologies for long-range connectivity, military forces can achieve a balanced and resilient communication network. The recent standardisation of Li-Fi through the IEEE 802.11bb framework marks a significant milestone, paving the way for broader adoption and interoperability across platforms.

Looking ahead, continued research and development will be crucial in overcoming the technical and operational challenges associated with Li-Fi. Innovations in modulation techniques, photodetector sensitivity, and energy-efficient designs will further enhance its viability for military applications. As countries invest in next-generation communication technologies to gain strategic advantages, Li-Fi's role in shaping the future of defence communications cannot be overstated.

In conclusion, Li-Fi represents a revolutionary leap in wireless communication, offering a secure, high-speed, and environmentally sustainable alternative to traditional systems. Its potential to address the critical communication needs of military operations, coupled with its adaptability to diverse environments, positions it as a cornerstone of future defence strategies. By embracing Li-Fi and fostering its integration with existing technologies, military forces can enhance their operational capabilities, ensuring readiness and resilience in an increasingly complex and interconnected world.

BIBLIOGRAPHY

Alleven, M. (2023, July 13). *IEEE releases LiFi standard*. Fierce Network. https://www.fierce-network.com/tech/ieee-standardization-shines-spotlight-lifi

Alshaer, H., Haas, H., & Kolawole, O. Y. (2021, June). An optimal networked LiFi access point slicing scheme for internet-of-things. In 2021 IEEE International Conference on Communications Workshops (ICC Workshops) (pp. 1-6). IEEE.

AWC. (2024). *Unifying LiFi with QKD*. Asianwirelesscomms.com. https://asianwirelesscomms.com/product-service-details?itemid=6154&post=unifying-lifi-with-qkd-461143

Badeel, R., Subramaniam, S. K., Hanapi, Z. M., & Muhammed, A. (2021). A Review on LiFi Network Research: Open Issues, Applications and Future Directions. *Applied Sciences*, *11*(23), 11118. https://doi.org/10.3390/app112311118

Baeza, V. M., & Garcia, R. A. (2023). LiFi Technology Overview: taxonomy, and future directions. arXiv preprint arXiv:2303.09690.

Bao, X., Yu, G., Dai, J., & Zhu, X. (2015). Li-Fi: Light fidelity-a survey. *Wireless Networks*, *21*(6), 1879–1889. https://doi.org/10.1007/s11276-015-0889-0

Boomgaarden, G. (2024, December 5). FINABEL - Consultation with the Managing Director of Aerolifi Company. Interview on Teams.

Bennett, T. (2016, August 10). *Naval Applications for LiFi: The Transmitting Tool*. Center for International Maritime Security. https://cimsec.org/naval-application-tech-lifi/

Benson, J. (2018). *Seeing the light: LiFi will revolutionize IT on mission command posts*. www.army.mil. https://www.army.mil/article/213936/seeing_the_light_lifi_will_revolutionize_it_on_mission_command_posts

Bhad, S. A., & Chavam, V. M. (2015). Li-Fi (Light Fidelity)-The Future Technology in Wireless Communication. *IJLTEMAS*, *IV*(VIII).

BMBF. (2022). *QuINSiDa — Vernetzung und Sicherheit digitaler Systeme*. Forschung-It-Sicherheit-Kommunikationssysteme.de. https://www.forschung-it-sicherheit-kommunikationssysteme.de/projekte/quinsida

Burchardt, H., Serafimovski, N., Tsonev, D., Videv, S., & Haas, H. (2014). VLC: Beyond Point-to-Point Communication. *IEEE Communications Magazine*, *52*(7), 98-105. https://doi.org/10.1109/MCOM.2014.6852089

Chatterjee, S., Agarwal, S., & Nath, A. (2015). Scope and challenges in light fidelity (LiFi) technology in wireless data communication.

Choi, C. Q. (2023). *Wi-Fi Boosts New, Ultrafast Li-Fi Standards - IEEE Spectrum*. Spectrum.ieee.org. https://spectrum.ieee.org/lifi-standards

Das, S. D. (n.d.). An Extensive Review on Underwater LiFi Technology in Defence Applications. *Veer Surendra Sai University of Technology*

Dinodia, N. P. (2024). Enhancing Wireless Communication with Li-Fi Technology: Development and Implementation for High-Speed, Visible Light Communication Systems. *Darpan International Research Analysis*, *12*(3), 352–362. https://doi.org/10.36676/dira.v12.i3.94

Fabiyi, S. D. (2016). Li-Fi: A Full-Fledged Wireless Communication Technology. *International Journal of Science and Research (IJSR)*, *5*(4), 1033–1036. https://doi.org/10.21275/v5i4.nov162213

FasterCapital. (n.d.). *Staying connected: Communication in the combat zone*. Retrieved January 8, 2025, from https://fastercapital.com/content/Staying-Connected--Communication-in-the-Combat-Zone.html#The-Lifeline-of-Communication-in-the-Combat-Zone.html

Flaherty, N. (2023, February 13). *Using LiFi to carry QKD quantum crypto keys*. EeNews Europe. https://www.eenewseurope.com/en/using-lifi-to-carry-qkd-quantum-crypto-keys/

GreyB. (n.d.). *How the researchers overcame one of LiFi problems?* GreyB. https://www.greyb.com/blog/lifi-problems-solutions/

Guan, H., & Hina, M. D. (2024). A Study on the Feasibility of LiFi in an Intra-Vehicular Data Transmission Application. *IEEE Access*, *12*, 42594–42613. https://doi.org/10.1109/access.2024.3376658

Haas, H. (2011). Wireless data from every light bulb | Harald Haas [YouTube Video]. In *YouTube*. https://www.youtube.com/watch?v=NaoSp4NpkGg

Haas, H., & Cogalan, T. (2019, August). LiFi opportunities and challenges. In 2019 16th International Symposium on Wireless Communication Systems (ISWCS) (pp. 361-366). IEEE.

Haas, H., Yin, L., Wang, Y., & Chen, C. (2015). What is lifi?. *Journal of lightwave technology*, *34*(6), 1533-1544.

Haigh, P. A. (2020). *Visible Light: Data communications and applications*. IOP Publishing.

Haiston, J. (2023, July 18). *Li-Fi vs Wi-Fi*. Symmetry Electronics. https://www.symmetryelectronics.com/blog/li-fi-vs-wi-fi/?srsltid=AfmBOoqbnTUOm-RxXU-69eZl-b4Z_2eAMtnQOL5RGOAl0bIMv-azdz4RG

Halper, M. (2023). At last: IEEE approves a Li-Fi standard (UPDATED). *Ledsmagazine.com*. https://doi.org/105437348.64b160daaa762

Hu, H., Zhu, K., & Liu, H. (2018). Research on the construction of Maritime Intelligent Emergency Command System. *Proceedings of the 2018 International Conference on Mathematics, Modelling, Simulation and Algorithms (MMSA 2018)*. https://doi.org/10.2991/mmsa-18.2018.111

IEEE. (2021, December 6). *IEEE 802.11ax-2021*. IEEE Standards Association. https://standards.ieee.org/ieee/802.11ax/7180/

Karthika, R., & Balakrishnan, S. (2015). Wireless Communication using Li-Fi Technology. *SSRG – IJECE*, *2*(3).

Kirrbach, R., Faulwaßer, M., Jakob, B., Schneider, T., & Noack, A. (2019, October). Li-Fi for

Augmented Reality Glasses: A Proof of Concept. In *2019 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)* (pp. 263-268). IEEE.

Komine, T., & Nakagawa, M. (2004). Fundamental analysis for visible-light communication system using LED lights. *IEEE transactions on Consumer Electronics*, *50*(1), 100-107.

Kuehner-Hebert, K. (2023, April 14). *Welcome, Li-Fi: Technology uses light to transmit data*. Electrical Contractor Magazine. https://www.ecmag.com/magazine/articles/article-detail/welcome-li-fi-technology-uses-light-to-transmit-data

Kumar, A. (2024, October 21). *Emerging Communication Technology Light Fidelity (Li-Fi) – A Game Changer for Modern Maritime Operations – CENJOWS*. Cenjows.in. https://cenjows.in/emerging-communication-technology-light-fidelity-li-fi-a-game-changer-for-modern-maritime-operations/

Kuttan, D. B., Kaur, S., Goyal, B., & Dogra, A. (2021). Light Fidelity: A future of wireless communication. *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, *198*, 308–312. https://doi.org/10.1109/icosec51865.2021.9591685

LiFi.Co. (n.d.-a). *LiFi eBook*. LiFi.co. https://lifi.co/lifi-ebook/

LiFi.Co. (n.d.-b). *LiFi White Paper*. LiFi.co. https://lifi.co/lifi-white-paper/

Lifimax. (2024, March 8). *The Role of LiFi in Command and Control Centers with Internet for Military Connectivity - LiFiMAX*. LiFiMAX . https://lifimax.ch/2024/03/08/the-role-of-lifi-in-command-and-control-centers-with-internet-for-military-connectivity/

Linnartz, J.-P. M. G., Hoelen, C., van Voorthuisen, P., Bitencourt Cunha, T. E., & Tao, H. (2022). LED assessment based on an improved quality factor for LiFi communication. In J. K. Kim, M. R. Krames, & M. Strassburg (Eds.), *Light-Emitting Devices, Materials, and Applications XXVI* (pp. 1-17). Article 120220F (Proceedings of SPIE - The International Society for Optical Engineering; Vol. 12022). SPIE. https://doi.org/10.1117/12.2611453

Livinus, C. (2023, November 17). *LiFi Acceptance: A Closer Look at the Global Integration and Adoption Challenges of LiFi Technology*. LiFi Tech News. https://www.lifitn.com/blog/lifiacceptance

Lowry III, P., & Suarez, M. (2019, November). Li-Fi Could Light Up the Dark Battlefield. *Proceedings*, *145/11/1,401*. The U.S. Naval Institute . https://www.usni.org/magazines/proceedings/2019/november/li-fi-could-light-dark-battlefield

Maher, M. (2007). Joint Tactical Radio System: Tactical Network Planning and Management. *MILCOM 2007-IEEE Military Communications Conference*, 1–7. https://doi.org/10.1109/milcom.2007.4455104

Mohsin, M. J., & Murdas, I. A. (2023). Performance analysis of an outdoor Li-Fi system-based AO-OFDM architecture under different FSO turbulence and weather conditions. *Optik*, *273*, 170427.

Müller, M. (2023). *Fraunhofer Heinrich Hertz Institute HHI*. Fraunhofer.de. https://newsletter.fraunhofer.de/-viewonline2/17386/789/3/6RFhct0v/n28DsXXw3G/1

Noshad, M., & Brandt-Pearce, M. (2014). Hadamard-Coded Modulation for Visible Light Communications. *IEEE Transactions on Communications, 64*, 1167-1175.

Oledcomm. (n.d.-a). *7 Ways LiFi Technology Revolutionizes Government Organizations*. Oledcomm. Retrieved December 5, 2024, from https://www.oledcomm.net/blog/7-ways-lifi-revolutionizes-govt-organizations/

Oledcomm. (n.d.-b). *Best military communication devices (2024-2025)*. https://www.oledcomm.net/blog/military-communication-devices/

Oledcomm. (n.d.-c). *LiFi vs WiFi: Understanding Core Differences*. Oledcomm. Retrieved December 5, 2024, from https://www.oledcomm.net/blog/lifi-vs-wifi/

Oledcomm. (n.d.-d). *The Role of LiFi in Command and Control Centers with Internet for Military Connectivity*. Oledcomm. Retrieved December 1, 2024, from https://www.oledcomm.net/blog/lifi-in-control-and-command-centers/

Pathak, P. H., Feng, X., Hu, P., & Mohapatra, P. (2015). Visible light communication, networking, and sensing: A survey, potential and challenges. IEEE communications surveys & tutorials, 17(4), 2047-2077.

PEO C3N. (n.d.). *Joint battle command-platform*. https://peoc3n.army.mil/Organizations/PM-Mission-Command/Joint-Battle-Command-Platform/

Pool, R. (2023, September 13). *Li-Fi: The Networking Standard That Could Change Wireless - EE Times Europe*. EE Times Europe. https://www.eetimes.eu/the-networking-standard-that-could-change-the-wireless-industry/

Pothanaicker, K. (2016). Survey and Challenges of Li-Fi with Comparison of Wi-Fi. 10.1109/WiSPNET.2016.7566262.

Priyadharsini, K., Kumar, J. D., Babu, C. G., Surendiran, P., Sankarshnan, S., & Saranraj, R. (2020, September). An experimental investigation on communication interference and mitigation during disaster using lifi technology. In *2020 International Conference on Smart Electronics and Communication (ICOSEC)* (pp. 794-800). IEEE.

pureLiFi. (n.d.). *About LiFi*. PureLiFi. https://www.purelifi.com/about-lifi/

Rajagopal, S., Roberts, R. D., & Lim, S. K. (2012). IEEE 802.15. 7 visible light communication: modulation schemes and dimming support. *IEEE Communications Magazine*, *50*(3), 72-82.

Sangikyo. (2021, August 17). *What's Li-Fi (2) Can you communicate with non line of sight?* Sangikyo. https://www.sangikyo.co.jp/article_service/led/blog/en/blog2021-6EN.html

Scace, S. (2021, December 8). *Pure LiFi*. PureLiFi. https://www.purelifi.com/us-army-expand-lifi-deployment/

Sharma, R., Raunak, & Akshay Sanganal. (2013). *Li-Fi Technology Transmission of data through light*. https://www.semanticscholar.org/paper/Li-Fi-Technology-Transmission-of-data-through-light-Sharma-Raunak/11d9bd7a32c6c96647461caaff0e1d221aba02eb

Singh, V., & Sharma, S. (2020). CHALLENGES AND OPPORTUNITIES OF LIGHT FIDELITY (LI-FI). *International Research Journal of Modernization in Engineering Technology and Science*, *02*(09).

Sullivan, B. P., Arias Nava, E., Desai, S., Sole, J., Rossi, M., Ramundo, L., & Terzi, S. (2021). Defining Maritime 4.0: Reconciling principles, elements and characteristics to support maritime vessel digitalisation. *IET Collaborative Intelligent Manufacturing*, *3*(1), 23–36. https://doi.org/10.1049/cim2.12012

Surampudi, A., Chapalgaonkar, S. S., & Arumugam, P. (2018, February). Can balloons produce Li-Fi? A disaster management perspective. In 2018 Global LIFI Congress (GLC) (pp. 1-5). IEEE.

Surampudi, A., Chapalgaonkar, S.S., & Paventhan, A. (2017). Can balloons produce Li-Fi? A disaster management perspective. *2018 Global LIFI Congress (GLC)*, 1-5.

Tan, Y., Wu, X., & Haas, H. (2019). Performance Comparison Between Coherent and DCO-OFDM LiFi Systems. *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, 1-6.

The WiFi Specialist. (n.d.). *Enhancing Connectivity for the Military: Robust Army WiFi Solutions* . The WiFi Specialist. Retrieved December 11, 2024, from https://thewifispecialist.co.uk/military-army-wifi/

To Be. (n.d.). *Li-Fi Technology*. To Be - Soluzioni LiFi. Retrieved December 5, 2024, from https://tobe-srl.it/en/lifi-security-network/

Van Gils, J. (2023, September 14). *Understanding the IEEE 802.11bb Li-Fi Standard and its Transformative Potential*. Copperpod IP. https://www.copperpodip.com/post/understanding-the-ieee-802-11bb-li-fi-standard-and-its-transformative-potential

Van Wyk, H., Cruz-Antonio, O., Quintero-Perez, D., Garcia, S. D., Davidson, R., Kendra, J., & Starbird, K. (2023). Searching for signal and borrowing wi-fi: Understanding disaster-related adaptations to telecommunications disruptions through social media. International Journal of Disaster Risk Reduction, 86, 103548.

Vego, M. (2008). *Operational Warfare at Sea*. Routledge.

Velastegui, N., Pavon, E., Jacome, H., Torres, F., & Pico, M. (2022). Technological advances in military communications systems and equipment. *Minerva*, *3*(8), 61–73. https://doi.org/10.47460/minerva.v3i8.65

Versa Technology. (2020, December 22). *Li-Fi: Internet at the Speed of Light | The Future of Networking*. Versa Technology. https://versatek.com/li-fi-internet-at-the-speed-of-light/?srsltid=AfmBOoqUXs2791b8Czc3kfgOrwyXG2vdJMKRRZnPWQj8qOlnhJbYELgK

Created in 1953, the Finabel committee is the oldest military organisation for cooperation between European Armies: it was conceived as a forum for reflections, exchange studies, and proposals on common interest topics for the future of its members. Finabel, the only organisation at this level, strives at:

- Promoting interoperability and cooperation of armies, while seeking to bring together concepts, doctrines and procedures;
- Contributing to a common European understanding of land defence issues. Finabel focuses on doctrines, trainings, and the joint environment.

Finabel aims to be a multinational-, independent-, and apolitical actor for the European Armies of the EU Member States. The Finabel informal forum is based on consensus and equality of member states. Finabel favours fruitful contact among member states' officers and Land Force Commanders in a spirit of open and mutual understanding via annual meetings.

Finabel contributes to reinforce interoperability among its member states in the framework of the North Atlantic Treaty Organisation (NATO), the EU, and *ad hoc* coalition; Finabel neither competes nor duplicates NATO or EU military structures but contributes to these organisations in its unique way. Initially focused on cooperation in armament's programmes, Finabel quickly shifted to the harmonisation of land doctrines. Consequently, before hoping to reach a shared capability approach and common equipment, a shared vision of force-engagement on the terrain should be obtained.

In the current setting, Finabel allows its member states to form Expert Task Groups for situations that require short-term solutions. In addition, Finabel is also a think tank that elaborates on current events concerning the operations of the land forces and provides comments by creating "Food for Thought papers" to address the topics. Finabel studies and Food for Thoughts are recommendations freely applied by its member, whose aim is to facilitate interoperability and improve the daily tasks of preparation, training, exercises, and engagement.

FINABEL
Quartier Reine Elisabeth
Rue d'Evere 1 box 44
B-1140 BRUSSELS

Tel: +32 (0)2 441 79 05 – GSM: +32 (0)483 712 193
E-mail: info@finabel.org

You will find our studies at **www.finabel.org**

Responsible publisher: Mario BLOKKEN - Finabel Permanent Secretariat - QRE - Rue d'Evere,1 - B-1140 Brussels - +32 (0)2 411 79 05