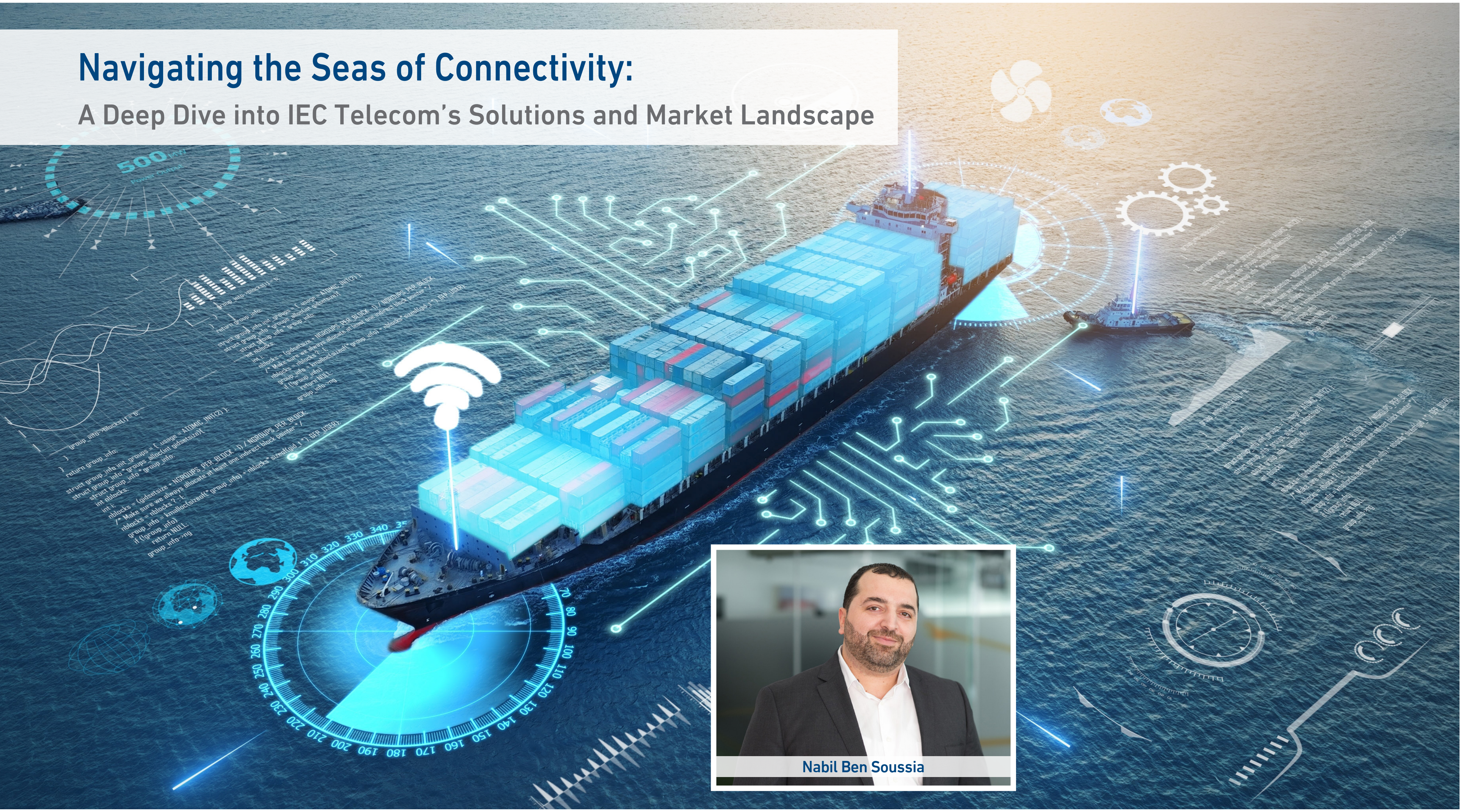

Navigating the Seas of Connectivity:

A Deep Dive into IEC Telecom's Solutions and Market Landscape

Nabil Ben Soussia

2023 witnessed significant shifts with the entry of major LEO players. These pioneers not only revolutionized data speeds, outperforming traditional VSAT services, but also introduced a new era of possibilities for seafarers through advanced digitalization.

Looking into the future, Nabil Ben Soussia, Group CCO, IEC Telecom discusses the ongoing advancements in LEO constellations and hybrid solutions, projecting a remarkable growth in the maritime satellite market.

Robban Assafina's interview with Ben Soussia further explores the influence of industry standards and regulations on the adoption of cybersecurity measures on board. With mandatory cyber policies introduced by the IMO, ship owners are compelled to establish a robust cyber risk management strategy.

How have LEO constellations changed the landscape of satellite-based communication for vessels in recent years?

In 2023, the maritime industry witnessed a significant transformation with the entry of two prominent Low Earth Orbit (LEO) players. Starlink took advantage of its first-mover status by introducing its marine portfolio in February. Just a few months later, in June, OneWeb announced the successful completion of its satellite constellation, offering maritime services to the seafaring community. These groundbreaking events forever altered the market landscape. The new operators revolutionized data speeds, delivering rates 20 times faster than traditional VSAT services, all while maintaining competitive pricing similar to GSM plans.

These advancements ushered in a new era of possibilities for seafarers, enabling them to harness the full potential of digitalization. This included advanced ship management through real-time data capture, enhanced crew welfare, access to educational and development programs, and much more.

However, with increased digitalization comes heightened cybersecurity risks. The maritime industry has witnessed a steady rise in cyberattacks in recent years, with numerous global ports falling victim to hacking incidents in 2023. Additionally, there has been a significant surge in maritime companies paying ransomware. According to a recent study conducted by the law firm HFW and maritime cybersecurity company CyberOwl, the average cost of unlocking computer systems in the maritime sector reached $3.2 million in 2023. A striking 14% of maritime industry professionals surveyed admitted to paying ransomware, a stark increase from the 3% reported in 2022.

Addressing these cybersecurity challenges is not a one-size-fits-all solution; it demands tailored approaches based on individual vessel operations and chain of command. Recognizing this evolving trend, IEC Telecom has introduced a cutting-edge cybersecurity solution known as OptiShield. This comprehensive toolkit was meticulously designed to meet the current requirements of ICT professionals. OptiShield offers essential threat protection and detection, while IEC Telecom's remote experts serve as a dedicated cyber incident team, ensuring vessels are equipped to execute an effective response and swiftly return to normal operations.

Tell us about the hybrid solutions' adaptation to the dynamic nature of vessels.

While LEO is gaining momentum, it will take a while before the new tech gets licensed by all seafarer nations. As a result, having LEO onboard is not enough. To ensure continuous digitalization, now more than ever, it is essential to equip your vessels with resilient backup infrastructure.

For example, think of our internet connectivity at home. Should our WIFI go down, we hop on our cellular hotspot. Hybrid solutions are designed to do just that: ensure continuity of digital operations based on the available network. A network management system, like OneGate by IEC Telecom, is the key engine of hybrid solutions. Its core mission is to support seamless failover between prime LEO, L-band back-up and LTE at least cost of routing.

While LEO and LTE can equally support real-time applications, L-band delivers up to 700 Kbs speed, significantly restricting digital operations on board. To resolve these technical issues and ensure business continuity even in low-bandwidth environments, IEC Telecom has developed a set of optimised applications which can enable critical apps, such as videoconferencing, video surveillance, remote maintenance, and telemedicine even under 100 kbps.

How do industry standards and regulations influence the adoption of cyber security measures on board?

Cybersecurity is no longer optional for vessels, with mandatory cyber policies introduced by IMO's MSC 428(98) Resolution, which took effect on January 1, 2021. The regulations followed a steep rise in the use of connectivity and data transfers on vessels during the COVID-19 pandemic, and data usage is expected to continue to rise.

In supporting ship owners with compliance, various organisations have crafted overarching recommendations, providing a structured framework for the establishment of a cyber risk management strategy. Ship owners can leverage them to identify and evaluate risks, safeguard their assets, and effectively address cyber threats, including response and recovery measures. In 2022, IMO further expanded its cyber security guidelines. In MSC-FAL.1/Circ.3/Rev.2, issued on June 7, the international organization recommended a new framework for enhancing cybersecurity in the maritime industry.

What about the future of vessel connectivity, considering the ongoing advancements in LEO constellations and hybrid solutions?

LEO technologies are undeniably reshaping market dynamics in the satellite communication industry.

This noteworthy evolution is set to have a profound impact on the maritime sector, catalyzing the widespread adoption of digitalization at sea. Statistically, the global maritime satellite market is projected to reach a remarkable $4.5 billion by 2030, boasting an impressive compound annual growth rate (CAGR) of 7%. Moreover, the adoption of LEO satellites in maritime applications is expected to surge, reaching an impressive 65% by the year 2027.

What implications does this hold for the maritime sector? It signifies a future marked by heightened automation, enhanced operational efficiency, and better working conditions, all of which present enticing prospects for the tech-savvy Generation Z.

What measures are being taken to safeguard against potential cyber risks to ensure the resilience and integrity of maritime operations?

Current cyber security infrastructure includes three layers of risk mitigation:

Risk Mitigation at the Level of Satcom Service Delivery: Satellite service operators are responsible for establishing a secure network architecture. With "point-to-point connectivity", all traffic is routed via satellite, which significantly reduces exposure to potential threats from terrestrial infrastructure.

Risk Mitigation at the Level of Service Providers: Next come service providers with a range of value-added services. Cyber packages start from basic email antiphishing to more advanced antivirus solutions. Additionally, service providers take charge of network development on board. Systems like OneGate by IEC Telecom allow the segregation of operational environments, reducing risks of cross-contamination. Risk Mitigation at the Level of the Managing Company: Vessel owners and operators are responsible for the actual deployment and adherence to cyber protocols. This includes investing in the technical set-up, establishing comprehensive user policies, and providing sufficient training to personnel.

Lastly, we must emphasize that cyber security on-board is greatly influenced by end-user behavior. To achieve success, it is imperative to foster a culture where seafarers genuinely recognize the importance of adhering to internal policies and following established rules. This cultural approach will play a pivotal role in ensuring the overall security of our operations.