Maritime Research and Technology

MRT
ISSN 2812-5622

http://dx.doi.org/10.21622/MRT.2024.03.1.747

The Influence of Computerized Simulation Techniques on Maritime Security Exercises: ISPS Code

Ahmed Mohy Ibrahim

Head of Quality Assurance Unit at Regional Maritime Security Institute, Arab Academy for Science, Technology and Maritime Transport (RMSI - AASTMT), Alexandria, Egypt.
ORCID: (0000-0001-5582-382X)

Emails: ahmedmohyyy@aast.edu, ahmedmohyy@gmail.com

Received on: 07 November 2023 Accepted on: 03 December 2023 Published on: 15 February 2024

ABSTRACT

Purpose: *Maritime security necessitates adept collaboration among port facility security teams, seafarers, and governing authorities. Maritime Education and Training (MET), guided by international standards, conforms to their competence and proficiency, especially in security exercises, boosting understanding of roles and responsibilities in challenging security scenarios. The pivotal role of international maritime communities in shaping future MET by embracing computerized simulation techniques indicates a new era in maritime safety simulations but lacks insights into adopting security scenarios. Revolutionizing the use of computerized simulators for seafarers in maritime safety sectors is advancing, yet there is limited intervention in security exercises.*

Design/Methodology/Approach: *This study explores integrating immersive technologies into theoretical "tabletop exercises", aiming to enhance the strengthening of realistic exposure to high-risk scenarios. The research emphasizes the significance of MET guided by international standards and proposes leveraging computerized simulation techniques, aiming to revolutionize security exercises. Employing a descriptive and analytical exploration approach, this study offers a thorough examination of challenges within maritime security training. It provides a comprehensive overview by not only describing the current state but also critically analyzing the potential impacts and effectiveness of immersive technologies. This assessment focuses specifically on how these technologies enhance practical training for maritime security personnel.*

Key-words:
Computerized Simulation Immersive Technologies, ISPS Code, Maritime Security Exercises, MET

MRT
ISSN 2812-5622
http://dx.doi.org/10.21622/MRT.2024.03.1.747

INTRODUCTION

The maritime industry's ongoing digital transformation is driving rapid change and is expected to persist as the maritime sector becomes more intelligent and automated, especially in Maritime Education and Training (MET) (Cicek et al., 2019; Tijan et al., 2021). Operating within a multifaceted global scene of challenges and risks, the complex maritime environment increasingly demands enhanced connectivity and technological advancements. Emphasizing the less focused aspects of the International Ship and Port Facility Security (ISPS) Code's measures, several areas might receive comparatively less attention. Focusing on leveraging emerging technologies presents a pivotal opportunity to mitigate severe security risks within maritime port facilities and onboard vessels, an area receiving comparatively less attention than safety in the industry's agenda (Bueger, 2015; Dalaklis, 2017; Tijan et al., 2021).

Furthermore, ensuring controlled technology integration to educate and train personnel is crucial in addressing the array of threats and vulnerabilities in this complex smart maritime industry (Ben Farah et al., 2022). Throughout history, the sea-to-shore interface has been a source of wealth and risk (Pagán et al., 2016). It remains vital for coastal governments to sustainably manage and protect sea resources (UNCLOS, 1982). The future vision of the Sustainable Development Goals (SDGs) for the international maritime community's efforts to conserve and responsibly utilize marine resources from inland waters to the high seas emphasizes the need for advanced security education and training scenarios within MET programs and assets to equip seafarers and Port Facility Security Personnel (PFSP), decision-makers, support agencies (such as bomb squads and firefighting teams), and stakeholders with skills and updated knowledge necessary from advanced security exercises approaches (Bueger et al., 2020; IMO, 2003; Kim et al., 2021; Ringsberg and Cole, 2020). At present, security exercises adhere to the basic requirements outlined in the ISPS Code, including the utilization of a traditional tabletop simulation approach (IMO, 2003). There is a missed opportunity to utilize advanced computerized simulation techniques (immersive technologies) compatible with technological advances to effectively address the evolving challenges and emerging risks in the maritime industry (Felsenstein et al., 2013; Mallam et al., 2019).

LITERATURE REVIEW

The absence of integrating immersive technological solutions by some maritime security exercise providers may potentially delay the progression of several aspects within the advancing trends of the smart maritime industry (Dewan et al., 2023). Furthermore, this oversight overlooks essential aspects, especially in fostering the mindset of security experts and their skills and knowledge. This encompasses the need for refined strategies, including rehabilitation techniques, to address piracy, armed robbery, cyber threats, vulnerabilities, and other increasingly relevant challenges and risks within today's dynamic and technologically advanced maritime industry (Tam and Jones, 2018). Consequently, maritime security personnel face ineffective preparation in dealing with emergent risks such as cyber threats and other evolving security scenarios (Afenyo and Caesar, 2023). This absence of sophisticated simulations based on immersive technological solutions, delays the comprehensive qualification and preparation of maritime security personnel, influencing their ability to effectively manage real-time security risks in the continually evolving maritime security challenges, whether within port facilities or aboard ships (Bueger et al., 2020; Erstad et al., 2023).

Efforts led by the International Association of Maritime Universities (IAMU) and World Maritime University (WMU) paved the way for innovative research exploring new computerized simulation techniques to adapt immersive technologies into MET. Collaborative projects between maritime industry stakeholders and educational institutions are actively developing novel MET strategies, particularly focusing on instilling crucial leadership skills through initiatives like the Global Maritime Professional - Body of Knowledge (GMP-BoK) (IAMU, 2019;IAMU, 2022). These initiatives aim to enhance the skill sets and knowledge base of maritime personnel in response to the industry's evolving demands. The adoption and integration of advanced computerized simulation techniques based on immersive technologies are crucial for modernizing educational and training methods, especially in renovating maritime security exercises within the maritime sector. Unfortunately, the prevalent reliance on traditional methods for security simulator exercises during epidemics and environmental disasters has exposed a significant technology integration gap at the local, regional, and international levels. This gap specifically concerns the integration of computerized simulation techniques within maritime institutes to meet the requirements outlined in the ISPS Code. This lack of optimal utilization or interest in immersive technology development is concerning.

Governing International Standards

The International Maritime Organization (IMO) is a specialized United Nations body for the maritime industry, its role involves uniting and fostering a safe and secure environment by facilitating coordination among contracting governments to establish codes and conventions. Since 1978, an essential element of the current security training has been outlined within the Standards of Training, Certification, and

MRT
ISSN 2812-5622
http://dx.doi.org/10.21622/MRT.2024.03.1.747

Watchkeeping for Seafarers (STCW) Convention (Lun et al., 2023). Furthermore, the obligations and recommendations regarding security needs are available in SOLAS conventions, especially Chapter XI-2 and ISPS Code enforcement in 2004, following the September 11th, 2001 aviation incident, the ISPS code was inspired by best practices from the aviation industry.

Maritime Security "Tabletop Exercise" Approach

The ISPS code mandates that security training "exercise" is required for the capacity-building of seafarers and shore security personnel. The implementation of the ISPS code indicates special methods to carry out security exercises, such as full-scale onsite, tabletop simulation or seminar, or combined exercises with different scenarios that should be performed regularly (Arof and Khadzi, 2018; IMO, 2003). Security exercises must be carried out at least once in consecutive Gregorian years, with a maximum of 18-month interval between each session. The ISPS Code underscores the necessity for security-specialized personnel who undergo training to address security breaches across various security levels (IMO, 2003). This security exercise could be conducted jointly for both the ship and the port facility, either separately or simultaneously. Thus, ensuring familiarity with security plans, security procedures, emergency plans, and the best practices for security mitigation approaches. Moreover, this security exercise scenario could be combined with safety scenarios such as firefighting, and more (Vukelic et al., 2023). Scopus database findings reveal limited sources discussing technology integration within ISPS Code security exercises, particularly focused on tabletop simulation methods for maritime security exercises.

The human factor persists as the game changer in every phase of the maritime industry (Ibrahim, 2022). The specialized security personnel should encompass a wide range of knowledge and training as specified in the ISPS Code; the emphasis on traditional tabletop simulations for MET fails to leverage advanced technological methods for the practical readiness (Kim et al., 2023). Despite the extensive training requirements outlined, covering security administration, legislation, emergency preparedness, and more, the Code's reliance on drills and exercises—typically conducted through tabletop simulations—reveal a limited integration of computerized simulation techniques within some maritime institutes. The Code stresses the importance of security exercises, but the lack of utilization of more advanced, immersive simulation techniques could disable the comprehensive preparedness and practical experience necessary to effectively manage and respond to immediate security threats in the maritime sector. Fig. 1 shows the traditional "Tabletop Simulation" layout parties for MET as the minimum requirement of the ISPS code.

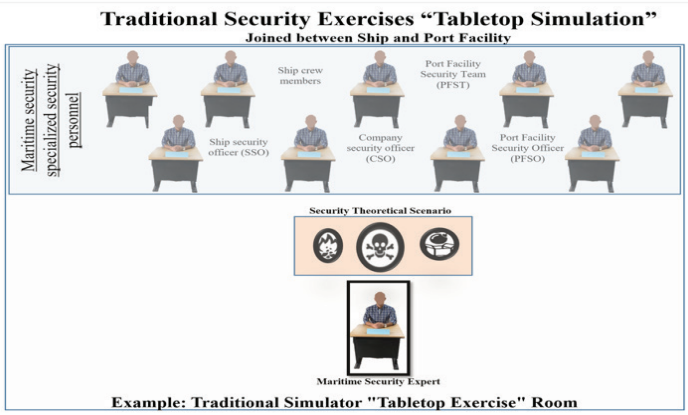

Fig. 1. The traditional security exercise "tabletop simulation".
Source: Author

Unforcefully, when it is utilized as "tabletop simulation", it is still conducted by the majority of MET providers with theoretical demonstration methods without the benefit of computerized simulation techniques. Nevertheless, demonstrations for the roles, responsibilities, and activities during the tabletop simulation scenarios for a security exercise most of the time during pandemics were conducted theoretically with a very rare reliance on the use of technological means to train the joint elements, especially considering that they are in charge of preparing for and fending off security threats. As a result, this would impact the effectiveness and efficacy of MET for the capacity-building of security specialists and would increase the security coordination gaps, for example, while implementing the Declaration Of Security (DOS). Fig. 2 shows the flow of information between the concerned parties when implementing the security levels. The DOS process establishes communication and coordination between a ship and a port facility or a ship and another ship to ensure security measures are aligned and implemented effectively.

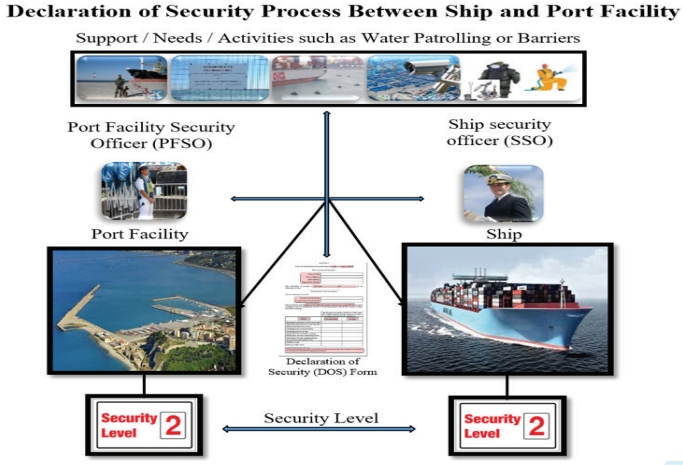

Fig. 2. The completion of the DOS between a ship and a port facility.
Source: Author

COMPUTERIZED SIMULATION TECHNIQUES

Utilizing simulators or engaging in practical training stands as one of the most effective approaches to acquiring experience, competencies, and essential skills within the maritime industry (Hjellvik and Mallam, 2023). Bridge simulators as examples designed realistically represent safety-simulated scenarios covering watchkeeping, collision avoidance, and other safety concerns. These simulators have found extensive use in practical training for seafarers (Wiig et al., 2023). However, these levels of computerized simulation techniques rarely combine or adapt security scenarios. The integration of computerized simulation techniques within security exercises, especially tabletop simulations, as outlined in the ISPS Code, leads to the potential benefits that could revolutionize the efficiency of MET. By utilizing computerized simulations, participants could experience realistic scenarios of security threats, such as cyber threats or piracy, enabling a more immersive and practical learning environment. This technology would bridge the gap between theoretical knowledge and practical application, offering a dynamic platform to test and adapt responses to various security challenges in the maritime sector (Longo et al., 2023). It would also provide hands-on experience to develop and refine security protocols, potentially leading to more competent and well-prepared responses to real-time security incidents within port facilities or onboard ships. Computerized simulation techniques stand as a pivotal asset in augmenting the capacity-building of security personnel across various industries. By replicating realistic scenarios, they offer an environment for personnel to practice responses to complex security challenges, fostering experiential learning that significantly enhances their capabilities. This allows individuals to learn from mistakes in a risk-free setting, promoting a culture of continual improvement and refining their skills without real-world ramifications (Hjellvik and Mallam, 2023; Longo et al., 2023). The customization capacity of these simulations allows industries to tailor scenarios, directly addressing specific security concerns and ensuring that training is precise and relevant to their field (Baldauf et al., 2016).

Incorporating computerized simulation techniques into security exercises, specifically tabletop simulations following ISPS procedures brings several additional benefits. It allows for the exploration of a wide range of dynamic security scenarios, creating a safe environment for testing response strategies to unforeseen maritime security threats and vulnerabilities (Bueger, 2015; Doolani et al., 2020). This approach also enables the monitoring and assessment of the performance of specialized maritime security personnel in computerized high-risk security scenarios, facilitating targeted improvements and ongoing training refinement while receiving feedback (Bueger et al., 2020; Paro et al., 2022). The interactive nature of these computerized simulations utilizing immersive technologies allows for a comprehensive evaluation of the performance of maritime security specialists participating in the security exercise. These tools collect extensive data during exercises, enabling in-depth assessments of each participant's responses and strategies. This data-driven approach, which offers a detailed understanding of individual strengths and weaknesses, could pave the way for tailored training programs that address identified gaps and enhance competencies effectively (Hilfert and König, 2016; Hjellvik and Mallam, 2023; Vukelic et al., 2023; Yin et al., 2021).

Furthermore, it encourages collaboration between the centers of maritime security responsibility, whether onshore or on board the ship, as various stakeholders within the maritime industry can participate in these simulations, fostering a more comprehensive and cohesive response network within a renovated smart maritime industry (Hjellvik and Mallam, 2023). Therefore, these simulations can significantly enhance the adaptability and readiness of the maritime security specialized personnel, thereby better preparing them to handle the complexities of modern security challenges effectively (Barrionuevo et al., 2021; Felsenstein et al., 2013). An additional advantage lies in the adaptability and currency of these simulations. They can be easily updated to reflect emerging security threats and changes in the smart maritime industry.

DISCUSSION

The conventional security "tabletop exercise" approach, while foundational to some extent in some cases as stated also in the ISPS code, exhibits gaps and limitations in the rehabilitation of the security specialized personnel at various levels within the maritime industry (Arof and Khadzi, 2018; Vukelic et al., 2023). For instance, in preparing for the multifaceted risks faced in the maritime industry in dealing with cyber threats, the tabletop exercise might discuss protocols theoretically, but a computerized simulation can immerse participants in realistic cyber breach scenarios. In the case of piracy or armed robbery, a tabletop exercise might simulate the situation verbally, whereas a computerized simulation could mimic real-time scenarios, offering practical insights into response strategies by utilizing immersive technologies as shown in Table I including Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR), Extended Reality (XR), Artificial Intelligence (AI), Metaverse, Haptic Feedback Systems, Wearable Technology, 3D Modeling and Visualization, Gesture Recognition, Biometric Recognition and Hologram

MRT
ISSN 2812-5622
http://dx.doi.org/10.21622/MRT.2024.03.1.747

Lighting (Doolani et al., 2020; Felsenstein et al., 2013; Hajjami and Park, 2023; Kim et al., 2023; Laera et al., 2023; Paro et al., 2022; Vukelic et al., 2023). The tabletop exercise limitations lie in its theoretical and discussion-based nature, whereas computerized simulations bridge these gaps by providing immersive, practical experiences for a more comprehensive understanding and response preparedness to diverse risks.

Computerized simulation techniques utilizing immersive technologies could replicate various maritime scenarios settings, such as different types of ships, port facilities, and complex infrastructures, offering a diverse range of security exercise environments for renovated "tabletop simulation". This exposure prepares security teams for a wide array of potential security challenges (Felsenstein et al., 2013). These technologies enable trainees to learn and practice security protocols in a risk-free environment (Hjellvik and Mallam, 2023; Longo et al., 2023). They can make mistakes, learn from them, and refine their responses without exposing actual maritime security. This helps in preparing security personnel for rare but critical situations (Felsenstein et al., 2013) and immersive technologies contribute to heightened practical training experiences for maritime security specialized personnel. Additionally, computerized simulation techniques facilitate repetitive training sessions, allowing maritime security specialized personnel to practice scenarios multiple times, improving response times, decision-making skills, and overall preparedness without real-world limitations creating more engaging and interactive training sessions, enhancing the learning experience. Table I shows an integration of computerized simulation techniques of immersive technologies possibilities that could revolutionize the maritime security exercise as per the ISPS code requirements in several ways.

Table I: The Benefits of Immersive Simulation Techniques for Security Exercise

Immersive Technology	Benefits for Security Exercise
Virtual Reality (VR)	Offers realistic, immersive simulations of maritime security exercise scenarios. Provides a practical, interactive experience for the security-specialized personnel.
Augmented Reality (AR)	Overlays virtual elements onto real-world environments, enhancing situational awareness and security exercise within authentic settings.
Mixed Reality (MR)	Merges real and virtual environments, allowing security-specialized personnel to interact with and manipulate virtual objects within their physical surroundings during the security exercise.
Extended Reality (XR)	Encompasses VR and AR, creating a more immersive and interactive security exercise experience by blending real and virtual worlds.
Artificial Intelligence (AI)	Enables dynamic and adaptive security simulations that respond to participants' actions during the exercise, providing personalized challenges and learning experiences.
Metaverse	Revolutionizes training through interconnected, persistent digital environments, allowing collaborative and comprehensive security exercises in a highly interactive, expansive digital space.
Haptic Feedback Systems	Provides tactile sensations for a more realistic simulation experience, enhancing muscle memory and physical skill development.
Wearable Technology	Integrates devices like smart glasses or smartwatches to provide real-time information, enhancing situational awareness and decision-making.
3D Modeling and Visualization	Offers detailed 3D models for in-depth exploration of ship and port facility security layout, aiding in comprehensive understanding and planning during security exercises.
Gesture Recognition	Allows participants to interact with simulations through hand and body signals, providing a more natural and intuitive training experience.
Biometric Recognition	Utilizes biometric data for security access training, enhancing understanding and protocols related to identity verification and security procedures.
Hologram Lighting	Augments the security exercise environment by projecting holographic images, enhancing visualization and understanding of complex maritime structures and security layouts.

Source: Author

MRT
ISSN 2812-5622
http://dx.doi.org/10.21622/MRT.2024.03.1.747

Adaptability of Computerized Simulations

Leveraging immersive technologies is exemplified through the integration of AR and gesture recognition systems, incorporating head-mounted devices and sensors worn on the hands of security specialized personnel. These devices, coupled with augmented software, are specifically tailored for constructing security scenarios, such as addressing suspicious objects on ships or within port facilities. The design of these scenarios involves the use of programs that seamlessly integrate them into AR, simulating the actual physical environment for security-specialized personnel. This immersive approach aims to enhance their abilities and skills, enabling them to comprehend and manage potential risks effectively. The milestones of implementing the security exercise simulator, illustrated in Fig. 3 and Table II for the 5C action application, exemplify the practical application of this technology, particularly in scenarios involving the combating of suspicious objects. Moreover, educational institutes with bridge simulators can take the initiative by integrating hologram lighting to display suspicious objects for specialized security personnel. This integration allows for the explanation of scenarios on dealing with such objects, seamlessly merging with safety-specialized simulators and implementing the procedures of the 5C Action application. The transformative influence of computerized simulation techniques on maritime security exercises emphasizes the significant opportunities presented by these immersive technologies.

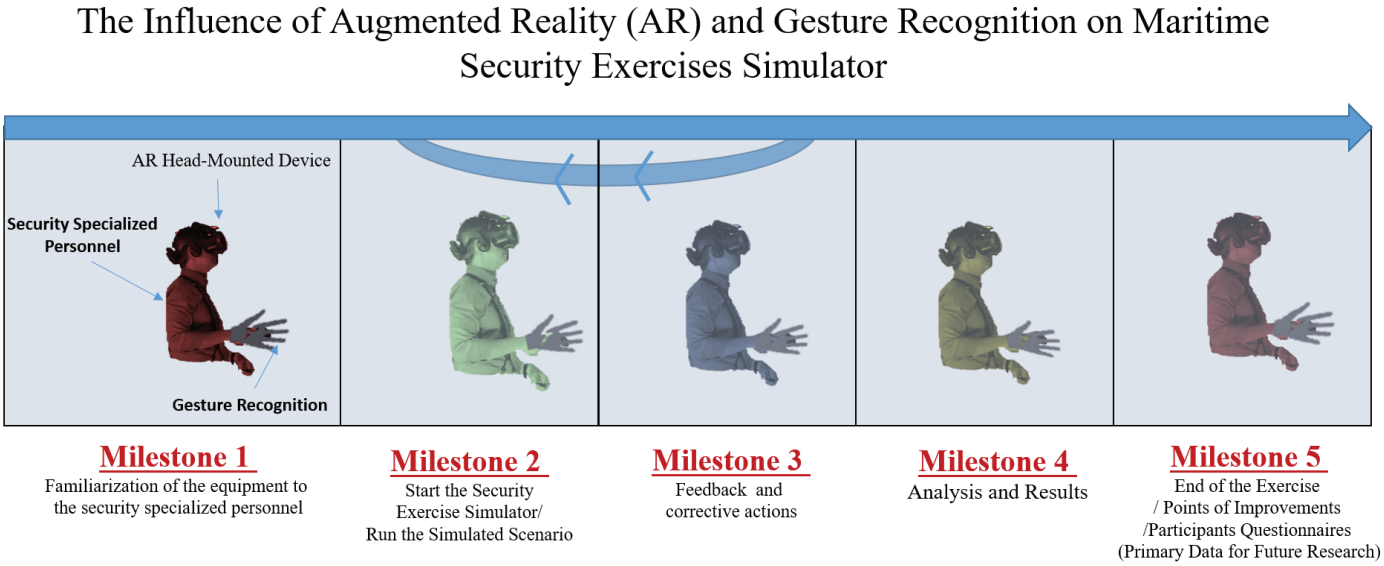

Fig. 3. The milestones of implementing the security exercise simulator
Source: Author

Table II: The 5C Action Application Combating Suspicious Objects

Action	Action Application
Confirm	Confirming the existence and nature of the suspicious object onboard the simulated ship/port facility
Communicate	Effective communication is vital during security incidents. This step involves notifying relevant authorities, such as the ship's security officer, port authorities, or support bodies (e.g. bomb squad).
Clear	Once the suspicious object is confirmed, the area is cleared. Evacuation procedures are implemented based on the simulated scenario for the ship or port facility (master station or shore assembly point).
Cordon	Creating a cordon around a suspicious object typically refers to establishing a secure perimeter or restricted area around the object, especially in scenarios where there is a potential threat or danger. The cordon serves to control access, contain the situation, and prevent unauthorized individuals from entering the area.
Control	This includes collaboration control between designated security personnel, authorities, and any additional resources required for a comprehensive response to deter the risk of the suspicious object.

Source: Author

The advent of computerized simulation techniques by implementing one or a combination of these immersive technologies within computerized simulation tabletop security exercises could significantly enhance the quality, depth, and breadth of security exercises more than the conventional "Tabletop Exercise" approach in the maritime industry, better preparing maritime security specialized personnel to handle a wide range of potential security threats and challenges.

CONCLUSION

Computerized simulation techniques utilizing immersive technologies in maritime security exercises may offer immersive benefits and practical experiences that better prepare maritime security personnel for multifaceted risks, such as cyber threats, piracy, and armed robbery, providing a more comprehensive understanding and response preparedness. These simulations replicate diverse maritime settings, allowing for exposure to various security challenges and the opportunity to practice risk-free, refining responses, decision-making skills, and immediate feedback. Additionally, they offer repetitive training sessions, improving overall preparedness without real-world limitations, resulting in engaging and interactive learning experiences.

The adaptability of computerized simulations ensures that security exercises for the port facility, the ship, or both remain relevant despite external factors like pandemics, while also facilitating remote training and multi-agency participation, fostering knowledge sharing among diverse locations and organizations. These techniques align with joint projects such as the GMP-BoK, fortifying stakeholders and seafarers in cognitive, affective, and psychomotor domains, crucial for their development. Furthermore, the purpose of these simulations, per the ISPS Code, is to ensure security personnel's proficiency in adhering to security incident standards and prompt response, enabling them to recognize and address any security concerns effectively. These technologies standardize training programs, ensuring consistent and comprehensive instruction for security personnel across various maritime facilities. The integration of one of the immersive computerized simulation techniques could significantly improve the preparedness and effectiveness of maritime security-specialized personnel in addressing security challenges within the smart maritime sector.

REFERENCES

Afenyo, M. and Caesar, L.D. (2023) 'Maritime cybersecurity threats: Gaps and directions for future research', *Ocean and Coastal Management*. Available at: https://doi.org/10.1016/j.ocecoaman.2023.106493.

Arof, A.M. and Khadzi, A.F.A. (2018) 'A Delphi study to identify important factors for determining the level of adherence to ISPS Code implementation', *International Journal of Supply Chain Management*, 7(4).

Baldauf, M., Dalaklis, D. and Kataria, A. (2016) 'TEAM TRAINING IN SAFETY AND SECURITY VIA SIMULATION: A PRACTICAL DIMENSION OF MARITIME EDUCATION AND TRAINING', in *INTED2016 Proceedings*. Available at: https://doi.org/10.21125/inted.2016.0983.

Barrionuevo, O., Guarda, T. and Victor, J.A. (2022) 'Impact of the Use of Simulators on Training and Specialization in the Navy', in *Smart Innovation, Systems and Technologies*. Available at: https://doi.org/10.1007/978-981-16-4884-7_14.

Bueger, C. (2015) 'What is maritime security?', *Marine Policy*, 53. Available at: https://doi.org/10.1016/j.marpol.2014.12.005.

Bueger, C., Edmunds, T. and McCabe, R. (2020) 'Into the sea: capacity-building innovations and the maritime security challenge', *Third World Quarterly*, 41(2). Available at: https://doi.org/10.1080/01436597.2019.1660632.

Cicek, K., Akyuz, E. and Celik, M. (2019) 'Future Skills Requirements Analysis in Maritime Industry', in *Procedia Computer Science*. Available at: https://doi.org/10.1016/j.procs.2019.09.051.

Dalaklis, D. (2017) 'Safety and Security in Shipping Operations', in. Available at: https://doi.org/10.1007/978-3-319-62365-8_9.

Dewan, M.H. *et al.* (2023) 'Immersive and Non-Immersive Simulators for the Education and Training in Maritime Domain—A Review', *Journal of Marine Science and Engineering*, 11(1). Available at: https://doi.org/10.3390/jmse11010147.

Doolani, S. *et al.* (2020) 'A Review of Extended Reality

(XR) Technologies for Manufacturing Training', *Technologies*, 8(4). Available at: https://doi.org/10.3390/technologies8040077.

Erstad, E. *et al.* (2023) 'A human-centred design approach for the development and conducting of maritime cyber resilience training', *WMU Journal of Maritime Affairs*, 22(2). Available at: https://doi.org/10.1007/s13437-023-00304-7.

Ben Farah, M.A. *et al.* (2022) 'Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends', *Information (Switzerland)*. Available at: https://doi.org/10.3390/info13010022.

Felsenstein, C., Benedict, K. and Baldauf, M. (2013) 'Maritime Safety and Security Challenges – 3D Simulation Based Training', *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 7(3). Available at: https://doi.org/10.12716/1001.07.03.02.

Hajjami, O. and Park, S. (2023) 'Using the metaverse in training: lessons from real cases', *European Journal of Training and Development* [Preprint]. Available at: https://doi.org/10.1108/EJTD-12-2022-0144.

Hilfert, T. and König, M. (2016) 'Low-cost virtual reality environment for engineering and construction', *Visualization in Engineering*, 4(1). Available at: https://doi.org/10.1186/s40327-015-0031-5.

Hjellvik, S. and Mallam, S. (2023) 'Integrating motivated goal achievement in maritime simulator training', *WMU Journal of Maritime Affairs*, 22(2). Available at: https://doi.org/10.1007/s13437-023-00309-2.

IAMU (2023) *Development of a VR Training Video Database*.

Ibrahim, A.M. (2022) 'The impact of neurotechnology on maritime port security—hypothetical port', *Journal of Transportation Security*. Available at: https://doi.org/10.1007/s12198-022-00253-x.

IMO (2002) 'International Ship and Port Facility Security Code and SOLAS Amendments ', in *nternational Maritime Organization*.

Kim, J. *et al.* (2023) 'Identifying Optimal Approaches for Sustainable Maritime Education and Training: Addressing Technological, Environmental, and Epidemiological Challenges', *Sustainability (Switzerland)*, 15(10). Available at: https://doi.org/10.3390/su15108092.

Kim, T. eun *et al.* (2021) 'The continuum of simulator-based maritime training and education', *WMU Journal of Maritime Affairs*, 20(2). Available at: https://doi.org/10.1007/s13437-021-00242-2.

Laera, F. *et al.* (2023) 'Evaluating an augmented reality interface for sailing navigation: a comparative study with a immersive virtual reality simulator', *Virtual Reality*, 27(2). Available at: https://doi.org/10.1007/s10055-022-00706-7.

Longo, G. *et al.* (2023) 'MaCySTe: A virtual testbed for maritime cybersecurity', *SoftwareX*, 23. Available at: https://doi.org/10.1016/j.softx.2023.101426.

Lun, Y.V., L.K.-H., C.T.E.& Y.D. (2023) 'Shipping Security and Safety', *Shipping and Logistics Management. Springer* [Preprint].

Mallam, S.C., Nazir, S. and Renganayagalu, S.K. (2019) 'Rethinking maritime education, training, and operations in the digital era: Applications for emerging immersive technologies', *Journal of Marine Science and Engineering*. Available at: https://doi.org/10.3390/JMSE7120428.

Pagán, J.I. *et al.* (2016) 'The influence of anthropic actions on the evolution of an urban beach: Case study of Marineta Cassiana beach, Spain', *Science of the Total Environment*, 559. Available at: https://doi.org/10.1016/j.scitotenv.2016.03.134.

Paro, M.R., Hersh, D.S. and Bulsara, K.R. (2022) 'History of Virtual Reality and Augmented Reality in Neurosurgical Training', *World Neurosurgery*. Available at: https://doi.org/10.1016/j.wneu.2022.08.042.

Ringsberg, A.H. and Cole, S. (2020) 'Maritime security guidelines: a study of Swedish ports' perceived barriers to compliance', *Maritime Policy and Management*, 47(3). Available at: https://doi.org/10.1080/03088839.2020.1711977.

Szwed, P. and Benton, G. (2022) 'Helping Accelerate the Global Maritime Professional Body of

MRT
ISSN 2812-5622
http://dx.doi.org/10.21622/MRT.2024.03.1.747

Knowledge up the S-Curve of Innovation', in *Proceedings of the International Association of Maritime Universities Conference*.

Tam, K. and Jones, K.D. (2018) 'Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping', *Journal of Cyber Policy*, 3(2). Available at: https://doi.org/10.1080/23738871.2018.1513053.

Tijan, E. *et al.* (2021) 'Digital transformation in the maritime transport sector', *Technological Forecasting and Social Change*, 170. Available at: https://doi.org/10.1016/j.techfore.2021.120879.

Unclos (2023) *United Nations Convention on the Law of the Sea*, *Official UN site*.

Vukelic, G. *et al.* (2023) 'Application of VR Technology for Maritime Firefighting and Evacuation Training—A Review', *Journal of Marine Science and Engineering*. Available at: https://doi.org/10.3390/jmse11091732.

Wiig, A.C., Sellberg, C. and Solberg, M. (2023) 'Reviewing simulator-based training and assessment in maritime education: a topic modelling approach for tracing conceptual developments', *WMU Journal of Maritime Affairs*, 22(2). Available at: https://doi.org/10.1007/s13437-023-00307-4.

Yin, R. *et al.* (2021) 'Wearable Sensors-Enabled Human–Machine Interaction Systems: From Design to Application', *Advanced Functional Materials*. Available at: https://doi.org/10.1002/adfm.202008936.