Masters Program in Geospatial Technologies

“PORT UNDER ATTACK”

DEVELOPING A SERIOUS GAME TO TEACH CYBERSECURITY CONCEPTS IN GNSS/SATCOM SYSTEMS USING GEOSPATIAL SIMULATION

Amin Ibrahim Fayiz Alameer

Dissertation submitted in partial fulfilment of the requirements
for the Degree of *Master of Science in Geospatial Technologies*

NOVA IMS INFORMATION MANAGEMENT SCHOOL
UNIVERSITAT JAUME·I
Universität Münster

“PORT UNDER ATTACK”:

DEVELOPING A SERIOUS GAME TO TEACH CYBERSECURITY CONCEPTS IN GNSS/SATCOM SYSTEMS USING GEOSPATIAL SIMULATION

Dissertation submitted in partial fulfillment of the requirements for the Degree of
Master of Science in Geospatial Technologies

by
Amin Ibrahim Fayiz Alameer

Supervised by:
Dr. Sven Casteleyn
Institute of New Imaging Technologies
Universitat Jaume I
Castellón, Spain

Co-supervised by:

Dr. Marco Painho
NOVA Information Management School
NOVA University Lisbon
Lisbon, Portugal

Dr. Tomas Bartoschek
Institute for Geoinformatics (ifgi)
University of Münster
Münster, Germany

29th January 2026

STATEMENT OF INTEGRITY

I declare that the work described in this document is my own and not from someone else. All the assistance I have received from other people is duly acknowledged and all the sources (published or not published) are referenced.

This work has not been previously evaluated or submitted to NOVA Information Management School or elsewhere. I further declare that I have fully acknowledged the Rules of Conduct and Code of Honor from the NOVA Information Management School.

Castellon/Spain, 18/02/2026

AMIN IBRAHIM FAYIZ ALAMEER

USE OF GENERATIVE ARTIFICIAL INTELLIGENCE

Tasks	NO	YES	Generative Artificial Intelligence tools
Better understand issues related to the research		yes	Gemini
Summarizing text from bibliography / resources		yes	Gemini
Summarizing the method(s) used		yes	ChatGPT
Translating text		yes	Gemini
Grammar check		yes	Gemini
Paraphrase or rewriting text from other people / resources		yes	ChatGPT
Coding in R, Python, etc.		yes	Gemini
Get help on a software		yes	microsoft Copilot
Creating and editing images, maps, videos, etc.	No		
Data analysis		yes	Gemini
Specify below other tasks not mentioned above:			Internet searching, paper summerizing, grammar checking

ACKNOWLEDGMENTS

First and foremost, I would like to express my deepest gratitude to my parents starting with my beloved mother Samira Shannak for being the motivation of starting this masters program, my father Ibrahim Alameer who stood by my back of just pushing forward with no doubts, my deeper appreciation is for my soul twin brother Saif Alameer, for being my steady anchor throughout this academic journey. Thank you for your patience, for your overseas push, for being there in the easy and hard times, for believing in me, and for making this adventure possible. I would also like to thank my true supporters who we met in the way of studying this masters and escalated to be very close to my heart, by standing by me and whose lifelong support provided the foundation upon which I built my education.

I would also like to thank my supervisors, Sven Casteleyn, Marco Painho and Thomas Bartoschek, for their invaluable guidance. Your knowledge of geospatial and cybersecurity was imperative to this study. I would like to thank you especially for your patience and helpful feedback, which made it possible for a mere idea to turn into a reality. I would also like to thank Sven Casteleyn for our enlightening discussions, which helped to iron out the technical details of my game.

In conclusion, I would also like to express gratitude towards the subjects of my study, the students and professionals who participated in playing the "Port Under Attack" game. Their feedback was useful to this thesis. Finally, I would like to thank my friends and colleagues at Universitat Jaume I (UJI) and the Erasmus Mundus community for the coffee breaks and technical debates. You made this international experience one I will never forget.

ABSTRACT

With growing dependence on GNSS for different fields and logistics in day to day life, this raises specialized cybersecurity awareness. Despite the rise in signal interference and deception, traditional educational methods often fall short in representing complex, real-time vulnerabilities of these types. This thesis introduces "Port Under Attack," an interactive serious game for teaching GNSS cybersecurity concepts through geospatial simulation.

The simulation is a web-based application that was made using Next.js and PixiJS. It puts the user in the role of an analyst. The analyst has a mission to defend a port, the game has a way of teaching that combines theory and practice. It uses scenarios to show what Jamming and Spoofing attacks look like.

The game has two types of modes: Learning Modes and Serious Modes. The Learning Modes are interactive, featuring hints, questions, explanations and yes/no prompts (guided discovery). The Serious Modes are intense and with selection option only to apply the learning objective. The game asks the players to find and label things that do not look right. They have to do this by recognizing patterns that they can see. The simulation is, about defending a military port from Jamming and Spoofing attacks. The efficiency of this method has been tested with a pre-test/post-test experimental design showing that geospatial simulation significantly supports technical cybersecurity education.

Keywords: GNSS, cybersecurity, serious games, jamming, spoofing, geospatial simulation, maritime security.

LIST OF ABBREVIATIONS

AABB : Axis-Aligned Bounding Box
AGC : Automatic Gain Control
AIS : Automatic Identification System
API : Application Programming Interface
CDMA : Code Division Multiple Access
CI/CD : Continuous Integration / Continuous Deployment
C/N_0 : Carrier-to-Noise Density Ratio
DLL : Delay Lock Loop
DOM : Document Object Model
ECDIS : Electronic Chart Display and Information Systems
FPS : Frames Per Second
GDPR : General Data Protection Regulation
GIS : Geographic Information Systems
GNSS : Global Navigation Satellite System
HUD : Heads-Up Display
PNT : Position, Navigation, and Timing
PVT : Position, Velocity, and Time
QA : Quality Assurance
SDLC : Software Development Life Cycle
SNR : Signal-to-Noise Ratio
SUS : System Usability Scale
TTFB : Time to First Byte
VTMS : Vessel Traffic Management Systems

LIST OF FIGURES

LIST OF TABLES

Table of Contents

1. INTRODUCTION

1.1 Motivation

The Global Navigation Satellite System (GNSS) has transformed from being a supporting tool within the field of navigation to the invisible spine within the framework of modern industries including maritime logistics and infrastructure. In the modern port environment, GNSS represents the principal means of obtaining Position, Navigation, and Timing (PNT), coordinating complex processes from automated crane control through to Vessel Traffic Management Systems (VTMS). This widespread dependency has led to a "single point of failure". As illustrated within the context of various reports concerning maritime safety, the industry's dependency on GNSS signals, which are inherently weak and unencrypted, represents a threat to the modern supply chain within the context of a new generation of cyber-physical threats (Medina et al., 2019).

The main importance behind this research work arises out of the alarming increase in "Navigational Warfare" (NAVWAR) in the past two years. The security environment has evolved from a theoretical to a practical threat. According to NATO Shipping Centre reporting and GPSPATRON analysis in 2025, incidents of signal interference has escalated to unprecedented proportions. One of the defining features of this increase came in April 2024, when no less than 117 ships in the Eastern Mediterranean reported being in a land location in relation to the Beirut-Rafic Al Hariri International Airport. The attack type, known as "falsified GNSS signals" or "mass displacement," is a coordinated attack in which the reported positions of multiple ships are manipulated to appear to be kilometers away from their actual location as illustrated in Figure 1 (GPSPATRON, 2025).

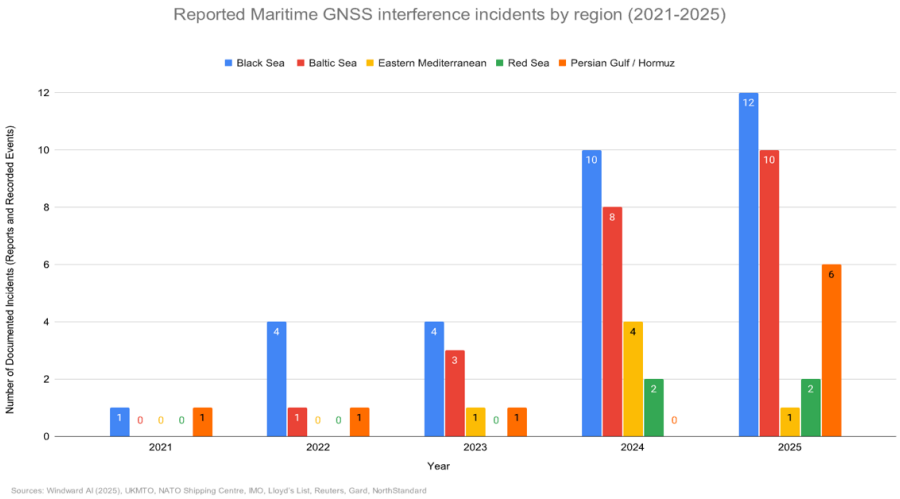

Figure 1: Visual analysis of GNSS interference showing the "circle spoofing" pattern observed near Beirut in April 2024. Adapted from GPSPATRON (2025).

These occurrences are more than mere glitches; they are dangerous threats not only to the safety of the maritime infrastructure, but also to its economic viability. In a busy maritime environment, the effect of the spoofing of one's own position, claiming the ship is 500 meters from its real location, can result in ship collisions, strandings, or the undetected entry of malicious persons inside restricted areas. According to Lloyd's List (2024), while modern ships are equipped with advanced Electronic Chart Display and Information Systems (ECDIS), these systems are only dependent on their sensor inputs. However, recent information provided by Spire Aviation (2025) on the Baltic Sea/Kaliningrad area indicates these threats are no longer fixed, but with the introduction of "mobile jamming", these interfering platforms are now on the move, making it even more difficult to defend against them. Despite the danger posed by these threats, there is a crucial void in the human aspect of cyber-defense. The maritime sector's generic approach to cybersecurity, as described in the Guidelines on Cyber Security Onboard Ships (BIMCO, 2021), is dominated by network security, malware defense, and generic navigation protocols. It provides very little information on the visual identification of electromagnetic signal interference. This is because the spoofing attack is normally confused with equipment failure or sensor malfunction due to the

absence of training on the visual cues of a signal attack (Medina et al., 2019). It is crucial to describe the difference between the two major types of signal interference, Jamming and Spoofing.

According to Morales-Ferre et al. (2020), Jamming is the deliberate transmission of strong electromagnetic interference on GNSS bands (L1/L5), with the aim of disrupting services. This attack that floods the satellite signal, resulting in the instantaneous degradation of the receiver's Signal to Noise Ratio (SNR), ultimately causing the receiver to "lose lock" with the satellites. This translates to an immediate and observable loss of positioning functions in the maritime domain, with the display screens becoming blank or frozen. This type of interference is easily detectable, since the system is either working or not.

Spoofing, on the other hand, is a much more malicious and complex threat. Based on the root definition provided by Psiaki and Humphreys in 2016, spoofing is explained as “Spoofing of Global Navigation Satellite System (GNSS) signals is the broadcast of false signals with the intent that the victim receiver will misinterpret them as authentic signals”. Unlike jamming, which overwrites the signal, spoofing captures the tracking loops of the receiver, allowing the attacker to control the position, velocity, and time solution, PVT, without triggering immediate alerts. From the perspective of a port operator, a spoofing event means that the ship will not vanish from the screen, but rather “drift off course,” or “teleport,” which is a position jump.

This work is further driven by the educational needs of the SpaceSuite Project (spaceSUITE, 2024; European Forum of Technical, Vocational Education, and Training, 2024). With the goal of filling the gap that exists between the complexity of downstream space technologies and educational curricula. It is important to shift from passive learning in educational institutions to active learning. Lecturing can explain the "carry-off attack" in mathematics, but not the pressure of detecting one on a live radar screen, Therefore, this thesis aims to develop a serious game titled “Port Under Attack” specifically targeting geospatial analysts and students to detect such “invisible dangers”. Through the concept of abstract signals made visible in serious game mechanics, this

study hopes to endow future professionals with cognitive patterns to discern differences between natural system errors and malevolent actions to improve the resilience of vital maritime infrastructure.

1.2 Problem Statement

The problem is exacerbated by the absence of proper visualization support in the traditional curriculum. According to Tomaszewski et al. (2020) in their research on disaster resilience, the development of “spatial thinking,” or the ability to visualize and interpret dynamic spatial phenomena, is a cognitively complex process that is not easily accomplished through passive learning alone. Without a serious game that links the behavior of invisible signals to the visible deviations of vessels, learners would not be able to connect their theoretical knowledge to operational decisions. Moreover, the traditional learning approaches in education tend to have the drawback of passive learning. According to Potkonjak et al. (2016), in the area of complex engineering, lectures and static case studies are not adequate because they do not provide students with the opportunity to test system failures in a safe environment. Potkonjak et al. (2016) illustrate the value of such 'Virtual Laboratories' through platforms like ROBOMOSP (see Figure 2), which allow learners to simulate complex robotic failures safely before interacting with physical hardware.

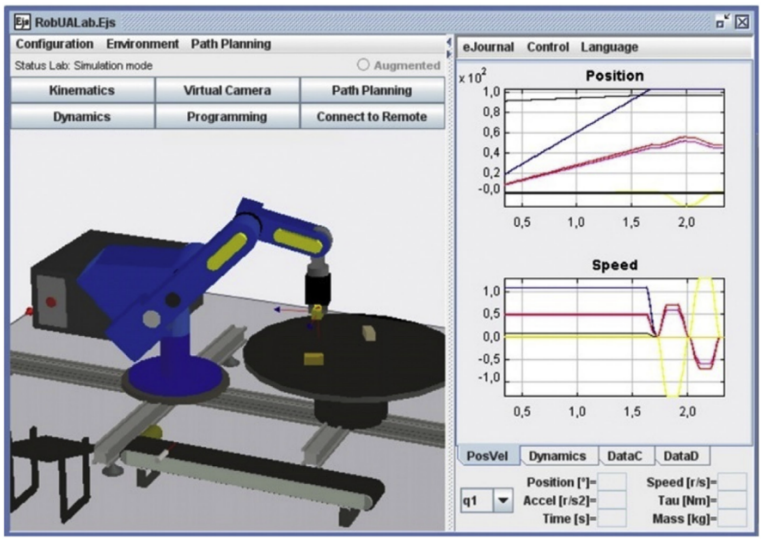

Figure 2: The ROBOMOSP virtual laboratory interface, demonstrating how complex engineering tasks can be simulated safely.

In the specific area of critical infrastructure, it is not possible to have a trial and error process in live systems due to safety reasons. Therefore, there is a lack of "Virtual Laboratories" that provide students with the opportunity to deal with Spoofing/Jamming attacks and see the outcome of their choices without real world consequences.

1.3 Objective and Research Questions

The main focus of this thesis is the design, development, and assessment of a serious game, the "Port Under Attack," to develop abstract GNSS cybersecurity into actionable visual gameplay. The research will also test whether the use of gamified simulation environments enhances the effectiveness of training geospatial analysts to detect and classify signal interference threats, specifically spoofing and jamming.

To achieve this objective, the research focuses on three specific questions:

RQ1: To what extent does the serious game "Port Under Attack" improve participants' ability to identify and classify GNSS jamming and spoofing threats?

RQ2: How participants perceive the usability of the developed serious game interface for educational purposes?

RQ3: How does the gameplay experience influence participants' self-perceived confidence in distinguishing between different GNSS attack types?

1.4 Core Hypothesis

The research work is based on the assumption that active learning through simulation is an effective method for recognizing and retaining dynamic cyber-physical threats.

In particular, one hypothesis is proposed: learners taking the Port Under Attack simulation will experience a positive gain in the accurate identification of the classification of ‘ambiguous’ threats to signal (i.e. Ghost Ships or Drift) beyond their pre-knowledge levels. Indeed, this particular hypothesis is based in direct support of the findings of Sitzmann (2011), as she uncovered in her exhaustive analysis of computer-based games, participants in more active learning conditions increased their factual, as well as skill, knowledge by 11% and 14%, relative to participants in more passive conditions respectively.

Applying these results to the field of GNSS security, it is hypothesized within this thesis that the "Port Under Attack" game will reproduce these benefits. This is because the game is intended to take the invisible, abstract processes involved in signal interference and transform them into something tangible. Therefore, it is hypothesized that the active elements of the game, whereby the player is forced to deal with the results of the

attacks (such as the attack on the port) regarding the initial class of the signal, would form strong cognitive anchors, resulting in players' greater accuracy on the post-test.

1.5 Thesis Structure

The thesis consists of seven chapters that are interdependent and follow the design science research approach. Chapter 1 establishes the research motivation, identifying the main weakness of GNSS technology in maritime ports, along with the current training approach and the pedagogical gap. Chapter 2 provides the theoretical background, defining the physics of jamming and spoofing attacks while reviewing the current state of serious games for cybersecurity education. Chapter 3 presents the methodological approach and conceptual design of the Port Under Attack game, describing the approach of mapping specific academic concepts to visual game mechanics. Chapter 4 details the technical design of the simulation engine, outlining the web architecture and implementation. Chapter 5 outlines the evaluation approach and experimental procedure used to assess participant performance. Chapter 6 analyzes the quantitative and qualitative results of the study, discussing pedagogical effectiveness, system usability, and learner confidence. Finally, Chapter 7 summarizes the research contributions, limitations of the study, and future directions for incorporating real-time AIS data into defensive training simulations.

2. LITERATURE REVIEW

2.1 Fundamentals of GNSS Security : Positioning and Timing in Maritime Logistics

Although "maps" and "navigation" are the conventional and colloquial associations with the Global Navigation Satellite System (GNSS), its contribution to modern civilization far surpasses mere directions. Within the domain of critical infrastructure, the GNSS offers a service akin to a global invisible energy grid, like electricity and water. The foremost role of the GNSS service, although the least appreciated and recognized of GNSS functions, is the provision of Precision timing synchronization. According to the seminal study by Sadlier et al. (2017), the 'invisible utility' of GNSS provides the heartbeat of the global economy by synchronizing high-frequency transactions for the banking industry via atomic clocks. Furthermore, the study highlights that this synchronization is critical for stabilizing the phase cycles of electrical power grids and managing the time-division multiplexing of cellular networks.

This dependency is structurally organized into three distinct segments, as illustrated in the Figure 3.

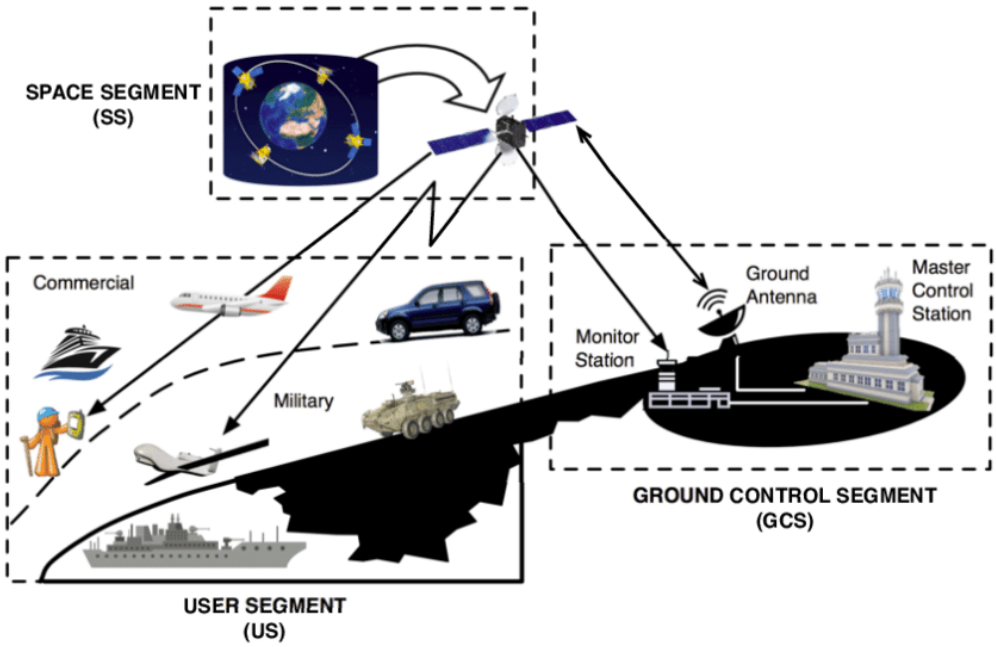

Figure 3: GNSS Segments (Source: Morales-Ferre, 2017).

This “invisible utility” is nowhere as critical and nowhere as vulnerable as in the marine environment. Today, a vessel is a moving critical infrastructure node. For a bank or a cell tower, one may think of having a hardwired “time-keeping” backup solution such as a fiber optic cable, for a ship off at sea, the User Segment is completely dependent on the Space Segment for the synchronization of their Automatic Identification System, stabilization of their Dynamic Positioning systems, as well as stabilization of their Electronic Chart Display and Information System. As underlined by the U.S. Department of Homeland Security (2021), the marine environment's dependency on GNSS is critical, as there is currently no widespread backup solution that offers similar precision.

Nevertheless, such an approach has a very unstable physical foundation. What primarily instigates the vulnerability of GNSS rests on the physics of its signal transmission. For instance, satellites position themselves above the earth at a point that reaches 20,000 kilometers in altitude. Consequently, when the signal reaches the user's receiver position at sea level, its power can be considered incredibly low. Specifically, its power can be comprehended at -160 dBW (decibel-watts). According to Kaplan & Hegarty (2017), such a power can be compared to detecting the light of a 20-watt bulb from a distance of 20,000 kilometers.

This extremely low signal strength, in turn, creates an inherent security loophole because an attacker can easily overpower this authentic signal. The signal generated

by satellites lies below the thermal noise floor and can thus be overwhelmed by a low-power jammer acting as a "shouting" transmitter against a "whispering" satellite, This highlights an uneven security model where a system costing billions can be jammed by a system costing less than a hundred dollars.

2.2 GNSS Attack Vectors: From Denial to Deception

To follow the mechanics of Port Under Attack simulation, it's necessary to strictly stipulate two major types of signal interference: Jamming – Denial of Service, and Spoofing – Deception. Even though these two attack modalities make use of low power levels of GNSS receivers, their modes of operation are quite disparate, with divergent maritime safety impacts.

2.2.1 Jamming: The Physics of Denial

Jamming means the intentional transmission of any electromagnetic signal on the frequency band of the GNSS signal (for example, the band for the L1 signal at 1575.42 MHz), with the intention of causing the receiver to be unable to acquire or make use of genuine navigation signals. The efficacy of jamming can be gauged with the Jamming to Signal (J/S) Ratio.

As established in Section 2.1, the authentic satellite signal arrives at the user's antenna with an extremely low power of approximately -160 dBW. A jammer functions as an artificial noise transmitter. According to Kaplan and Hegarty (2017), if the jamming power exceeds the satellite signal power by a sufficient margin—typically a J/S ratio of 20 to 30 dB, depending on the receiver's quality—it saturates the receiver's Automatic Gain Control (AGC). Consequently, the noise floor rises to a level where the receiver can no longer correlate the satellite's unique Code Division Multiple Access (CDMA) sequence against the background noise.

Translated into the operational maritime context, this means a "Loss of Lock”. The receiver just stops calculating a position. On the bridge of a ship, this might be manifested as a "Blackout" or "Dead Reckoning" alarm, whereby the GPS coordinates disappear altogether. This binary state—both working and broken—is the basis for the "Signal Fade" mechanic in the game, wherein high-intensity interference causes vessels to vanish from the screen.

2.2.2 Spoofing: The Mechanics

In contrast to jamming, where information is subjected to brute force destruction, spoofing involves the intelligent manipulation of information. Psiaki and Humphreys (2016) refer to spoofing as sending counterfeit GPS signals with structures or formats

made to precisely imitate authentic signals, thereby inducing a fake Position, Velocity, and Time (PVT) Solution.

Spoofing attacks can be divided into two main levels of sophistication:

Meaconing (Replay Attack): It is the simplest spoofing attack, wherein the legitimate signals are recorded at one position and retransmitted at another position, which essentially makes the receiver show the position of the attacker and not the receiver itself.

Signal Generation (Sophisticated Spoofing): In this technique, the attacker generates a signal synthetically using mathematical algorithms. In order for the fake signal to work acceptably, the timing and phase must match the authentic signal. The attacker sends the fake signal a little stronger to capture the Delay Lock Loops (DLL) of the target receiver.

Once the tracking loop has been acquired, the attacker can execute a "Carry-Off Attack". As described by Psiaki and Humphreys (2016), the attacker slowly shifts the timing of the fake signal, causing the computed position to drift away from the true location. Because this drift is gradual, it does not trigger the receiver's integrity alarms.

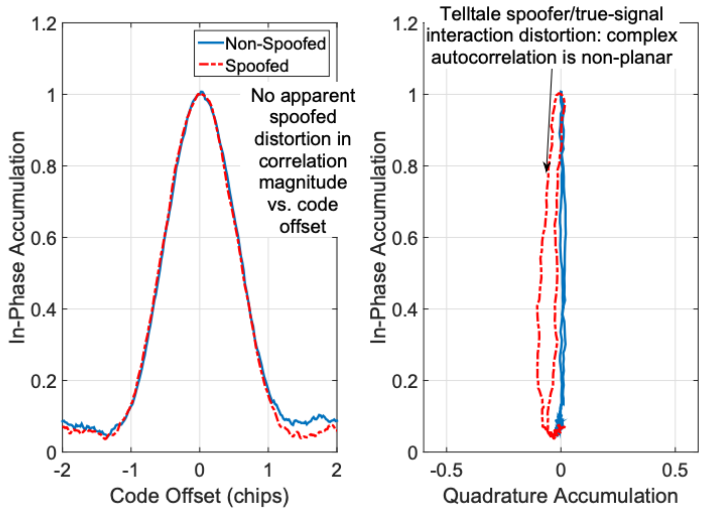

Figure 4: Two 2D views of the unspoofed (blue) and spoofed (red) correlation function, illustrating signal distortion (Source: Psiaki & Humphreys, 2016).

This phenomenon provides the theoretical basis for the "Ghost Ship" mechanic implemented in the game for example. As illustrated in Figure 4, a sophisticated spoofer generates a secondary correlation peak (shown in red) that attempts to overlay the authentic signal peak (shown in blue). During the intermediate phase of an attack, if these signals are not perfectly aligned, the receiver's correlation function becomes

distorted, causing the tracking loops to momentarily lock onto both peaks simultaneously. This results in the system perceiving two potential locations for a single vessel, a "Ghost" effect that visually indicates that the authentic signal is being contested by a malicious counterfeit (Psiaki & Humphreys, 2016).

2.3 Serious Games in Technical Education: Gamification and Active Learning Theory

In order to appropriately place the "Port Under Attack" project within the overall context of educational technology, it is necessary to carefully differentiate between two terms often used interchangeably, namely "Gamification" and "Serious Games". This differentiation is not superficial and actually speaks to differing educational philosophies and their outcomes.

2.3.1 The Limitations of Gamification

according to the fundamental definition provided within the foundational work carried out by Deterding et al. (2011), is the "use of game design elements in non-game contexts". These are generally implemented within the form of adding an additional reward scheme to an existing activity to improve the level of motivation for the user. This style, although effective for certain repetitive and structured tasks, proves to pose a number of limitations within the context of higher-level learning for technical subjects. Gamification maintains an emphasis and focus on the reward scheme rather than the inherent quality of the task being undertaken. For a highly complex subject such as GNSS security, where the intention is to elicit situational awareness rather than the simple regurgitating of memorized facts, the effectiveness of the utility provided by gamification is utilized to a great degree, but the intricate nature and complications are not effectively emulated within the reward schemes implemented.

2.3.2 Serious Games and the "Game Cycle"

Unlike the extrinsic nature of gamification, the nature of the educational game "Port Under Attack" is that it has been developed and tailored under the concept of 'Serious Game.' Garris et al. (2002) have explained the concept of serious game, and according to the authors, it refers to the game that has been developed as full-scale simulation, with the instructional content being intrinsic to the game itself. It has also been explained that the instructional potential and the most important part of the game are not the rewards that are available for the game itself, but the process and the interaction itself have been referred to by the authors as the 'Game Cycle,' which includes 'Input-Process, This process involves engaging the learner in an ongoing cyclic process that mirrors mental processes needed in actual operations.

User Judgment (Input): During this step, the player needs to analyze his or her environment, which requires filtering out noise to find hidden anomalies, such as distinguishing between jamming and spoofing.

Behavior (Process): In this phase, the action that the player undertakes, as a result of their assessment, could be to flag a vessel or to re-calibrate the sensor. This is the application of what was learned.

System Feedback (Outcome): There are quick and obvious effects. When the player does not correctly identify a spoofer, the ship crashes or the mission fails.

This immediate feedback loop is what enables Active Learning. In passive learning engagements (teaching or studying books), a misconception may not be addressed until the final test or assessment. In the game, however, the immediate cycle enables "hypothesis testing," where the student creates a mental model of GNSS interference, tests that against the physical worlds presented within the game, and refines that mental model immediately. This is an important process for ingraining the deep neurological patterns that allow for quick reaction in the field.

2.4 Related Works

Developing serious games that address the topic of cybersecurity has actually become an established field, nonetheless, an examination of recent literature and available tools to aid in security gamification reveals that there exists a major representational drawback when it comes to addressing radio-frequency physical-layer threats. Actual tools being used today are divided into two distinct categories, and neither of them effectively addresses maritime security.

2.4.1 Existent Cyber Security Games

The first category, focusing on the logical layer, is represented by serious games dealing with "general information technology security”. A very well-known case in this category is CyberCIEGE developed by the Naval Postgraduate School. Its structure has been extensively analyzed in the paper presented by Irvine et al. in 2005. CyberCIEGE is a sophisticated simulation tool used for learning information assurance topics including the design of the topology of networks, the management of a firewall system, etc.

Even though CyberCIEGE is very effective for instructing network administrators, the scope of the simulation is strictly the "logical" layer of the OSI protocol reference. It is one thing to deal with digital packets of information traveling across either wired or wireless networks under the jurisdiction of various computer protocols. It is another thing to deal with the "physical" layer of the electromagnetic spectrum. CyberCIEGE cannot hope to emulate the pattern of travel of the radio wave itself, the satellite

constellation, or the presence of the signal-to-noise ratio of the "jammer". Indeed, the student trained on such traditional cyber games would still have no idea how to detect the presence of the GNSS spoofing attack, as it completely evades the firewall by the threat actor's manipulation of the physical sensors of the vessel.

2.4.2 Industrial GNSS Simulators: The Engineering

The second category type is associated with professional industrial simulators, particularly those intended for the aerospace sector or the maritime sector (Spirent, Safran, Rohde & Schwarz, etc.). These are highly accurate simulation tools intended to create RF signals, particularly to test receiver hardware.

However, these tools also pose a large barrier to entry for an educational setting. First and foremost, these tools were not built for educating people but for validating equipment. Hence, when one thinks to use a simulation for educating a student, he/she will need to deal with a multitude of complex parameters and not a visualization tool for the threat. Moreover, these tools do not have the methodology nor the design for a serious game; hence, there is no scenario to meet, nor a 'win' and 'lose' condition to attain. A student will merely observe data and not a visualization of the threat he/she is to combat.

2.4.3 Gamified Competitions: The "Hack-A-Sat" Challenge

A third category, more recently defined, focuses on "Capture the Flag" competitions based on "Gamified Space Assets". So far, the best-known competitions in this category are the "Hack-A-Sat" competitions held by the US Air Force Research Laboratory on an annual basis. For details on the competition framework, the reader is directed to the Cyber Security & Information Systems Information Analysis Center's discussion on "Hack-A-Sat," published in 2023, Hack-A-Sat game, in which security researchers are presented with complex challenges in the areas of satellite command links in orbital mathematics.

While Hack-A-Sat is a massive step in game development, it should be described that this is intended for an utterly different audience from Port Under Attack. Hack-A-Sat targets elite cybersecurity researchers and reverse-engineers; its gameplay involves writing Python scripts, analyzing binary code, and interacting with command-line interfaces. It does not simulate the visual interface of a ship's bridge, nor does it teach the operational "situational awareness" required by a maritime officer. The game teaches how to hack a satellite, not how to navigate through an attack.

2.4.4 Bridging The Gap

This review finds an essential intersection that still remains an uncharted territory in the state of the art. In summary, there is a lack of an easily accessible serious game that is specific to the visualization of GNSS signal attacks, especially for operators.

The need for Port Under Attack was forged in the gap between these two areas and seeks to bridge the gap by utilizing the engaging "Game Cycle," characteristic in most Cyber Security Games (such as Cyber CIEGE itself) and applying it to the physical world with RF interference common in Industrial Simulations. This then enables the democratization of training materials for those in the world of GNSS Cyber Security who are not engineers.

3. METHODOLOGY

To facilitate a systematic and scientifically valid approach, this thesis adopts the Design Science Research Methodology (DSRM) framework (Peffers et al., 2007). This methodology is particularly suited for the design and validation of innovative IT artifacts, such as the "Port Under Attack" serious game in this thesis. The research methodology is divided into five consecutive phases, which correspond directly to the chapters of this dissertation.

As shown in Figure 5, the research methodology encompasses the identification of GNSS vulnerabilities in maritime logistics and the current pedagogical gaps (Phase 1). This theoretical basis forms the basis for the conceptual design of the serious game, where abstract physics are modeled into visual mechanics (Phase 2). The conceptual design is then implemented through an iterative and agile technical implementation phase (Phase 3). To validate the artifact, an empirical study with a one-group pretest-posttest design is performed (Phase 4), which concludes with the synthesis of quantitative and qualitative findings to answer the fundamental research questions (Phase 5).

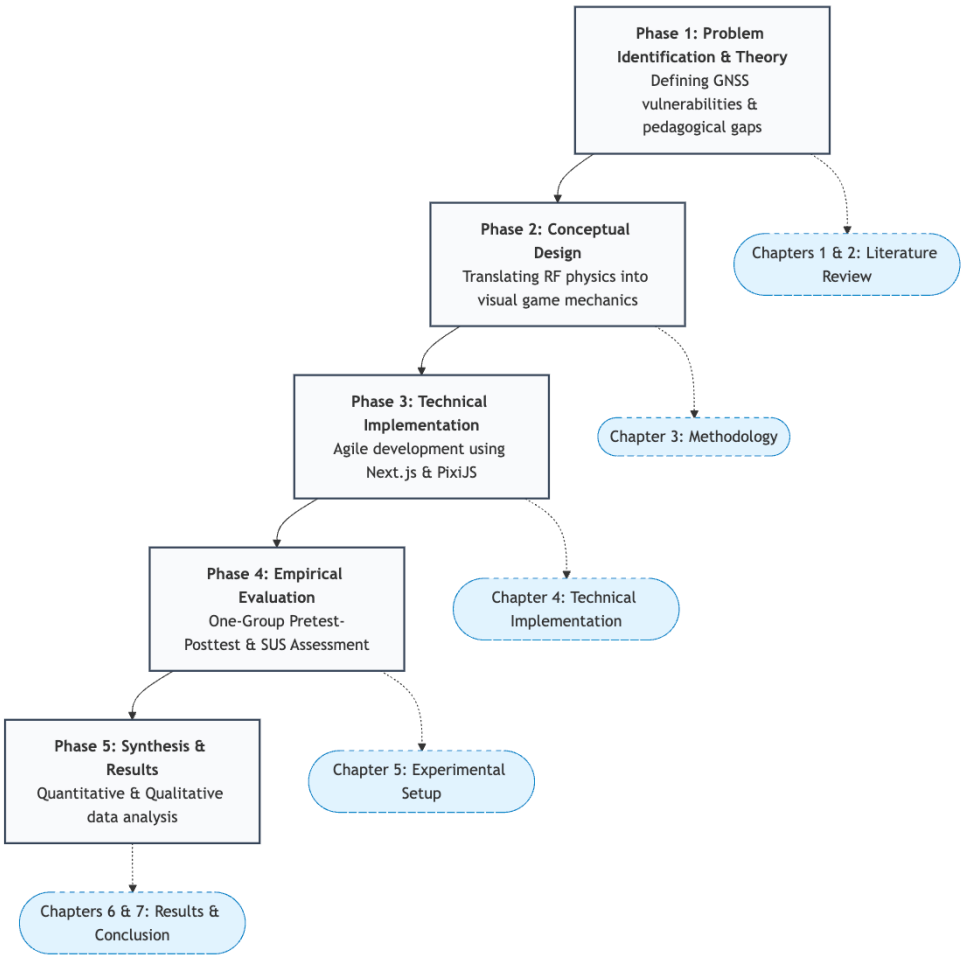

Figure 5: Overall research methodology workflow mapping the Design Science approach to the thesis structure.

3.1 Game Concept and Narrative Context

The Port Under Attack simulation is underpinned by a conceptual framework drawing on a “high-stakes” discourse for military defense situations aiming to influence a change in the player's states of mind from passive observation to active alert. Additionally, the player takes on the persona of a Signal Security Analyst—Callsign: ATLAS—within the context of a commanding facility for a strategically important international logistics center: “IRON TOWER”.

This particular narrative construct follows the guidelines provided by the "Commander Role-Play" approach as presented by Samovi's study in 2018, where the application of such an instructional construct proves to be beneficial for improved decision-making efficacy and situational awareness. With this particular scenario, the educational objective of identifying GNSS signal variations is reframed for purposes of national security considerations, gameplay view can be seen in Figure 6.

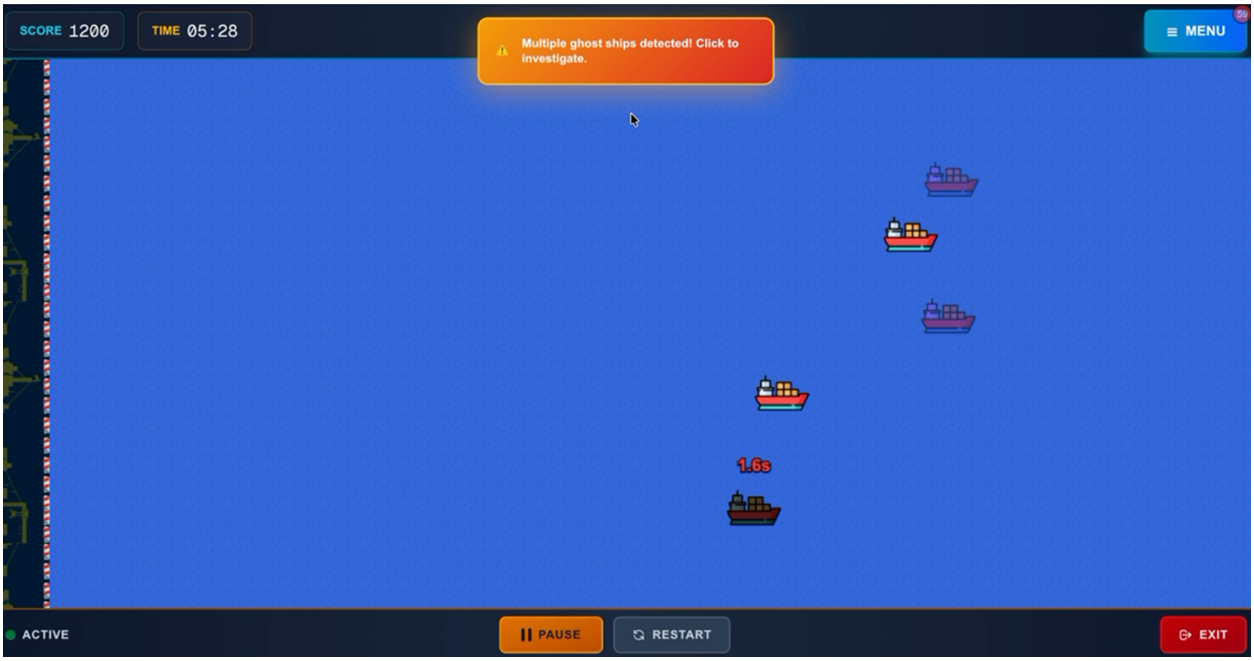

Figure 6: port under attack game play in mixed threats combined.

3.1.1 The Narrative Premise: The Hostile Threat

The environment of the simulation is set in a thickly fogged harbor where visual navigation is not possible; hence, the GNSS sensors are the primary means of navigation. The main conflict of the game takes the form of an undetectable enemy vessels attempting to breach the harbor's defenses with the aid of complex electronic warfare technology.

Unlike in regular maritime traffic, where intentions are simply revealed, the hostile ships will employ spoofing and jamming techniques that will obscure their true intent from detection. The setting of the story establishes that standard detection equipment will be compromised owing to interference. Therefore, the security of the port will lie solely with the Analyst's capacity to visually grasp the raw signal output from incoming ships. Here, a "Zero-Defect" scenario emerges, in that should the Analyst incorrectly classify a ship as non-hostile, the ship will enter the port, explode, leading to a failed mission.

3.1.2 The "Army Style" Command Hierarchy

In order to immerse the gamer in that military environment, there is a strict command and control system of dialogue. The gamer is not simply left on his own and is directly given instructions from Central Command (Callsign: IRON TOWER). The command and control is established from the off in the pre-briefing, where there is a use of a tactical radio interface.

The dialogue structure explicitly differentiates between "BASIC" vessels (neutral traffic) and "ISSUE" vessels (hostile threats), as illustrated in the following transcript from the game's opening sequence (see Figure 7):

IRON TOWER (COMMAND): *"ATLAS, this is IRON TOWER. Enemy ships are moving toward our port... Radar is unreliable. The enemy is using GPS spoofing and jamming to hide their real position".*

ATLAS (ANALYST): *"Understood. That means some ships may show false or unstable positions".*

IRON TOWER (COMMAND): *"Correct... Watch how each ship behaves. Identify whether it is affected by spoofing or jamming. Once you classify the ship correctly, our defense system locks on. A missile is launched and the enemy ship is destroyed".*

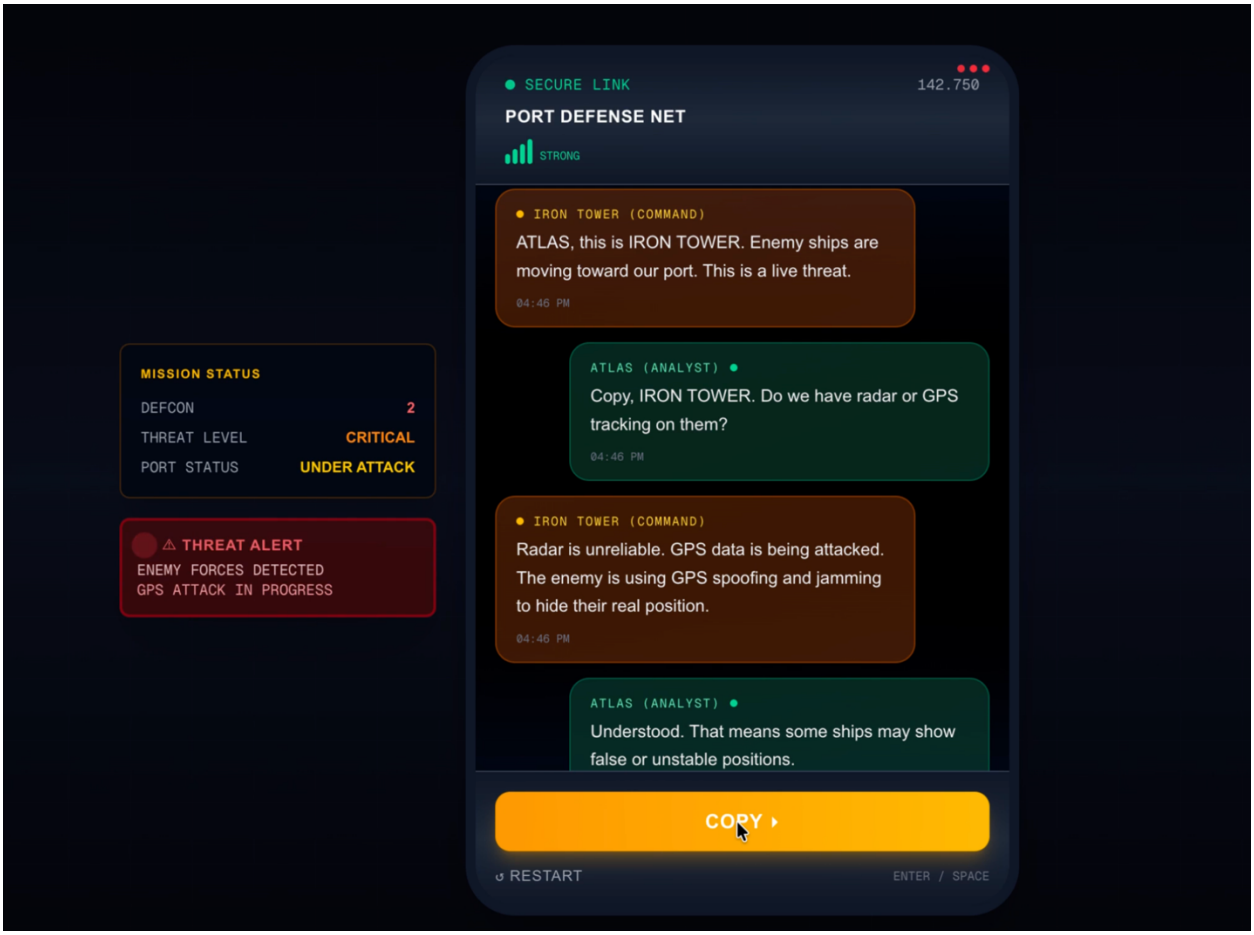

Figure 7: The 'Army Style' command hierarchy. The dialogue interface immerses the player in the role of an analyst (ATLAS) receiving orders from command (IRON TOWER).

This conversation achieves two useful purposes for pedagogical reasons. It confirms the "Active Defense" mechanism by identifying that the Analyst's intelligence report

serves as the trigger for the Army's counterattack measure (the rocket attack). It also meets the sense of pressure and answerability by meeting the NATO guidelines for effective adaptability training, as set out by NATO (2016).

3.1.3 The Operational Loop: Analysis as a Weapon

In this narrative framework, the "Game Cycle" described in Section 2.3 is operationalized as a combat loop. The player is not merely labeling data; they are authorizing defensive strikes.

1. **Surveillance:** The enemy sends waves of mixed traffic (both legitimate and hostile).
2. **Intelligence Analysis:** The player (ATLAS) scans for visual anomalies—such as a ship "blinking" (Signal Fade) or "teleporting" (Position Jump).
3. **Authorization:** The player classifies the specific attack type via the command console.
4. **Engagement:** Upon correct classification, the Iron Tower batteries fire a precision rocket, neutralizing the threat before it breaches the perimeter.

This "Analysis as a Weapon" approach ensures that every theoretical concept (e.g., Signal-to-Noise Ratio) has a direct, visible impact on the game world, reinforcing the link between abstract physics and operational reality.

3.2 Game Structure and User Journey

Before engaging with the fundamental defense mechanisms, the player goes through a controlled "Pre-Mission" process, intended to set up the in-game contextual immersion and technical requirements. The "Pre-Mission" process comprises the "Loading Screen," "Main Menu," and "Tutorial"; these elements are intended to facilitate the transition in the user's state, bringing him/her to "Active Alertness," away from normal web-surfing consciousness and into a functional state for the simulation.

3.2.1 Loading and Atmospheric Establishment

When the player opens the interface, they encounter a visual discourse which denotes a military-grade interface as opposed to a recreational interface. On the Loading Screen, the color range is dark, ranging from Slate-950 through Black, along with the use of animation, which includes a radar spinner. The phrase 'Loading Mission. Preparing navigation systems' denotes a user request as if booting a console instead of opening a webpage.

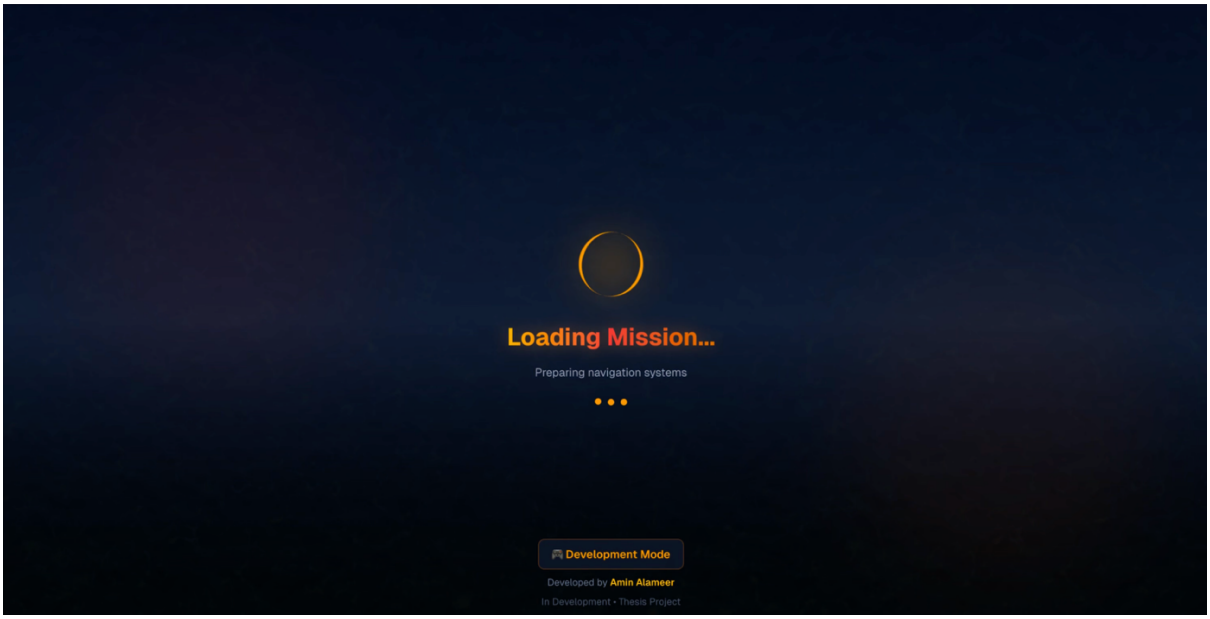

Figure 8: The Loading Interface designed to establish the 'Magic Circle'.

This design choice (see Figure 8) constructs a “Magic Circle” Salen and Zimmerman (2004), an idea in game studies that the player leaves reality and enters a reality of one's own that is subject to game rules. By simulating a boot sequence for a defense terminal's computer, it conditions the user to accept the stakes of the “Zero Defect” mission before any graphical element renders.

3.2.2 Identity Creation: The Callsign System

The **Main Menu** enforces a mandatory "Identity Creation" step. The player cannot proceed without entering a "Callsign" (Username), which simulates the login protocol of a secure terminal.

This mechanic serves two purposes:

1. **Immersion:** It reinforces the military role-play (e.g., "ATLAS-01") rather than anonymous browsing, forcing the player to assume the persona of an active operator.
2. **Pedagogical Persistence:** The username is keyed to the browser's local storage (pua_scores), allowing the system to track performance metrics and "Global Best" scores across sessions. This persistence introduces a competitive element that motivates repeated attempts to master the content.

3.2.3 Tutorial and Mission Briefing

The Tutorial Page acts as the "Rules of Engagement" briefing, as illustrated in Figure 9. Instead of a generic "Help" file, it presents a tactical "Mission Brief Card" that visually distinguishes the two primary states of the simulation:

Friendly Port (The Base): Depicted with an Emerald glow, representing safety and order.
Enemy Threat (The Target): Depicted with a Red glow, representing chaos danger.

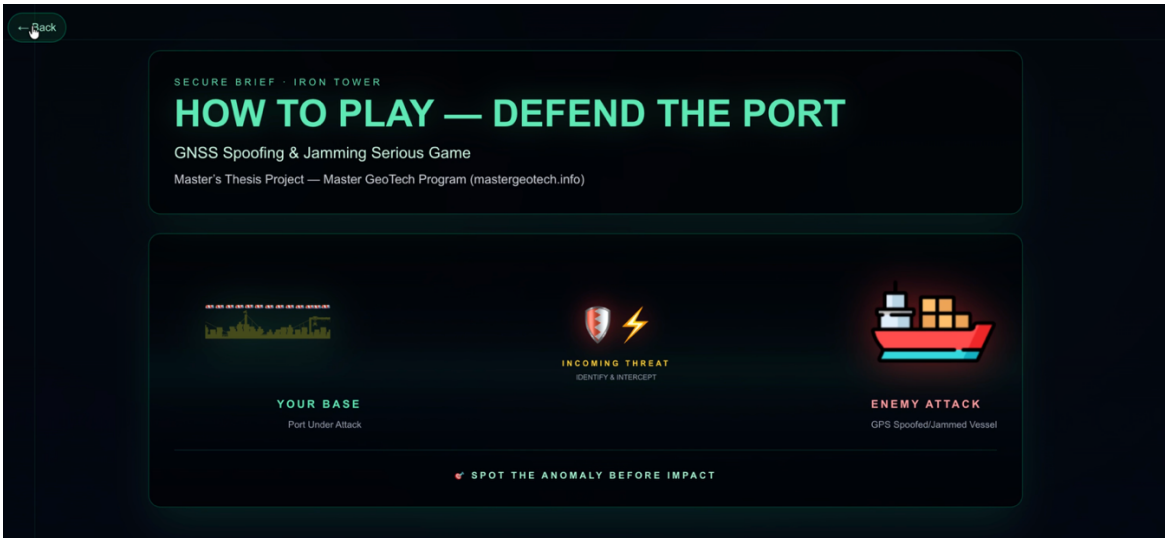

Figure 9: The Mission Briefing interface providing cognitive scaffolding by visually distinguishing friendly (Green) and hostile (Red) signatures.

This visual dichotomy simplifies the complex physics of GNSS interference into a binary logic for the player: *Green is Safe, Red is Suspect*. The briefing also introduces the **"**Five-Step Core Flow**"** (Track → Observe → Analyze → Classify → Engage), providing the cognitive scaffolding necessary for the player to understand their tasks before the time pressure of the live game begins.

3.3 Core Gameplay Mechanics and Modes

The "Active Learning" cycle developed by Garris et al. (2002) paper can be best implemented in the context of the simulation game "Port Under Attack," whereby a very active learning cycle forces the gamer to constantly make a transition from observation to analysis to action through a very rigorous cycle that does not allow the gamer 'guess,' or 'click,' randomly in the game but forces a very active cycle of analysis before authorizing the response to defend the Port from attack, the complete sequence of game phases, from the beginning of target tracking to final threat engagement and mode switching, is visually mapped out in Figure 10.

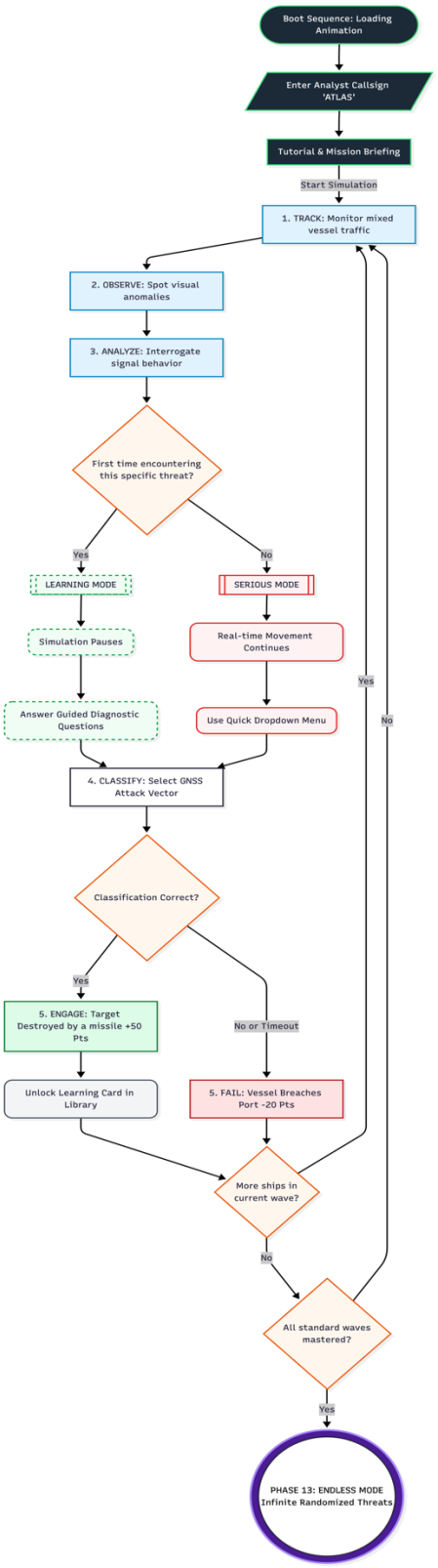

Figure 10: Flowchart illustrating the user journey, the five-step Active Defense Loop, and the dynamic branching between Learning Mode (scaffolding) and Serious Mode (application).

3.3.1 The "Active Defense" Loop

The core interaction of the game is defined by a five-stage "Active Defense" loop. This loop simulates the cognitive workflow of a real-world intelligence analyst:

1. **Track:** The player monitors the movement of multiple vessels entering the harbor. Friendly ("BASIC") ships move smoothly, while hostile ("ISSUE") ships exhibit specific behavioral anomalies.
2. **Observe:** Upon spotting a potential threat, the player must visually isolate the specific anomaly (e.g., a sudden position jump vs. a gradual drift).
3. **Analyze:** The player interrogates the signal behavior. In the early stages, the system provides guided "Yes/No" cues to assist this analysis (e.g., *"Does the ship reappear after disappearing?"*).
4. **Classify:** The player accesses the Command Console to formally classify the threat from a standardized library of GNSS attack vectors (e.g., "Spoofing: Position Jump" or "Jamming: Signal Fade").
5. **Engage (Feedback):** If the classification is correct (+50 Points), the game provides immediate positive feedback: a defensive missile is launched, neutralizing the vessel before it breaches the port. If incorrect (-20 Points), the system logs the failure, allowing the hostile vessel to continue its approach.

3.3.2 Dual-Mode Pedagogy: From Scaffolding to Mastery

To ensure the novice is not burdened by the complexity of signal physics, the game provides a "Dual-Mode" structure in which guidance is progressively removed as the novice demonstrates their competence.

1. Learning Mode (Scaffolding Phase) When a player encounters a specific threat type for the first time (e.g., the first time a "Ghost Ship" appears), the game automatically show instructions and enters Learning Mode, see Figure 11.

- **Mechanism:** An interactive modal window appears, interrupting the time pressure.
- **Interaction:** The player is forced to answer diagnostic questions (e.g., *"Do you see multiple ship positions for one vessel?"*) before they can select a classification.
- **Goal:** This enforces "Scaffolding," ensuring the player understands *why* a visual pattern corresponds to a specific attack type before they are tested on it.

Figure 11: The 'Learning Mode' interface. The simulation pauses and uses diagnostic questioning (Scaffolding) to guide the learner's hypothesis testing before allowing classification.

2. Serious Mode (Application Phase) Once a threat type has been successfully identified in Learning Mode, the game shifts that specific threat into Serious Mode for all future encounters, see Figure 12.

- **Mechanism:** The game no longer assisting by hints.
- **Interaction:** Clicking a suspect vessel opens a "Quick Dropdown" menu. The player must classify the threat in real-time while the ship continues to move toward the port.
- **Goal:** This simulates "Fading" (the removal of instructional support), forcing the player to rely on internalized knowledge and rapid pattern recognition under stress.

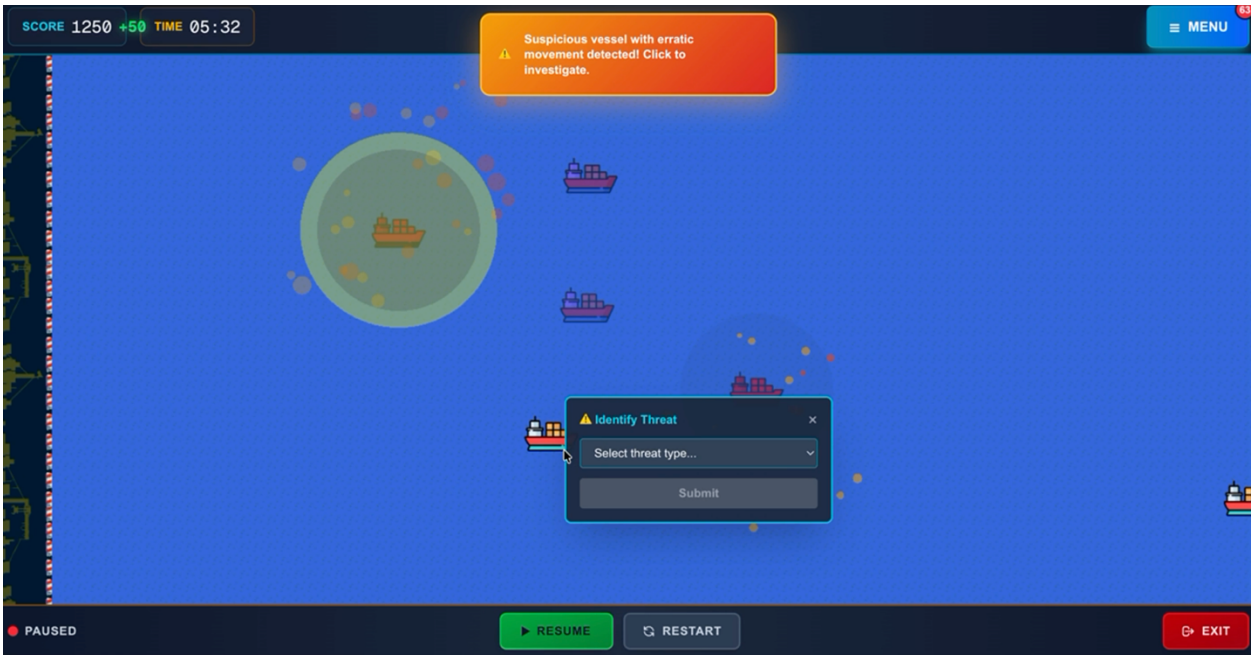

Figure 12: The 'Serious Mode' interface showing the Quick Classification Dropdown. The user must classify the threat in real-time while the vessel continues its trajectory.

3.3.3 Mastery Verification: Endless Mode

This last phase is called "Endless Mode" or "Phase 13". This mode is triggered once all the attacks have been mastered. This mode presents the player with "an endless supply of random attacking vector types (.Basic, Fade, Jump, Ghost, Slow, Blackout, SNR)," with all of these attacking vectors scaling in rates. This is called "Mastery Verification"; it measures if the player has the capacity to think clearly over a long period of time, a possibility not usually available in real life.

In the Endless Mode (Phase 13), which activates only after the player has encountered all threat types.

- **Mechanism:** The system generates infinite waves of vessels with randomized attack vectors (Basic, Fade, Jump, Ghost, Slow, Blackout, SNR) at increasing speeds.
- **Goal:** This serves as the "Mastery Verification". By removing the safe, segmented structure of the earlier phases, Endless Mode tests the player's ability to maintain situational awareness and accuracy over a sustained period, mirroring the fatigue and unpredictability of prolonged real-world operations.

3.4 Scenario Design: Translating GNSS Threats to Game Logic

The game design innovation that underlies this specific pedagogical tool is that of a direct correspondence of invisible aspects of signal processing to more tangible gameplay elements, and Port Under Attack achieves this through a simulated Threat Library that consists of six unique "Scenario Ships" that each attempt to portray a specific form of GNSS interference.

3.4.1 The Visual Interface: Spatializing the Threat

The primary interface, named the "Game Engine," is also organized in a manner that affords a sense of directional urgency at a visual level. The interface is divided into two distinct areas of the screen, for in this game, the Maritime Domain will occupy 95% of the right side of the screen, while the Defensive Port will occupy the crucial remaining 5% of the screen. Enemy ships will begin from a position at the 95% mark of the right side of the screen, crossing from the sea into the port, located at the 5% mark of the left side of the screen. The player must analyze and classify the threat in the "sea" zone before it crosses the threshold of the "port" zone, where a collision triggers a mission failure.

3.4.2 Incremental Progression: The Wave System

The game utilizes an incremental "Wave System" to introduce GNSS threats progressively. The game is divided into 13 distinct phases, where each phase introduces a specific scenario (e.g., Phase 2 introduces "Signal Fading" exclusively) before mixing it with previously learned threats, while another waves include mixed learned threats. When a new enemy ship appears in a wave, the player initiates the learning process by tapping on the ship. This interaction pauses the combat simulation and triggers a diagnostic sequence, allowing the user to deconstruct the visual anomaly (e.g., "Why is this ship blinking?") and classify it by guided questions without the pressure of an immediate crash. This ensures that the player builds a mental model of each specific attack vector in isolation before being tested on them in complex, multi-threat scenarios.

3.4.3 The "Signal Fade" Scenario (Jamming)

- **Visual Mechanic:** The vessel intermittently disappears and reappears on the tracking screen, creating a "blinking" effect.
- **Academic Justification:** This mechanic simulates Low-Power Jamming. According to Kaplan and Hegarty (2017), when a jamming signal pushes the Signal-to-Noise Ratio (SNR) slightly below the receiver's tracking threshold, the receiver loses its "lock" on the satellite code. However, if the interference is fluctuating or borderline, the receiver may repeatedly lose and re-acquire the signal.

- **Game Implementation:** The ship's opacity (alpha channel) oscillates between 0% and 100%, forcing the player to recognize that the target is not gone, but merely "masked" by noise.

3.4.4 The "Position Jump" Scenario (Spoofing)

- **Visual Mechanic:** The vessel moves normally, then instantly "teleports" to a new coordinate (±50 pixels) before continuing.
- **Academic Justification:** This represents a Position, Velocity, and Time (PVT) Discontinuity. As defined by Psiaki and Humphreys (2016), an unsophisticated spoofing attack that does not perfectly align its code phase with the authentic signal will cause the receiver's computed position to "jump" instantaneously to the false location dictated by the spoofer.
- **Game Implementation:** The code applies a random X/Y displacement every 120 frames. This "impossible movement" defies the physics of maritime inertia, serving as the primary visual cue for a spoofing attack.

3.4.5 The "Slow Drift" Scenario (Carry-Off Spoofing)

- **Visual Mechanic:** The vessel exhibits erratic speed changes, alternating between a slow "crawl" and sudden "catch-up" bursts, eventually drifting off the designated shipping lane.
- **Academic Justification:** This simulates a Carry-Off Attack. Psiaki and Humphreys (2016), a sophisticated spoofer first aligns with the authentic signal and then introduces a gradually increasing delay. This introduces a growing error in the pseudo-range measurements, causing the computed position to slowly "drift" away from reality without triggering immediate integrity alarms.
- **Game Implementation:** Unlike the "Jump" ship, the "Slow" ship never teleports. Instead, its velocity vector is manipulated, requiring the player to observe the rate of change rather than just the position.

3.4.6 The "Ghost Ship" Scenario (Multi-Source Spoofing)

- **Visual Mechanic:** The authentic vessel is flanked by semi-transparent "Phantom" copies that mimic its movement but with slight spatial offsets.
- **Academic Justification:** This visualizes Multi-Peak Correlation Distortion. As shown in the Psiaki and Humphreys (2016) analysis, a spoofer can create a secondary correlation peak. While a standard receiver tries to lock onto the strongest peak, the presence of two competing signals creates ambiguity in the tracking loops.

- **Game Implementation:** The game renders "Ghost" sprites with a purple tint and 50% opacity. This serves as a visual metaphor for the internal signal ambiguity, teaching the player that multiple signal returns for a single object are a definitive signature of electronic deception.

3.4.7 The "Blackout" Scenario (High-Power Jamming)

- **Visual Mechanic:** The ship freezes completely in place, turns gray, and a red countdown timer appears above it. If the timer reaches zero, the ship is considered "lost".
- **Academic Justification:** This represents Broadband Saturation. When the Jamming-to-Signal (J/S) ratio exceeds the dynamic range of the receiver's Automatic Gain Control (AGC), the receiver enters a total "Denial of Service" state. It cannot track any satellites, effectively blinding the navigation system.
- **Game Implementation:** The "Freeze" mechanic represents the loss of a PVT solution. The "Countdown" introduces the element of time-criticality—in a real scenario, a ship without navigation in a fog-bound port is an immediate collision risk.

3.4.8 The "SNR Degradation" Scenario (Signal Quality, Jamming)

- **Visual Mechanic:** The vessel is surrounded by a pulsing red aura, and a "Signal Bar" above the ship fluctuates from Green to Red.
- **Academic Justification:** This simulates Carrier-to-Noise Density (C/N_0) Degradation. As detailed by Kaplan and Hegarty (2017) in their analysis of interference effects, the C/N_0 value is the primary metric for signal quality. Before a receiver completely loses its lock (which would cause a "Fade" or "Blackout"), the presence of interference (noise) raises the noise floor, causing the observable C/N_0 value to drop. An alert analyst can use this metric to detect an attack before the navigation solution is lost.
- **Game Implementation:** This is the most advanced scenario. The ship moves normally, forcing the player to look at the *metadata* (the signal bar) rather than the *movement*, training the highest level of "Active Alertness".

3.5 Scoring, Feedback, and Performance Metrics

A well-designed serious game does not only depend upon the precision attained within its simulation; there are indeed aspects concerning its "feeling of feedback". For example, within "Port Under Attack," a complex system of time management, alert systems, and score-tracking has been developed with the intention of offering a constant stream of informative data back toward the user, with the aim of having them maintain a "Active Alertness" without experiencing any form of cognitive overload.

3.5.1 Temporal Pacing and Alert Systems

In order to enable proper orientation in the game scenario in particular, there is a specific temporal arrangement in the simulation process of that game world itself. Once inside the "Game Engine" graphical interface, there is a buffer of ten seconds before the onset of the first 'hostile' craft in that world to allow for what has been termed an "Orientation Phase". This has to be seen as a central aspect of pedagogical game design in reducing irrelevant cognitive load in order to keep the "working memory" of a learner free for threat recognition in particular.

However, as soon as the active phase starts, a "Toast Notification System" becomes visible. Before a wave of new ships appears on the display, a noticeable graphical alert usually in the form of a "Red Emergency Warning" together with a textual message specifying what kind of threat a player faces (e.g., "Incoming Wave: Signal Fade Detected") appears on display. They are designed to clearly signal to a user what so-called "Just-In-Time" cues actually are – a way to direct a user's attention to certain specific graphical anomalies. They clearly demarcate episodes of a game by signaling a specific wave of events.

3.5.2 The Scoring Economy and Immediate Feedback

It first operationalizes the main feedback loop of decision-making through a binary point system with immediate consequences for the actions of the Analyst. Correct classification of hostile vessel grants the player an award of +50 Points, while incorrect classification or failure to intercept results in a penalty of -20 Points.

This scoring economy is not only a gamification element but also a direct application of the reinforcement strategies advocated by behaviorist learning theory. As Garris et al. (2002) immediate feedback is critical for making the "Game Cycle" work as a learning mechanism. That +50 score is a confirmation signal that verifies your mental model of the threat-"This blinking ship is a Jammer"-matches the system's logic. By the same token, that immediate penalty is compelling you to revise that model. This rapid "Trial-Error-Correction" loops accelerate the learning of pattern recognition skills much faster than any delayed feedback methodology, such as a summary at the end of the game.

3.5.3 Knowledge Retention: The Learning Card System

To aid in the retention process and reduce the space between gaming experience and theory application, the simulation presents the player with the ability to gain access to the unlockable "Learning Card" library. Once the player discovers the new type of threat for the first time (e.g., the introduction in the "Ghost Ship" mission), the game will unlock the relevant encyclopedia entry in the game itself, see Figure 13.

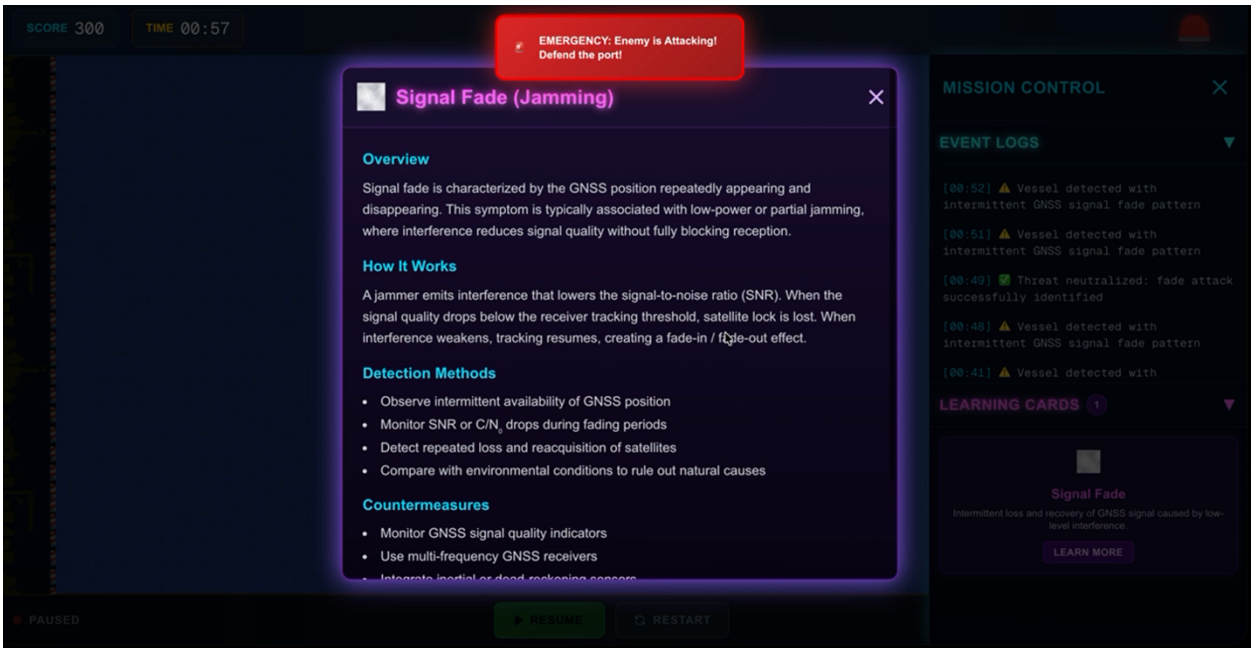

Figure 13: The 'Learning Card' library. Unlocked content provides detailed academic definitions, bridging the gap between game mechanics and GNSS theory.

Each Learning Card has the technical definition of the attack, the explanation given from an academic standpoint (using examples like Multi-Peak Correlation Distortion), and the actual visual manifestation or symptoms that were shown within the game. Thus, the fleeting nature of a game is changed forever. By having the player earn these cards through successful gameplay, there is a value given to knowledge. There is a reward for the successful utilization of the knowledge.

4. TECHNICAL IMPLEMENTATION

4.1 Web Architecture and Agile Development Framework

The technical underpinning for Port Under Attack was designed from its inception to be accessible, performant, and modularly scalable. In contrast to other serious games traditionally developed and deployed on a desktop platform-one that requires significant local installation and hence hardware dependency-this game took a web-first approach. This decision was decidedly appropriate due to the pedagogical requirement to ensure

students universally could access the tool on numerous devices with no technical friction. By embracing modern web standards, this simulation executes natively within the browser, eliminating the onboarding friction and enabling immediate educational deployment.

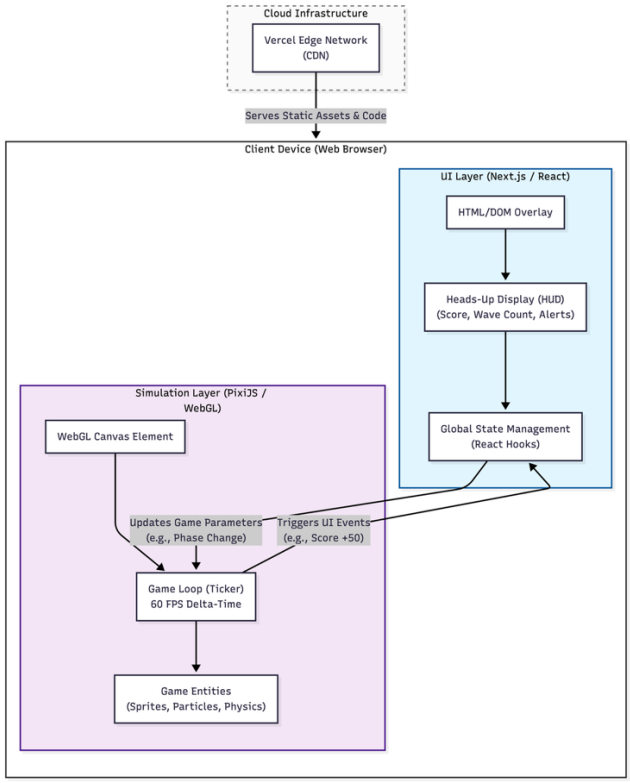

Figure 14: High-Level System Architecture. The diagram illustrates the hybrid rendering approach, where the Next.js UI layer (DOM) manages the global state while the PixiJS layer (WebGL) handles high-frequency simulation physics.

In order to meet the level of performance required for a real-time simulation in a defensive context, a hybrid rendering method has been chosen and implemented by the application. The user interface itself, including menus, a HUD system (Heads-Up Display), and a tactical log system, has its user interface built by means of a React.js application stack referred to as Next.js. This choice was based on its solid component-based architecture, permitting a complex "Global State" management by means of React Hooks. This "Global State" refers to variables including score, wave phase, and learning cards.

However, standard web technologies that make use of the native browser's DOM are inherently insufficient for the high-frequency motion that needs to be displayed for the game simulation itself. For this reason, the project integrates the high-performance 2D rendering engine PixiJS, which uses WebGL for hardware acceleration during rendering, (see Figure 14). This dichotomy of responsibilities is important for the "application logic and UI overlay," thanks to the use of Next.js, while the "Game

Canvas," showing the sprites, explosion effects, and even physics-heavy calculation for game objects alike, can pride itself on displaying 60 fps across the stable performance of the game.

The software development process undertaken for Port Under Attack was non-conformal to the conventional "Waterfall"-style Software Development Life Cycle (SDLC), which depends upon strict sequential steps in software requirements definition, software design, and software implementation. Though this approach has a high level of certainty in software development projects in general, it lacks adaptability to a creative process like game software development, in which the potency of a pedagogical software element—such as a difficulty curve of a "Signal Fade"-style scenario—can only be assessed through genuine playtesting of software prototypes composed around it.

Rather, the project used an Agile Methodology. More specifically, an Iterative and Incremental Software Development Approach was used. This means that adaptive software development and rapid prototyping are given high priorities within this methodology. In this way, a dynamic response to various challenges faced during software development is enabled. In other words, the dynamic and evolutionary nature of this type of system development ensures that various features can be developed and tested independently. In this respect, the "Active Defense Loop" was prototyped and iteratively changed many times to make sure that its feedback timing is compatible with Chapter 3.

To operationalize this Agile methodology, a ClickUp app was used, which is a cloud-based project management tool. It was used to systematize the process by creating a Kanban board with tasks flowing through various states or columns, including "Backlog," "In Progress," "Testing," and "Completed".

This system enabled further decomposition of intricate "Epics," i.e., overarching objectives like "Implement Spoofing Mechanics," into smaller "User Stories," i.e., minute actionable items such as "Code Position Jump Logic" and "Design Red Flash Asset". This helped manage dependencies to perfection. For instance, before graphics were created for a ship, the underlying code logic was settled. In addition, this documentation acted as a "living design document," which kept track of all developments and ensured that the final product remained strictly aligned with the underlying academic objectives.

4.2 Game Engine Logic and Performance Architecture

The core simulation engine of Port Under Attack is based on a deterministic "Game Loop" architecture powered by PixiJS. In contrast to standard DOM-based web applications, which invalidate the interface only on discrete user events-which include clicks and scrolls-a serious game simulation requires a continuous high-frequency update cycle running typically at 60 FPS, recalculating the state of every entity in the

maritime domain. This section is about object management, the algorithmic implementation of the movement physics, and collision detection systems.

4.2.1 The Render Loop and Temporal Delta Consistency

In order for the simulation to be consistent, regardless of devices' processing power, e.g., a high-end desktop compared with a mobile tablet, the engine relies on a Delta Time (Δt) normalization strategy. The PixiJS Ticker system invokes the update loop continuously but, in real-world terms, the time between frames would change depending on the CPU's load.

If the simulation simply added a fixed value for the velocity every frame, such as through ($x \mathrel{+}= 5$), a device running at 120 FPS would result in moving the ships twice as fast as one running at 60 FPS and would invalidate the pedagogical validity of the reaction time testing. To solve this, all of the physical calculations have been normalized against the time elapsed since the last frame. The updated position formula for any entity E is given by:

$$P_{new} = P_{old} + (V \times \Delta t)$$

Where:

- P represents the entity's position vector (x, y).
- V represents its velocity vector (pixels per tick).
- Δt is the scalar time difference coefficient (where 1.0 represents the expected frame duration of ~16.6ms).

This implementation ensures that a "Slow Drift" ship moves at the exact same perceptible speed regardless of hardware frame rate.

4.2.2 Vector-Based Movement and Interception Physics

The motion of both vessels and defense rockets is based on 2D vector calculations. Vessels follow a normal, non-dynamically calculated vector motion in a linear path towards the port (V_x < 0, V_y = 0),while the calculation for the firing of defensive rockets is dynamic to hit a moving target.

Once the player authorizes a strike action by the engine, it will calculate the angle of rotation (θ) by which the rocket sprite must turn to point at the target vessel. This calculation will make use of the inverse tangent of the difference between the target coordinates (T_x , T_y) and the coordinates of the rocket sprite (R_x , R_y):

$$0 = \arctan 2(T_y - R_y , T_x - R_x)$$

Once the angle is determined, the rocket's velocity vector is decomposed into its Cartesian components to drive the frame-by-frame animation:

$$V_{rocket\_x} = S \,.\cos(\theta)$$

$$V_{rocket\_y} = S \,.\sin\,(\theta)$$

where S is the scalar speed of the projectile. This trigonometric calculation permits the game to visually simulate for the audience a precision strike and reinforces the "Iron Tower" narrative of advanced defense technology.

4.2.3 Object-Oriented Entity Management

The code relies on the hierarchical scene graph of PixiJS; every visual element is treated as a programmable "Object", not just some static image. The specific task at hand will define how it extends the core PIXI.Container and PIXI.Sprite classes to create custom game entities that hold both their visual graphics and their logic. This architecture is based on a master BaseShip class, which defines the common properties all vessels have: movement velocity, hitbox dimensions, and click event listeners. This BaseShip class is "extended" by subclasses specific to each threat type, namely FadeShip, JumpShip, and GhostShip, etc…, These subclasses override the common update() function to inject their interference pattern. For example, the class for JumpShip contains the code to teleport, while the BaseShip just moves left. Such an Object-Oriented approach enables the main Game Loop to handle every vessel generically as a "Ship", with each object running its own unique behavior.

The way the simulation manages its game entities is through a very rigid Object-Oriented Programming (OOP) style for maximum memory efficiency. Each vessel is not represented as an image object but as a much more specialized object derived from the general Pixi.Sprite class, The component-based design allows for the varied behavior of the "Scenario Ships". A parent Ship class provides standard rendering and hitbox properties. The hostile threat classes inherit from this parent, injecting specific interference logic while avoiding code duplication.

The "Jump" Logic, This subclass redefines the normal update method with a non-linear function. In this function, an inherently random offset is added to the position vector every N frames.

$$P(t)_{jump} = P(t) + \text{Random}(\pm\delta_{offset})$$

"The Ghost" Logic, The subclass follows the logic for the hierarchy of a scene graph. In this subclass, "Real" ships are the parent nodes, while "Phantom" ships are child nodes. By acquiring the matrix of the parent's transformation matrix, the ghosts mimic the

movement of the parent's vector (V_{parent}) while keeping an offset locally (P_{local}) Thus, the ghosts mimic the impression of a cooperative multi-source spoofing attack.

4.2.4 Collision Detection and Boundary Logic

Since this is a linear path based on the port defense problem domain and traverses from East to West, this highly optimized AABB is used to check when failure occurs. Instead of a computationally expensive check to see if two polygons intersect, we rely on keeping track of the x-coordinate of all active vessels with respect to a constant X_{port}. This is essentially where we determine the port polygon visual boundary is. The failure condition is evaluated logically as:

$$\text{IF}(Ship_x < X_{port})\text{AND}(Ship_{state} \neq \text{Neutralized}) \rightarrow \text{TRIGGER CollisionEvent}$$

For the "Rocket Strike" impacts, the engine utilizes a Euclidean Distance check to determine when the projectile has reached its target. The distance d is calculated each frame:

$$d = \sqrt{(T_x - R_x)^2 + (T_y - R_y)^2}$$

When $d < Threshold$ (typically 10 pixels), the engine registers a direct hit, triggering the particle explosion system and removing the enemy entity from the render batch to free up memory.

4.3 Deployment and Accessibility Architecture

Another critical requirement for educational software is that of "Universal Accessibility," which means that users should have access to the game with any device. In order to do this within our project, we have to leverage a cloud-native deployment mode with responsive front-end UI and Continuous Integration/Continuous Deployment.

4.3.1 Responsive Interface Design

The application uses a hybrid responsive strategy to maintain the playability of the game across disparate screen aspect ratios, for example 16:9 Laptops vs. 4:3 Tablets.

UI Layer Next.js: The HUD (score, wave counter, and classification dropdowns) is constructed using CSS Flexbox. This allows the interface elements to "float" and anchor themselves to the edges of the screen like, for example, the Score is always Top-Right and ensures that these never obscure the central game play area whatever the screen

dimensions.

The Simulation Layer (PixiJS): A "Fixed Logical Resolution" strategy is used. The internal game engine will do physics calculation on a virtual, normalized 1920x1080 coordinate system. The canvas itself is then scaled by CSS transform into the user's window, while still maintaining the crucial 95% / 5% spatial ratio between the Maritime Domain and the Port. This makes sure that the "Time-to-Impact" stays predictable; be it on a large monitor or on a tiny smartphone, a ship traveling at 50 pixels/sec will need the same amount of time to cross the screen, and the pedagogical difficulty curve is preserved on any device.

4.3.2 Continuous Integration and Deployment (CI/CD)

The project deploys a stringent automated Continuous Integration, or CI, via GitHub Actions to guarantee the stability of its simulation logic before those reach production. This is a quality assurance configuration, not just a utility for maintaining code integrity. The workflow is architected to trigger automatically whenever a developer pushes code onto the repository or opens a Pull Request. Defining these rules in a YAML configuration file located within the .github/workflows directory allows the project to ensure each modification is handled in the same environment of standardized testing, taking the variability away from individual developer machines.

Specifically, the implementation was named "Production Build Check," and it uses the command to start up a virtualized Ubuntu environment through the GitHub Actions runner's instantiation. Once initialized, the system will sequentially check out the latest version of the code snippet, set up the Node.js environment to match the specifications of the server's environment, and run the "rm -rf .next" command to ensure that version differences will not hinder the implementation successfully. Once the dependencies have been successfully installed, the build script will run (this is executed through "npm run build"). This is an important step as the application is built on top of Next.js, and during the build step, there is static checking, where if any type, syntax, or image issues exist, the build will stop immediately, never allowing the bad code to be deployed to the "live" URL and thus ensuring that the integrity and usability of the educational tool are maintained.

This process replaces a manual and error-prone process with a deterministic process by the following steps:

- Version Control (Git): Any code change follows the standard path within a Git repository where "Feature Branches" (eg, feature/ghost_ship_logic) can be made.

- Automated Build Pipeline: Once code is committed to the source code repository, a GitHub Action kicks off the execution of a build script pertaining to the code committed. This script builds the Next.js web application (see Figure 15) as well as optimizes the static resources (ship sprites, sounds, etc.).

- Reference: Running a command like `npm run build` will check for errors that might prevent some code from working properly, and that code will not be deployed to

- Immutable Deployments: Each successful build is automatically deployed on Vercel to have its own "Preview URL". This provides the capability to conduct A/B testing on various difficulty configurations prior to their merging into the "Production" branch.

```yaml

name: Production Build Check

on:
  push:
    branches: [ "main" ]
  pull_request:
    branches: [ "main" ]

jobs:
  build:
    runs-on: ubuntu-latest

    strategy:
      matrix:
        node-version: [18.x]

    steps:
    - name: Checkout repository
      uses: actions/checkout@v3

    - name: Set up Node.js ${{ matrix.node-version }}
      uses: actions/setup-node@v3
      with:
        node-version: ${{ matrix.node-version }}
        cache: 'npm'

    - name: Install Dependencies
      run: npm ci

    - name: Run Linter (Static Analysis)
      run: npm run lint

    - name: Verify Build
      run: npm run build

```

Figure 15: The GitHub Actions CI Configuration (.github/workflows/ci.yml)

After this successful CI check, Continuous Deployment, better known as CD, is handled through Vercel. In contrast to CI, which checks verification, the process of CD focuses on delivery. Vercel continuously monitors the Git repository, and with a "success" signal from the pipeline, it automatically pulls in the validated code, optimizes all of the assets for the Edge Network, and hot-swaps the production URL to point to the new version. Thereby, it creates a bullet-proof "Zero-Downtime" deployment cycle because of the smooth passing of the baton from GitHub Actions for verification to Vercel for delivery.

4.3.3 Global Accessibility via Edge Network

The final application is hosted and served by a platform called "Vercel Edge Network," which is a "Content Delivery Network" (CDN). This processes the game's assets to various server nodes located across the world, reducing "Time to First Byte" (TTFB). This will ensure that the high-resolution assets, such as an explosion particle texture, are immediately served to students located anywhere in the world, The infrastructure makes the simulation accessible to users beyond a single machine by supporting hundreds of concurrent users without server degradation.

5. EVALUATION

In order to test the underlying hypothesis, which relates to active simulation and its positive effect on improving the GNSS threat identification process, a quantitative one group Pretest-Posttest experimental design has been designed as explained in figure 16. This accepted framework within educational research was defined by (Campbell and Stanley 1963), enabling the measurement of knowledge gain through a comparison of the participants' performance before and after the intervention-the gameplay session.

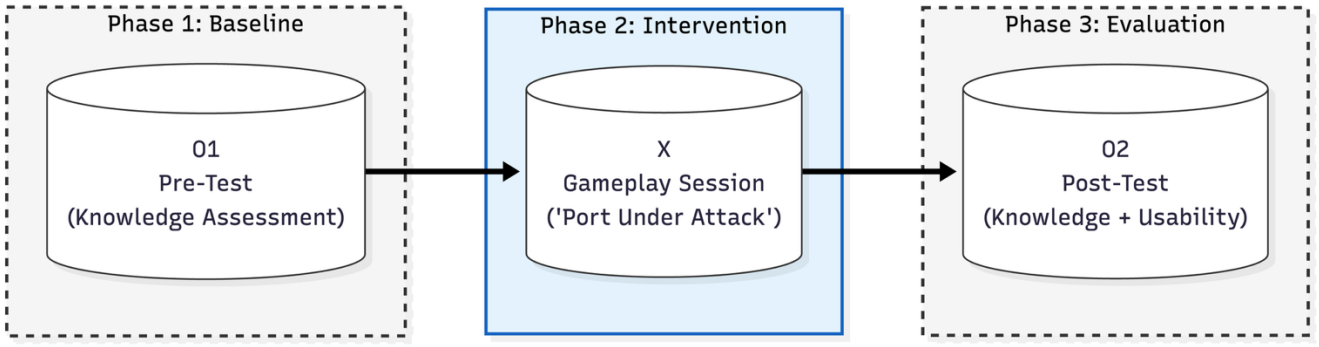

Figure 16: The One-Group Pretest-Posttest Experimental Design

This chapter dives deep in the experimental procedure, the research instruments used, and the specific statistical framework used to deliver answers regarding to the three Research Questions defined in Chapter 1, the phases are explained in Figure 16.

5.1 Experimental Design and Procedure

The evaluation approach was conceived with the view to assess three different variables, The sampling method adopted for recruitment was purposive sampling with a target group size $N = 21$ from Geospatial Technologies masters program students and students in the information technology fields. The criteria adopted ensure sampling from individuals with a certain level of understanding in areas such as navigation or technology but without an expert understanding in identified areas regarding GNSS signal vectors. The goal in all cases was ensuring that the target group corresponded

with the "learner profile" category needing skill development in areas such as detection techniques for information security scenarios.

The three main outcomes of the evaluation are the Pedagogical Effectiveness (RQ1) by quantifying the specific knowledge gain in threat identification accuracy between pre- and post-intervention states, testing the hypothesis that active simulation enhances pattern recognition, Second, measuring System Usability (RQ2) to guarantee that the web-based interface functions as an accessible educational tool without introducing technical friction, Third, assessing Learner Perception (RQ3) to determine if the gameplay experience successfully translates into a higher degree of self-reported confidence regarding complex GNSS security operations.

Regarding data collection and data protection, Two different online tools were used for this thesis, developed by Google Forms, formed the framework from which the data was collected and contains of 2 main parts, Pre-Test and Post-Test, The Pre-Test, which served as a questionnaire, gathered demographic responses and presented 8 multiple-choice technical questions of theoretical definition, such as: (e.g., "What is the primary mechanism of a Jamming attack?"), while the Post-Test, taken after immediately completing gameplay, again measured 8 concepts via scenario questions in order to ascertain "Knowledge Gain". Furthermore, it incorporated "Perceived Learning," employing Likert scale questions assessing participants' level of confidence in their responses, Lastly an SUS assessment in order to evaluate system access through an established methodology with proven reliability in data collection with smaller demographic samples sizes, such as in this situation, where The SUS is known for its reliability in assessing accessible systems (Brooke, 1996), Researcher Ethical Guidelines were strictly followed in relation to Art. 13 GDPR EU Regulation (European Parliament, 2016), utilizing an electronic consent mechanism in order to guarantee confidentiality in results collection. A data protection and consent form was sent to all participants prior to the evaluation, and the full document is available in the ANNEX.

In summary Post-Test used as Assessment Test where it's data will used for measuring and answering the research questions as the Knowledge Assessment (RQ1), System Usability Scale (RQ2) and Confidence Self-Assessment (RQ3).

The procedure of the evaluation start by sending thesis evaluation call for participants, the form included in the Annex where the evaluation process explained in details to guide the participants to effectively participate completely, the experiment followed a 3-step workflow:

1. Induction: Participants received an invitation via email and fill the Pre-Test.

2. Intervention: They were directed to the *Port Under Attack* web simulation, where they completed the Tutorial and engaged with the "Learning Mode" and "Serious Mode" for an estimated 20–30 minutes. link: https://portattack.vercel.app/

3. Evaluation: Immediately upon completing the mission or failing, participants accessed the Post-Test link to record their results and qualitative feedback.

The content of the questionnaires can be found in ANNEX.

5.2 Quantitative Analysis Framework

This segment will outline the statistical framework developed to assess the collected data metrics, Due to the small sample size ($N = 20$), non-parametric statistical tests were selected to ensure the validity of the results.

5.2.1 Demographic Distribution

First analysis will classify the pool of participants ($N = 20$) based on the data from the Pre-Test. Frequency distributions were created to represent the participants' educational backgrounds and past experience with GNSS technologies. This demographic profiling was necessary to ensure that the sample truly represented the desired target "novice-to-intermediate" learner profile and that subsequent performance data is not contaminated by expert-level participants.

5.2.2 Measuring Knowledge Acquisition (RQ1)

In order to answer Research Question 1, a comparative analysis tool will be utilized, which compares the Baseline Score, i.e., Pre-Test, and Evaluation Score, i.e., Post-Test. Since the total number of participants is low $N < 30$ descriptive statistics will be carried out using the following.

Wilcoxon Signed-Rank Test, Instead of a standard paired t-test, the Wilcoxon Signed-Rank Test was utilized to evaluate the probability of observable differences ($p < 0.05$). This test is recommended for small sample sizes that will not follow a normal distribution (Field, 2013; Hollander et al., 2013).

Normalized Learning Gain (g)**,** To measure the effectiveness of the instructional design independent of the students' starting knowledge, Hake's Normalized Gain Hake's (1998) was calculated using the formula:

$$g = \frac{\%Post - \%Pre}{100\% - \%Pre}$$

As a result a positive normalized gain indicates improvement in post-test performance relative to baseline.

.

5.2.3 System Usability Scoring (RQ2)

To examine Research Question 2, raw data from the 10-item System Usability Scale would be analyzed through (Brooke's 1996) standard algorithm:

1. For odd-numbered items, i.e., 1, 3, 5, etc., it is that value minus one.
2. For even-numbered items (i.e., 2, 4, 6, etc.), the score contribution is 5 minus the position in the scale
3. The sum of each contribution will then be multiplied by 2.5 as a means of creating a normalized Usability Score between the value ranges of 0 and 100. The end result will then be subject to a standardized assessment by referencing the Adjective Rating Scale as proposed by Bangor et al. (2008). The Usability score will then determine if it is "Above Average" if higher than 68 and "Excellent" if higher than 80.3. This provides an indication of perceived usability of the system.

5.2.4 Perception and Confidence (RQ3)

To answer RQ3, descriptive statistics of participant feedback regarding the questions related to their self-confidence were used. Likert scales have an ordinal data scale, which ranges from 1 to 5, and hence, the Median and Mode were used for finding the data points related to user sentiment concerning their ability to distinguish between Jamming and Spoofing attacks.

5.3 Qualitative Feedback

Aside from these quantifiable results, another important feature of this evaluation was the qualitative feedback collected in the Post-Test, which served to contextualize how the results were produced, based on the triangulation of such numeric results with the actual user experience.

To do this, open-ended questions about the difficulty and interest experienced by the user were analyzed through an Inductive Thematic Analysis technique (Braun & Clarke, 2006), with three aspects of the user experience analyzed, **Visual Clarity**, as how intuitive metaphors such as the 'Ghost Ship' were, **Scaffolding Effectiveness**, as the adequacy of the 'Learning Mode' supporting element; and **Technical Friction**, as those aspects of the technical system which may have hindered the learning process. Quotes from user experiences are used to contextualize these results in the Results chapter.

6. RESULTS AND DISCUSSION

This chapter will introduce the empirical results that have been gathered through the evaluation of the "Port Under Attack" game. The results are analyzed in relation to the research hypotheses..

Data Processing and Analysis Framework To ensure statistical accuracy and reproducibility, all data analysis was performed programmatically within a Python environment. The raw data collected during the Pre-Test and Post-Test phases was exported in CSV format and pre-processed using the Pandas library to handle missing data and convert categorical responses on the Likert scale to numerical values.

Statistical hypothesis testing, employing the Wilcoxon Signed-Rank Test, was carried out using the SciPy (scipy.stats) library, while data visualization was done using Matplotlib and Seaborn libraries to ensure proper representation of data in the visualizations. This enabled the automatic computation of complex values such as Hake's Normalized Learning Gain (g) and the System Usability Scale (SUS) score, ensuring computational reproducibility and transparency in the final results, lastly to triangulate these results with the qualitative user feedback, Natural Language Processing (NLP) methods were employed. The TextBlob library was used for lexicon-based sentiment polarity analysis, and the WordCloud library was used for the visualization of the lexical frequency distributions.

6.1 Participant Demographic Profile

The sample for the study was made up of 21 participants recruited using purposive sampling ($N = 21$). As shown in Figure 17, the largest proportion of the sample (85.7%) are students with backgrounds in engineering or technical disciplines, while (9.5%) of the sample comprised professionals in the field of Logistics or IT security and remaining (4.8%) were from other backgrounds. This sample composition reflects the purpose of the study, which is to assess the effectiveness of the tool on individuals who have basic technical literacy but are not experts in GNSS security

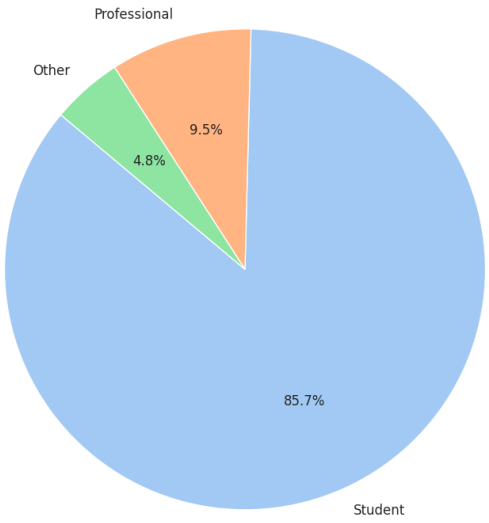

Figure 17: Distribution of participants by academic and professional background (N=21).

The age of the participants varied between 24 and 33 years, with an average age of 27.8 years (SD = 2.4). In line with the principles of data minimization and privacy,

gender demographic information was deliberately not collected for this research. The evaluation was centered on the participants' technical knowledge and academic background, which are the primary modifying variables for cognitive learning gain in cybersecurity, and not on a gender-based comparison.

In order to guarantee the validity of the measurements of the learning gain (RQ1), it was essential to verify that the sample was not composed of experts, which would have caused a "ceiling effect" in the pre-test data. The participants were asked to evaluate their level of prior knowledge of GNSS technologies using a Likert scale ranging from 1 (No Knowledge) to 5 (Expert).

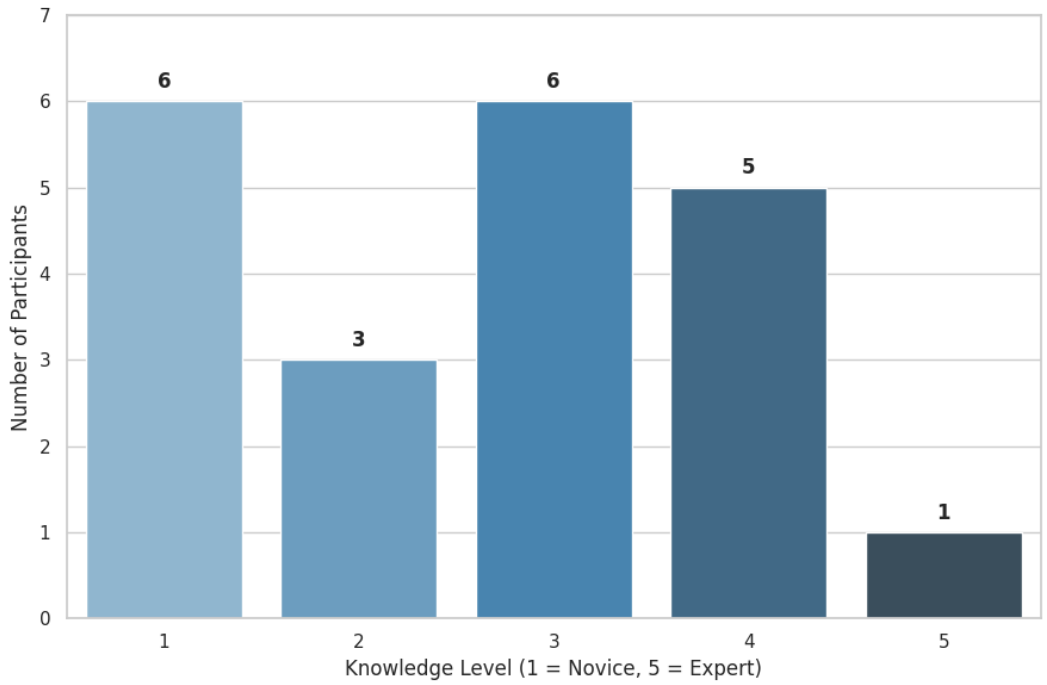

Figure 18: Frequency distribution of self-reported prior knowledge of GNSS technologies (1 = No Knowledge, 5 = Expert).

As illustrated in Figure 18, there is an obvious skew in the distribution of prior knowledge towards the novice/intermediate level. To be more precise, 42.8% of the participants ($n = 9$) assessed their knowledge to be low (Levels 1-2), while 28.6% ($n = 6$) chose the intermediate level (Level 3). Only one participant (4.8%) assessed themselves to be experts. This further reinforces the fact that the sample represents the "learner profile" intended, thus ensuring that the observed gains in performance are a result of the educational intervention and not due to prior knowledge.

6.2 Pedagogical Effectiveness (RQ1)

To assess the effectiveness of the simulation in enhancing the skills of GNSS threat identification, a comparison was conducted between the Baseline Score (Pre-Test) and

the Evaluation Score (Post-Test). As evident from Figure 19, there was a valid improvement in performance after the gameplay intervention.

Descriptive statistics indicate that the mean score has improved from $M = 5.00$ $(SD = 2.81)$ in the Pre-Test to $M = 7.00$ $(SD = 1.57)$ in the Post-Test. The decrease in the standard deviation in the post-test suggests a more homogeneous performance distribution in the post-test, thereby closing the performance gap between those with and without prior knowledge, A detailed breakdown of these descriptive statistics is presented in Table 1.

Table 1: Descriptive Statistics of Pre-Test and Post-Test Scores

Assessment Phase	Mean (M)	Std. Deviation (SD)	Median	Min	Max
Pre-Test	5.00	2.81	6.00	1	8
Post-Test	7.00	1.57	8.00	4	8

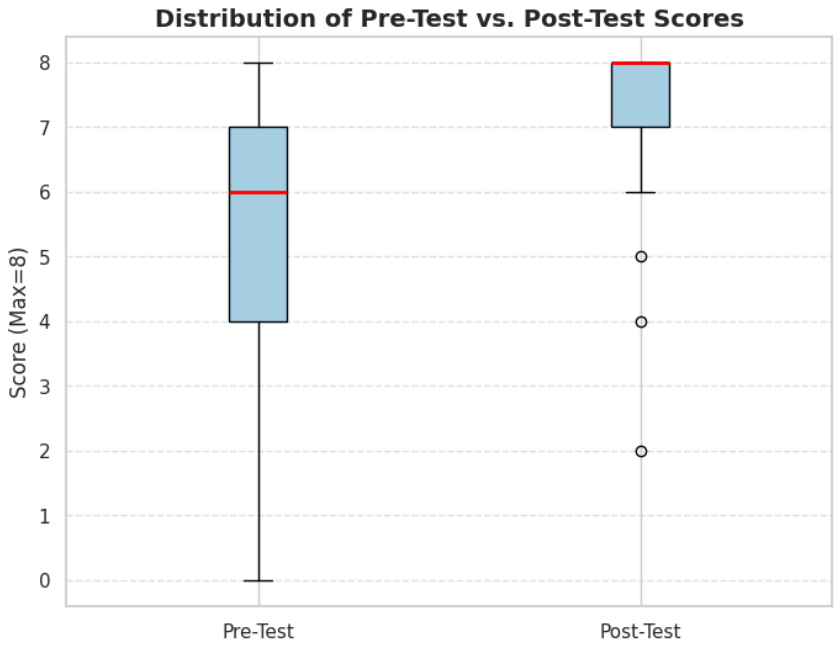

Figure 19: Comparison of Pre-Test and Post-Test score distributions.

To verify the statistical significance of this gain, the Wilcoxon Signed-Rank Test was applied. This non-parametric test was selected due to the small sample size $(N = 21)$ and the paired structure of the data. The test showed a notable difference between the

pre-test and post-test results ($Z = 2.29, p = 0.0218$), thus rejecting the null hypothesis. This suggests a notable increase in participants' ability to recognize GNSS threats.

Secondly, the instructional efficiency was calculated using Hake's Normalized Gain (g). This value calculates the ratio of the actual gain to the maximum possible gain, thus isolating the learning gain from the pre-existing knowledge (Hake, 1998). The results showed that the average gain was $g = 0.83$, which falls into the "High" level of effectiveness ($g > 0.7$). As shown in Figure 20, the learning gains are skewed to the right, indicating that most of the participants gained a notable amount of knowledge regardless of their pre-existing knowledge level.

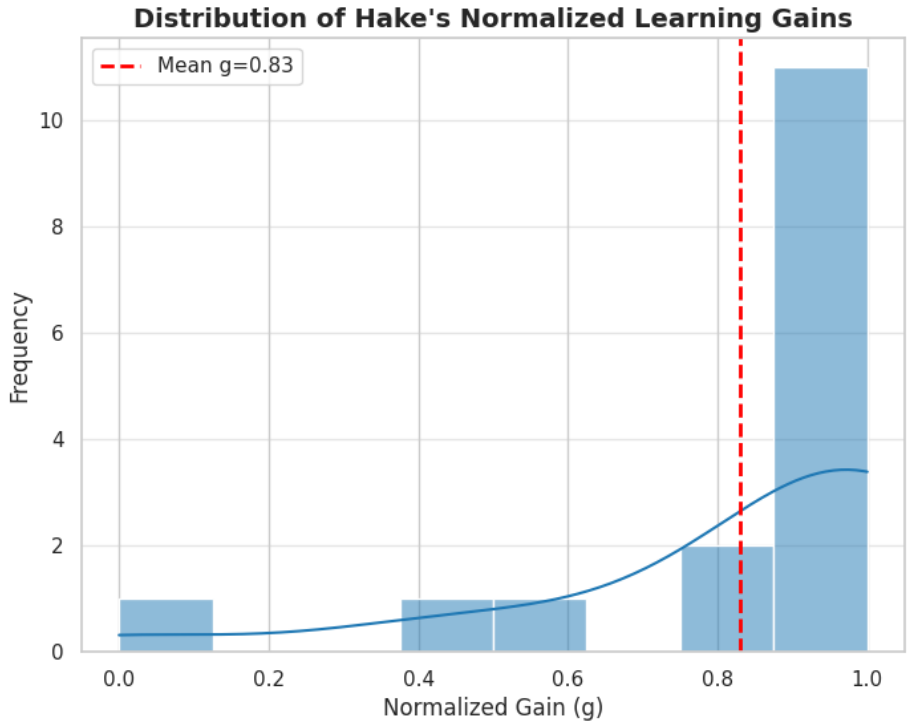

Figure 20: Distribution of Hake's Normalized Learning Gains (g).

Consequently, the response to Research Question 1 is positive. The results of the statistical analysis reveal that "Port Under Attack" contributed to the enhancement of learning outcomes, increasing the average score from 5.00 to 7.00. In addition, the large Normalized Learning Gain ($g = 0.83$) reveals that the game was not only entertaining but also demonstrated substantial learning gains in core GNSS threat concepts, namely the difference between Jamming and Spoofing, to a non-expert audience.

6.3 System Usability Evaluation (RQ2)

To determine the usability and accessibility of the "Port Under Attack" game, the System Usability Scale (SUS) questionnaire was used for all participants. The SUS

provides a single composite score from 0 to 100, which enables a direct comparison with the industry standard of 68.0, which is the benchmark for "average" usability as defined by Brooke (1996).

Analysis of the post-test results indicates that the system has a Mean SUS Score of 80.1 ($SD = 14.0$). As shown in Figure 21, this score is 12.1 points above the industry benchmark, which places it in the "Excellent" category based on the adjective rating scale developed by Bangor et al. (2009). This suggests that participants perceived the interface as intuitive and easy to use, despite the technical nature of the subject matter.

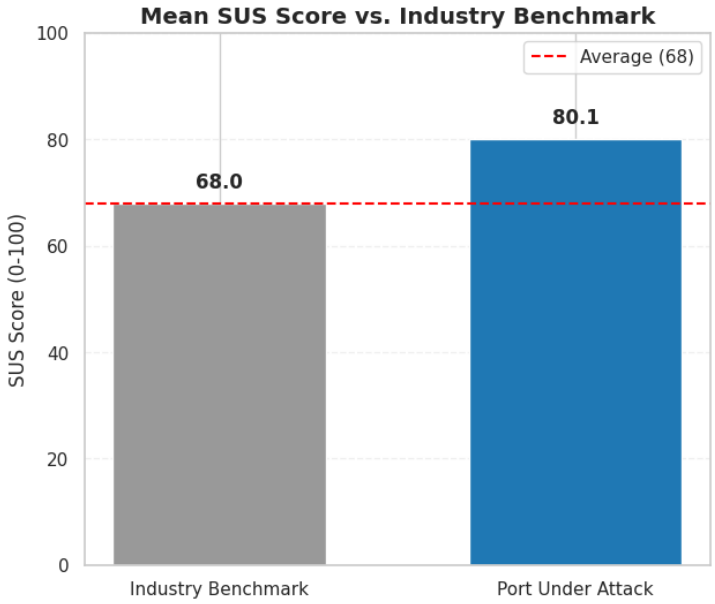

Figure 21: Comparison of the system's Mean SUS Score against the industry benchmark

To further support this result, the distribution of individual usability scores was assessed for any polarization of user experience. Figure 22 illustrates a boxplot of the participant scores with individual data points superimposed. The distribution appears negatively skewed, with the median score (87.5) well above the mean.

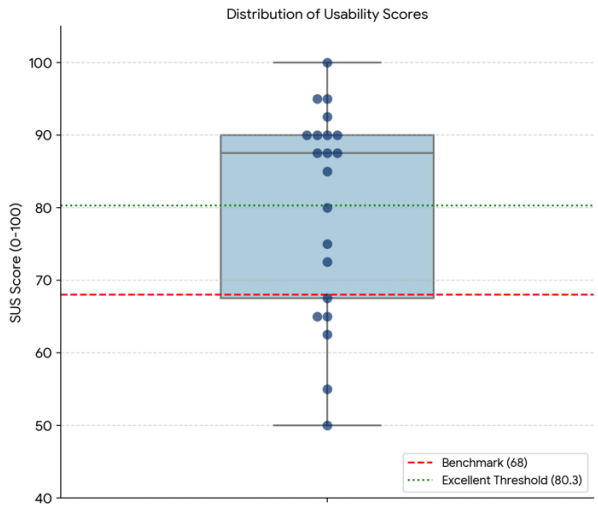

Figure 22: Distribution of participant SUS scores with benchmark thresholds.

Finally, to provide a qualitative assessment of the user experience, the scores were plotted against the standard acceptability thresholds. As illustrated in Figure 23, the frequency distribution clearly shows that 76% of the participants rated the system above the 68.0 benchmark, with the mode of the distribution falling within the 80-90 range. Most importantly, no values fell below the marginal usability threshold of 50. This clustering of high scores suggests relatively consistent usability perceptions across participants with diverse demographic group, supporting that the design of the game was intuitive and accessible.

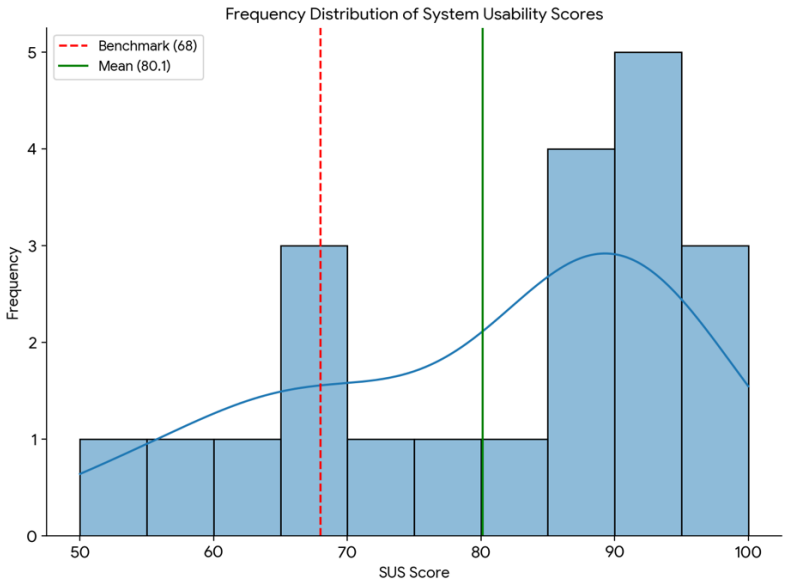

Figure 23: Frequency distribution of System Usability Scores.

6.4 Learner Perception and Confidence (RQ3)

To address Research Question 3, the research aimed to examine the subjective user experience of the learning process. A 5-point Likert scale survey was conducted after the game play, targeting self-efficacy, engagement, and the use of visual metaphors.

The calculation method was involved determining the number of responses for each category (1 = Strongly Disagree to 5 = Strongly Agree) and transformed into percentage distributions to standardize the data for the sample ($N = 21$). The resulting distributions were plotted using a Diverging Stacked Bar Chart to enable a direct comparison between positive (Agree/Strongly Agree) and negative (Disagree/Strongly Disagree) responses.

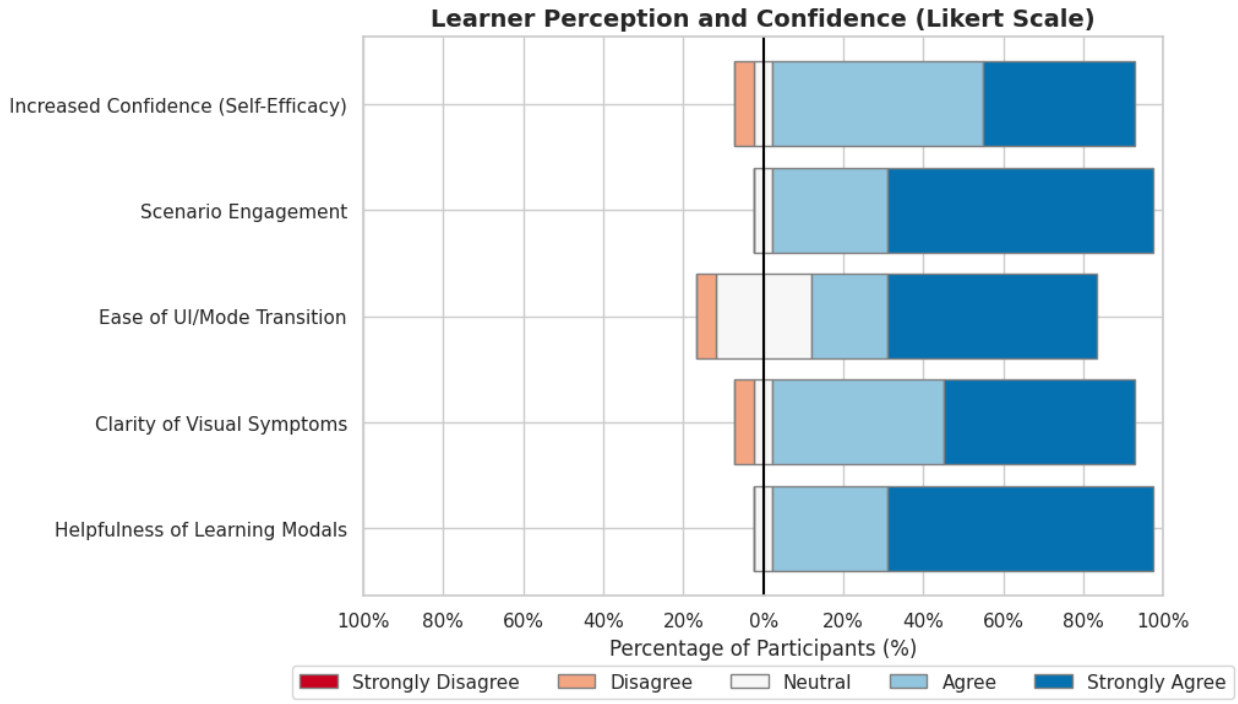

Figure 24: Diverging stacked bar chart of participant agreement with learning experience statements.

As shown in Figure 24, the data shows a high level of user satisfaction and self-efficacy:

Learner Confidence (Self-Efficacy): One of the most important aspects of this finding is that 90.5% of the participants ($N = 19$) agreed or strongly agreed that they felt more confident in identifying the difference between Jamming and Spoofing after playing. This is important because confidence is the precursor to competence, and in a real-world maritime security operation, an analyst must be confident in their decisions in order to act quickly on a threat. The alignment between subjective confidence improvements and the objective score gains (Section 6.2) suggests contribution to the development of perceived operational confidence.

Visual and Scaffolding Effectiveness: The design elements of the "Serious Game" were highly well-received. 95.2% of the participants agreed that the "Learning Mode" modals were effective in understanding the definitions, and 90.5% agreed that the visual manifestations of symptoms (blinking, teleporting) effectively represented the technical aspects. This is a testament to the effectiveness of the "just-in-time" scaffolding approach in teaching non-experts.

Usability of Assessment Mechanics: Although still positive, the lowest agreement score was found in the "Interface Usability" in transitioning to Serious Mode (71.4% Agreement). This is very important to be used in further enhancement for later stages.

Thus, RQ3 is answered in the affirmative. The results from the qualitative analysis have confirmed that the game not only led to improvements in objective performance but also was successful in promoting a high level of self-efficacy and engagement among the participants.

6.5 Qualitative Insights and Discussion

In order to triangulate the results of the quantitative analysis and identify the mechanisms underlying the learning success, a dual-method qualitative analysis was conducted. First, an Inductive Thematic Analysis (Braun & Clarke, 2006) was applied to the open-ended responses to identify key themes such as **Visual Clarity**, **Scaffolding Effectiveness**, and **Technical Friction**. Subsequently, an automated text analysis was performed on the open feedback questions. This analysis combined the results of all five qualitative questions in the post-test, ranging from "most difficult scenarios" to "visual effectiveness".

As can be seen from the Word Cloud created from the participants' answers (Figure 25), the most prominent words were "Visual," "Signal," "Understand," "Drift," and "Ghost". The prominence of these words suggests strong support to the hypothesis that the particular visual metaphors used were the key cognitive enablers for the users'

experiance, closing the gap between the abstract signal theory and the interface.

Figure 25: Word Cloud of frequently used terms in participant feedback.

Moreover, a sentiment analysis was performed on the user comments using the TextBlob lexicon-based algorithm to establish the polarity of the comments (Range: -1.0 to +1.0). As shown in Figure 26, there were 32 Positive, 15 Neutral, and 19 Negative comments, which indicates that the overall sentiment is predominantly positive. Based on the domain-specific vocabulary, the sentiment analysis results were manually inspected to ensure consistency in the classification and to establish the themes (clusters) that influence the polarity of the sentiments.

Positive Sentiment Clusters: The positive comments centered on Visual Scaffolding and Concept Clarity. The players directly connected the game mechanics to their success in learning, as seen in the following comments: “The ghost ships and the blinking of the ships made it easy to distinguish between the two,” and “The visual representation of signal noise and spoofing was very intuitive”. Another player said, “Seeing the ship jitter and fade makes it concrete”.

Negative Sentiment Clusters: The 19 comments that were labeled as "Negative" (Polarity < 0) were analyzed and found to be linked to Scenario Difficulty and Technical Friction, and not related to dissatisfaction with the educational value. For instance, the comments that were identified as negative by the algorithm included those related to the difficulty of the simulation, such as: “the slow drift because it goes so fast,” and “The game ended too quickly! I would have liked 5 more minutes”. Other negative polarities were linked to UI-specific comments, such as: “The transition to the assessment mode was slightly confusing,” and “The ships moved too fast in Serious Mode”. This supports

the idea that the negative sentiment was linked to the expected frustration of the learner with the difficulty of the game and the user interface, which is consistent with the "Technical Friction" theme.

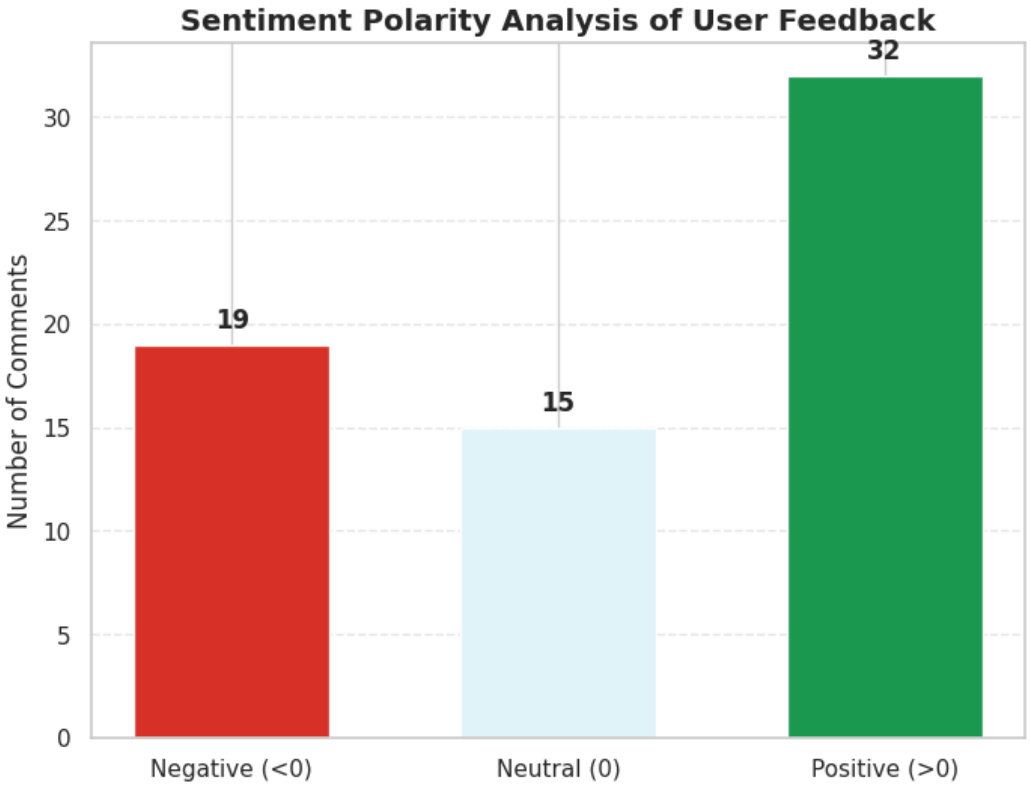

Figure 26: Sentiment polarity distribution of participant feedback (TextBlob Analysis).

The merging of these qualitative findings with the quantitative results enables a strong conclusion to this chapter. The large positive change in post-test scores (Section 6.2) suggests that competence was gained. The high System Usability Score (Section 6.3) demonstrates that accessibility was preserved. Finally, the qualitative sentiment analysis (Section 6.5) suggests that these improvements were made because of the specific visual scaffolding included in the "Port Under Attack" simulation.

In particular, the qualitative feedback indicates that the "Ghost Ship" metaphor successfully closed the gap between abstract signal theory and practical operational detection. The users consistently reported that the ability to see the action (e.g., "blinking" for Jamming vs. "teleporting" for Spoofing) enabled them to get around the requirement for complex mathematical knowledge. This verifies that the serious game appears to have met its primary design objective: to build an intuitive, low-barrier training aid for maritime GNSS security, Furthermore, the analysis of the feedback survey has provided critical insights that have created a roadmap of solutions for future system improvements.

7. CONCLUSION

This thesis presented “Port Under Attack,” a serious game with educational purposes, aiming to teach the basic concepts and methods of GNSS signal interference, particularly jamming and spoofing. the system is based on a cyber-attacked vessels reaching a port under war scenario, which serves as an interactive narrative context where the learner takes on the role of an analyst tasked with the detection of signal anomalies and the interpretation of their operational implications. The main goal was to translate theoretical signal interference concepts into observable events that could be better understood by learners with less experience.

The tasks involved in the work included the design of the serious game and the evaluation of the game-based learning experience. The design of the game involved the development of a high-fidelity web simulation using Next.js and PixiJS. The evaluation showed that the game had a positive effect on both objective threat identification skills and subjective self-efficacy.

7.1 Research Questions Answers

The empirical results offer conclusive answers to the three research questions:

RQ1: To what extent does the serious game "Port Under Attack" improve participants' ability to identify and classify GNSS jamming and spoofing threats (Pedagogical Effectiveness)?
The game was found to be highly effective in improving the participants’ performance in threat identification, with mean scores rising from 5.00 to 7.00. The Hake Normalized Learning Gain (g = 0.83) suggests that the simulation approach is highly effective in teaching GNSS interference concepts to non-experts.

RQ2: How do participants perceive the usability of the developed serious game interface for educational purposes (System Usability)?
The participants found the interface of the game to be very accessible and user-friendly for learning. The SUS test resulted in a score of 80.1, which rates the system as "Excellent”. This suggests that the web-based interface did not create any hindrances in the learning process.

RQ3: How does the gameplay experience influence participants' self-perceived confidence in distinguishing between different GNSS attack types (Learner Confidence)?
The results suggest that the participants’ confidence in self-capability to identify jamming and spoofing scenarios has improved by 90.5% after the simulation. The participants often correlated this improvement with the visual scaffolding approach used in the simulation to make abstract signal behavior more interpretable.

The project goals have been met. This thesis work offers a feasible framework for teaching complex GNSS cybersecurity concepts using the simulation approach.

7.2 Limitations of the Study

Although this research design creates a comprehensive framework through which serious games in this sector can be assessed, certain limitations with regard to the overall scope and generalization of this study must be recognized. First, regarding **sample size and demographics**, this experimental evaluation process employs a purposive sample of $N = 21$ participants from geospatial and technical disciplines. Although this sample population is effectively targeted at the "novice to intermediate" user profile, the sample size is still limited with regard to overall statistical power. Second, regarding **short-term retention**, this experimental process measures "Knowledge Gain" immediately following this process (the gameplay session). Accordingly, this study does not measure retention of these skills (for example, by testing participants two weeks after this process), which would be necessary to measure permanent cognitive anchoring. Lastly, regarding **simulation fidelity,** to accommodate universal web accessibility, this simulation employs a 2D "top-down" interface to abstract the maritime environment, which, while effective at teaching signal logic, does not fully simulate the multi-screen 3D environment of a vessel bridge, which might limit direct transferability of "muscle memory" to physical hardware.

7.3 Future Work

The Port Under Attack game establishes the technical basis for a number of potential research directions that could further improve cybersecurity education by the following ways:

Integration of Real-Time AIS Data: Future versions could be integrated with real-time APIs (such as Spire or MarineTraffic) to create game scenarios based on real-world ship trajectories, This could allow scenarios to reflect real-world vessel traffic patterns traffic and topological characteristics of their own ports (for example, Rotterdam or Singapore).

Adversarial Multiplayer Scenarios: The current system is a single-player "PvE" (Player vs. Environment) experience. Future development could extend this to a "Red Team vs. Blue Team" multiplayer scenario, in which one student plays the attacker with jammers, and another plays the defender. This would be similar to adversarial learning approaches explored in existing cyber-defense games such as CyberCIEGE (Irvine et al., 2005).

Immersive VR/AR Integration: The graphics of the game could be repurposed for a Virtual Reality (VR) or Augmented Reality (AR) platform to enhance immersion and the perception of signal disruption scenarios. This extension would enable future research

to examine the impact of immersive environments on engagement, situational awareness, and decision-making for cybersecurity training tasks.

References

Agile Alliance. (2024). *The Agile Manifesto*. https://www.agilealliance.org/agile101/

Bangor, A., Kortum, P. T., & Miller, J. T. (2008). An Empirical Evaluation of the System Usability Scale. *International Journal of Human-Computer Interaction, 24*(6), 574-594. https://doi.org/10.1080/10447310802205776

BIMCO, ICS, INTERCARGO, & INTERTANKO. (2021). *The Guidelines on Cyber Security Onboard Ships (Version 4.0)*. https://www.bimco.org/regulatory-affairs/policy-positions/cyber-risk-management/

Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology, 3*(2), 77–101. https://doi.org/10.1191/1478088706qp063oa

Brooke, J. (1996). SUS: A Quick and Dirty Usability Scale. In P. W. Jordan, B. Thomas, B. A. Weerdmeester, & A. L. McClelland (Eds.), *Usability Evaluation in Industry* (pp. 189-194). Taylor & Francis. https://www.researchgate.net/publication/228593520_SUS_A_quick_and_dirty_usability_scale

Campbell, D. T., & Stanley, J. C. (1963). *Experimental and Quasi-Experimental Designs for Research*. Houghton Mifflin. https://www.sfu.ca/~palys/Campbell&Stanley-1959-ExptI&QuasiExptIDesignsForResearch.pdf

ClickUp. (2024). *One app to replace them all*. https://clickup.com/

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From game design elements to gamefulness: Defining "gamification". *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments*, 9–15. https://doi.org/10.1145/2181037.2181040

European Parliament. (2016). *Regulation (EU) 2016/679 (GDPR)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Field, A. (2013). *Discovering Statistics Using IBM SPSS Statistics* (4th ed.). https://www.scirp.org/reference/ReferencesPapers?ReferenceID=2046660

Garris, R., Ahlers, R., & Driskell, J. E. (2002). Games, motivation, and learning: A research and practice model. *Simulation & Gaming, 33*(4), 441–467. https://journals.sagepub.com/doi/10.1177/1046878102238607

GPSPATRON. (2025). *Maritime GNSS Interference Worldwide: A Cumulative Analysis*. https://gpspatron.com/maritime-gnss-interference-worldwide-a-cumulative-analysis-2025/

Hake, R. R. (1998). Interactive-engagement versus traditional methods: A six-thousand-student survey of mechanics test data for introductory physics courses. *American Journal of Physics, 66*(1), 64–74. https://doi.org/10.1119/1.18809

Hollander, M., Wolfe, D. A., & Chicken, E. (2013). *Nonparametric Statistical Methods* (3rd ed.). John Wiley & Sons. https://download.e-bookshelf.de/download/0004/0695/89/L-G-0004069589-0002628419.pdf

Irvine, C. E., Thompson, M. F., & Allen, K. (2005). CyberCIEGE: Gaming for information assurance. *IEEE Security & Privacy, 3*(3), 61–64. https://ieeexplore.ieee.org/document/1439504

Kaplan, E. D., & Hegarty, C. J. (2017). *Understanding GPS/GNSS: Principles and Applications* (3rd ed.). Artech House. https://api.pageplace.de/preview/DT0400.9781630814427_A37804737/preview-9781630814427_A37804737.pdf

Lloyd's List. (2024, April 5). *War zone GPS jamming sees more ships show up at airports*. https://www.lloydslist.com/LL1148748/War-zone-GPS-jamming-sees-more-ships-show-up-at-airports

Mayer, R. E. (Ed.). (2014). *The Cambridge Handbook of Multimedia Learning* (2nd ed.). Cambridge University Press. https://doi.org/10.1017/9781108894333

Medina, D., Lass, C., Pérez Marcos, E., Ziebold, R., Closas, P., & García, J. (2019). On GNSS Jamming Threat from the Maritime Navigation Perspective. *22nd International Conference on Information Fusion (FUSION)*, 1-8. https://elib.dlr.de/128050/

Morales-Ferre, R. (2017). *Analysis of GNSS replay-attack detectors exploiting unpredictable symbols* [Master's Thesis, Universitat Autònoma de Barcelona]. ResearchGate. https://www.researchgate.net/publication/339473727

Morales-Ferre, R., Richter, P., Falletti, E., de la Fuente, A., & Lohan, E. S. (2020). A Survey on Coping With Intentional Interference in Satellite Navigation for Manned and Unmanned Aircraft. *IEEE Communications Surveys & Tutorials, 22*(1), 249–291. https://ieeexplore.ieee.org/document/8882350

NATO Research Task Group. (2016). *Serious Gaming Design for adaptability training of military personnel*. NATO Science and Technology Organization. https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-MSG-143/MP-MSG-143-04.pdf

Next.js. (2024). *The React Framework for the Web*. https://nextjs.org/

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77. https://doi.org/10.2753/MIS0742-1222240302

PixiJS. (2024). *The HTML5 Creation Engine*. https://pixijs.com/

Potkonjak, V., Gardner, M., Callaghan, V., Mattila, P., Guetl, C., Petrović, V. M., & Jovanović, K. (2016). Virtual laboratories for education in science, technology, and engineering: A review. *Computers & Education, 95*, 309-327. https://www.sciencedirect.com/science/article/pii/S0360131516300227

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS Spoofing and Detection. *Proceedings of the IEEE, 104*(6), 1258-1270. https://doi.org/10.1109/JPROC.2016.2526658

Sadlier, G., Flytkjær, R., Sabri, F., & Herr, D. (2017). *The economic impact on the UK of a disruption to GNSS*. London Economics. https://www.gov.uk/government/publications/the-economic-impact-on-the-uk-of-a-disruption-to-gnss

Salen, K., & Zimmerman, E. (2004). *Rules of Play: Game Design Fundamentals*. MIT Press. https://mitpress.mit.edu/9780262240451/rules-of-play/

Samčović, A. (2018). Serious games in military applications. *Vojnotehnički glasnik/Military Technical Courier, 66*(3), 597–613. https://doi.org/10.5937/vojtehg66-16367

Schmidt, D., Radke, K., Camtepe, S., Foo, E., & Ren, M. (2016). A Survey and Analysis of the GNSS Spoofing Threat and Countermeasures. *ACM Computing Surveys, 48*(4), 64:1-64:36. https://dl.acm.org/doi/10.1145/2897166

Sitzmann, T. (2011). A Meta-Analytic Examination of the Instructional Effectiveness of Computer-Based Simulation Games. *Personnel Psychology, 64*(2), 489–528. https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1744-6570.2011.01190.x

Spire Aviation. (2025). *GNSS interference report: Russia 2024/2025 - Kaliningrad & the Baltic Sea*. https://spire.com/blog/space-reconnaissance/gnss-interference-report-russia/

Tomaszewski, B., Walker, A., Gawlik, E., Lane, C., Williams, S., Orieta, D., McDaniel, C., Plummer, M., Nair, A., San Jose, N., Terrell, N., Pecsok, K., Thomley, E., Mahoney, E., Haberlack, E., & Schwartz, D. (2020). Supporting Disaster Resilience Spatial Thinking with Serious GeoGames: Project Lily Pad. *ISPRS International Journal of Geo-Information, 9*(6), 405. https://www.mdpi.com/2220-9964/9/6/405

U.S. Department of Homeland Security. (2021). *PNT Integrity Library: Spoofing and Jamming*. CISA. https://www.cisa.gov/resources-tools/resources/pnt-integrity-library

ANNEX

Pre-Test Questionnaire and Answer Key

Section 1: Demographic and User Information

1. What is your email address? [Short answer text]

2. What is your full name? [Short answer text]

3. What is your date of birth? [Date picker]

4. Academic or Professional Background?

- Student (Other Engineering/Technical field)
- Professional (Logistics)
- Professional (Cybersecurity / IT)
- Other

5. How often do you play video games or interactive simulations?

- Daily
- Weekly
- Monthly
- Rarely / Never

6. Prior Knowledge: GNSS/Satellite Navigation?

- 1 (No knowledge)
- 2
- 3
- 4
- 5 (Expert)

Section 2: Baseline Knowledge Assessment *Welcome to the study! Before playing Port Under Attack, please answer these 8 questions to establish your initial understanding of GNSS/SatCom threats, specifically Jamming (interference) and Spoofing (deception). Don't worry if you are unsure of some answers; this is simply to measure your progress later.*

1. What is the primary mechanism of a GNSS "Jamming" attack?

- To trick the receiver into showing a false location.
- **[✓] To emit interference that raises the noise floor, preventing the receiver from tracking satellites.**
- To increase the precision of the satellite clock.

2. Which statement best defines a GNSS "Spoofing" attack?

- A physical obstruction blocking the satellite's line-of-sight.
- **[✓] The transmission of counterfeit signals that force a receiver to compute a false position.**
- A software update that improves the receiver's security.

3. What is occurring when a vessel's reported position suddenly teleports to a different location instantly?

- Signal Fade.
- Complete Blackout.
- **[✓] Position Jump.**

4. A "Complete Blackout" scenario is categorized as which type of threat?

- **[✓] High-power broadband jamming causing a Total Denial of Service (DoS).**
- A subtle spoofing attack designed to bypass security filters.
- A natural loss of signal due to the ship's movement.

5. Why is a "Carry-Off" (Slow Drift) attack considered more dangerous than a sudden jump?

- It uses more power.
- It creates multiple ghost signals.
- **[✓] It moves gradually, often failing to trigger the receiver's integrity alarms.**

6. What is the observable result of a "Signal Fade" jamming attack to a vessel?

- Multiple "ghost" signatures appear on the navigation screen.
- **[✓] Intermittent loss and recovery of the signal as the interference fluctuates near the tracking threshold.**
- The ship begins to move in a perfectly circular pattern.

7. What is a "PVT Discontinuity" in the context of navigation security?

- When the satellite runs out of battery.
- **[✓] An instantaneous, physically impossible shift in the calculated position.**
- A gradual loss of signal accuracy.

8. What does a significant drop in the "Signal-to-Noise Ratio (SNR)" typically indicate to a GNSS Analyst?

- **[✓] Potential low-power jamming or a precursor to a spoofing attack.**
- That the receiver has successfully authenticated the signal.
- That the ship has reached its destination port.

Post-Test Questionnaire and Answer Key

Section 1: Knowledge Assessment *Let's see what you've learned! This section tests your ability to identify specific GNSS/SatCom threats based on the visual patterns and symptoms you just encountered during the simulation.*

1. In the game, you saw a vessel repeatedly fading in and out of transparency (blinking). Which attack does this represent?

- **[✓] Signal Fade (Jamming)**
- Position Jump (Spoofing)
- Complete Blackout (Jamming)

2. When a vessel suddenly "teleports" to a different location instantly, it represents a physically impossible movement known as:

- A high-power Jamming attack.
- **[✓] Position Jump (Spoofing)**
- A natural signal loss due to weather.

3. You encountered a scenario where the vessel froze and a 5-second countdown appeared. Academically, this "Complete Blackout" is:

- A sophisticated "Ghost Ship" spoofing signal.
- **[✓] High-power broadband jamming causing a total Denial of Service (DoS).**
- The receiver successfully cross-checking its position with Radar.

4. A vessel exhibiting subtle, gradual deviation from its path (often tinted yellow/orange) is a "Slow Drift". Why is this spoofing attack dangerous?

- It causes the ship to explode instantly.
- **[✓] It is subtle and designed to bypass standard detection filters over time.**
- It immediately triggers all port safety alarms.

5. If you observed multiple purple-tinted duplicate signatures moving in synchronization with a main vessel, you were detecting:

- Signal-to-Noise Ratio (SNR) degradation.
- **[✓] Ghost Ships (Spoofing).**
- A multi-frequency Jamming attempt.

6. A red circular glow around a ship accompanied by a degrading signal bar represents an "SNR Drop". What does this tell an analyst?

- **[✓] The signal quality is degrading, often as a precursor to a complex attack.**
- The ship has safely entered the port perimeter.
- The GNSS signal is being authenticated by a secure satellite.

7. Based on the game, which category of attack focuses on "deceiving" the receiver with false information rather than "blocking" it?

- Jamming
- **[✓] Spoofing**
- Blackout

8. Which technique is used if an attacker's goal is to "drown out" the legitimate satellite signal with loud noise to prevent any positioning?

- Spoofing
- **[✓] Jamming**
- Meaconing

Section 2: System Usability Evaluation (SUS) *Please rate your agreement with the following statements regarding the game interface (1 = Strongly Disagree, 5 = Strongly Agree).*

1. I think that I would like to use this system frequently.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

2. I found the system unnecessarily complex.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

3. I thought the system was easy to use.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

4. I think that I would need the support of a technical person to be able to use this system.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

5. I found the various functions in this system were well integrated.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

6. I thought there was too much inconsistency in this system.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

7. I would imagine that most people would learn to use this system very quickly.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

8. I found the system very cumbersome to use.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

9. I felt very confident using the system.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

10. I needed to learn a lot of things before I could get going with this system.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

Section 3: Learning and Game Experience *Please rate your agreement with the following statements regarding your learning experience (1 = Strongly Disagree, 5 = Strongly Agree).*

1. The "Learning Mode" modals helped me understand the definitions before I had to identify them.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

2. The visual symptoms (blinking, teleporting, purple ghosts) clearly represented the technical concepts.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

3. I feel more confident in my ability to distinguish between Jamming and Spoofing after playing.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

4. The game interface and transition to "Serious Mode" (dropdowns) were easy to use.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

5. The maritime defense scenario made the technical content more interesting than a traditional text.

- 1 (Strongly Disagree) / 2 / 3 / 4 / 5 (Strongly Agree)

Section 4: Qualitative Feedback

1. Which specific attack scenario did you find the most difficult to identify? Why? [Open-ended response]

2. How did the visual cues (animations and colors) help your understanding of the GNSS threats? [Open-ended response]

3. In your opinion, what was the most effective part of the game for teaching you the difference between Jamming and Spoofing? [Open-ended response]

4. What is one feature you would change to improve the learning experience in "Port Under Attack"? [Open-ended response]

5. Any other comments or suggestions regarding the game? [Open-ended response]

Data Protection form

Data protection policy in accordance with Art. 13 GDPR and consent form

Project/reason: Developing a serious game to teach cybersecurity concepts in GNSS/SatCom systems using geospatial simulation**:**

1. Name and address of the responsible controller

The responsible controller as defined in the EU General Data Protection Regulation (GDPR) and other national data protection laws of the EU member states as well as other data protection-related provisions is:

Universitat Jaume I (UJI) Av. de Vicent Sos Baynat, s/n, 12071 Castelló de la Plana, Castelló, Spain **Email:** proteccio-dades@uji.es

If you have any questions about the project, please contact the responsible staff member: **Amin Alameer** <amin.alameer9@gmail.com> (MSc student of Geospatial Technologies, mastergeotech.info).

2. Contact data of the Data Protection Officer

You can contact the Data Protection Officer at: **UJI Data Protection Office** Edifici de Rectorat i Serveis Centrals **Email:** proteccioalumnisauji@uji.es

3. Data processing in connection with "Developing a serious game to teach cybersecurity concepts in GNSS/SatCom systems using geospatial simulation"

The purpose of this study is to evaluate the effectiveness of serious gaming as a tool for teaching complex cybersecurity concepts, such as jamming and spoofing, within GNSS and Satellite Communication (SatCom) systems. Participants will interact with a geospatial simulation game, *Port Under Attack*, to identify and classify signal threats. Data collected will be used to measure knowledge acquisition and the educational impact of the simulation.

a) Scope of data processing The following personal data is processed in connection with this project:

1. First and last name
2. Date of birth
3. Email address
4. Academic or professional background related to geospatial technologies.

b) Purposes of data processing The personal data listed above is processed strictly for carrying out the research project. The data will be used to draw scientific conclusions about group learning trends. Anonymized data might be published in academic journals, presentations, or open science repositories, but never in a way that allows individual identification. Withdrawal of data from aggregated analyses may not be possible one week after the study's completion.

c) Legal basis for processing personal data Your consent serves as the legal basis for processing your personal data, as stipulated by Art. 6 (1, 1a) GDPR.

d) Further recipients of your personal data Your personal data will not be shared with recipients outside of the research team at Universitat Jaume I.

e) Duration of storage of personal data The personal data listed above is stored for as long as necessary for carrying out the project but shall not exceed 10 years (subject to UJI research data policies). Upon withdrawing your consent, we shall delete your personal data.

Evaluation Procedure: By signing this form, you agree to follow the study workflow in the following order:

1. **Step 1: Baseline Knowledge Assessment (Pre-Test)** Before playing the game, you will complete a short questionnaire to establish your current knowledge of GNSS threats. **Link:** Pre-Test Form
2. **Step 2: Interactive Simulation (Gameplay)** You will then access the *Port Under Attack* simulation. You will act as a GNSS Analyst, using "Learning Modals" to understand theory and "Serious Mode" to identify and classify signal anomalies. **Game Access:** https://portattack.vercel.app
3. **Step 3: Final Evaluation (Post-Test & Feedback)** Immediately after gameplay, you will complete a final form to measure knowledge gain and provide feedback on the game's usability. **Link:** Post-Test & Usability Form

---

Declaration of consent

Subject/reason: Developing a serious game to teach cybersecurity concepts in GNSS/SatCom systems using geospatial simulation

Full name: _____

Date of birth: _____

Email address: _____

With your consent, you hereby grant permission to Universitat Jaume I to collect and process the personal data listed under (3a) for the purposes indicated in (3b). You have the right to withdraw your consent at any time.

With my signature, I indicate confirmation of the following: "I have read the data protection statement for the project **Developing a serious game to teach cybersecurity concepts in GNSS/SatCom systems using geospatial simulation**. I hereby voluntarily consent to having my personal data collected and processed. I have been informed of the scope and purpose of data collection, as well as the right to withdraw consent".

City, Date: _____

Signature: _____

Informed Consent Form

Informed Consent Form

Study title: Developing a serious game to teach cybersecurity concepts in GNSS/SatCom systems using geospatial simulation

Dear Participant, thank you for your participation in the study.

Researcher(s): Amin Alameer - amin.alameer9@gmail.com (MSc student of Geospatial technologies)

Purpose of the study: The purpose of this study is to understand if interactive, scenario-based serious games can effectively support or enhance traditional education in GNSS cybersecurity, specifically regarding jamming and spoofing awareness. In the study, you will use an interactive serious game called *Port Under Attack* which simulates a maritime defense environment. You will act as a GNSS/Geospatial Intelligence Analyst identifying various signal anomalies and classifying attack types. The results will be used to investigate whether gamification and simulation are effective pedagogical tools for teaching complex technical concepts related to Global Navigation Satellite Systems (GNSS) security threats.

Procedure: The study will take place in an individual online session. Before the session, you will receive an information sheet and a consent form by email. At the beginning of the session you will complete a short online questionnaire. This will include a few demographic questions (for example, about your age range and experience with GNSS or geospatial technologies) and a pre-test to establish your baseline knowledge of signal interference and manipulation. After that, you will be guided through a threat identification task using the serious game prototype shown on screen. You will encounter various scenarios, such as signal fading, position jumps, or ghost ships, and will be asked to identify the attack type based on visual behaviors. The researcher will give you clear instructions on how to interact with the game. After specific phases of the game, you will complete a short questionnaire about your experience (for example, how clear the educational content felt). At the end, you will answer a few post-test questions to measure knowledge gain and can share any comments or feedback you have.Your data will be analyzed in anonymized form, so your name will not appear in any results. The whole session is expected to last about 30–45 minutes, and you can take breaks or stop your participation at any time without giving a reason.

Duration: 30 - 45 minutes

Potential risks: This study involves no physical tasks and only minimal risk. All activities take place while seated at a compute. Possible minor discomforts include looking at a screen for about 30–45 minutes, or mild self-consciousness about your performance in

the identification tasks. Participants can take breaks at any time or stop their participation without giving a reason.

Privacy: Original data obtained from this study will be anonymised and only processed to draw scientific conclusions about groups, not about individual participants. Anonymised data might be published in academic journals, presentations, open science data repositories, or other media, but not in a way that would allow individual identification. One week after the completion of the study it might no longer be possible to retract your data from such aggregated analyses. You can contact the researcher in order to access your data or request its removal.

If you have any questions, please ask them now. For further questions, complains or issues, please contact the institute's Ethics-Committee:

amin.alameer9@gmail.com.

- I confirm I volunteered to participate in this study.
- I confirm I was allowed to ask questions and that I was provided with responses.
- I confirm I was presented with this document prior to the beginning of the study.
- I confirm and I understand my right to quit the study at any time.
- I agree to be audio recorded during the study.
- I agree to be video recorded during the study.

Date: _____

Signature of researcher: _____

Signature of participant: _____

Email address (optional): _____ *(Please provide your email address if you would like to be informed about future studies)*

I have read the data protection statement for GNSS Cybersecurity Education Through Serious Gaming and hereby voluntarily consent to having my personal data collected and processed as described in the statement. I have been informed of the right to withdraw my consent at any time without giving reasons.

Email: _____

Signature of participant: _____

Game Visuals

This annex presents the visual interface elements developed for the *Port Under Attack* simulation,

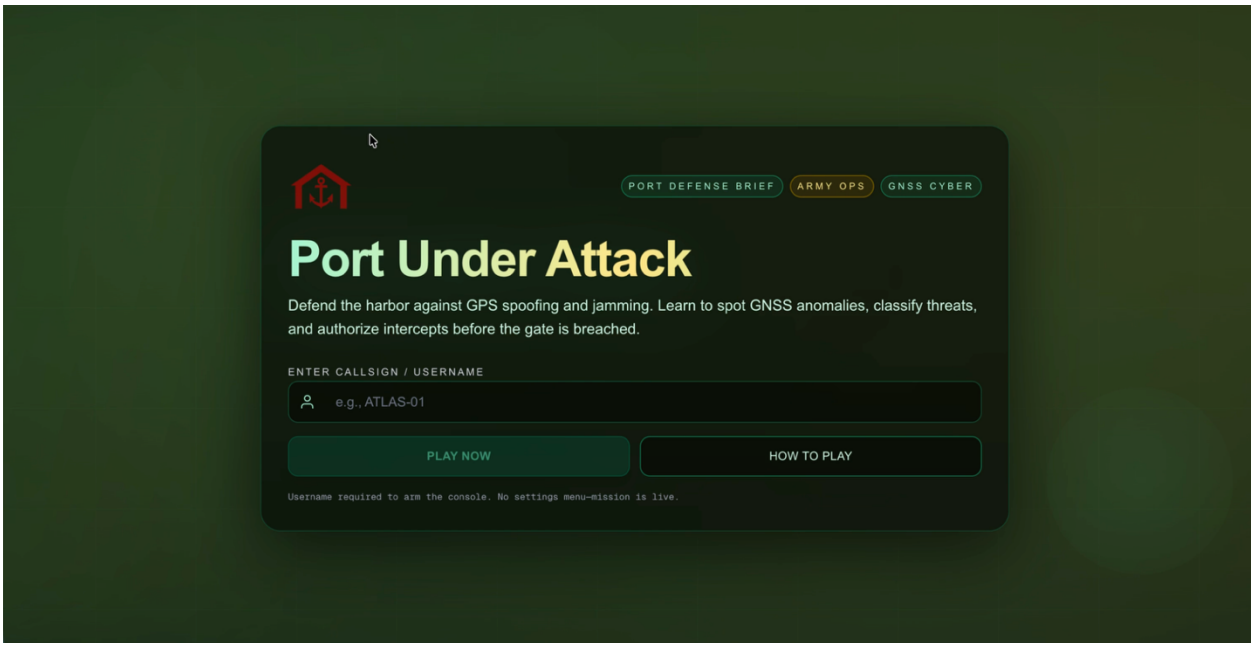

Figure 27: The Main Menu and Identity Creation interface. Users must enter a specific callsign (e.g., ATLAS-01) to initialize the session.

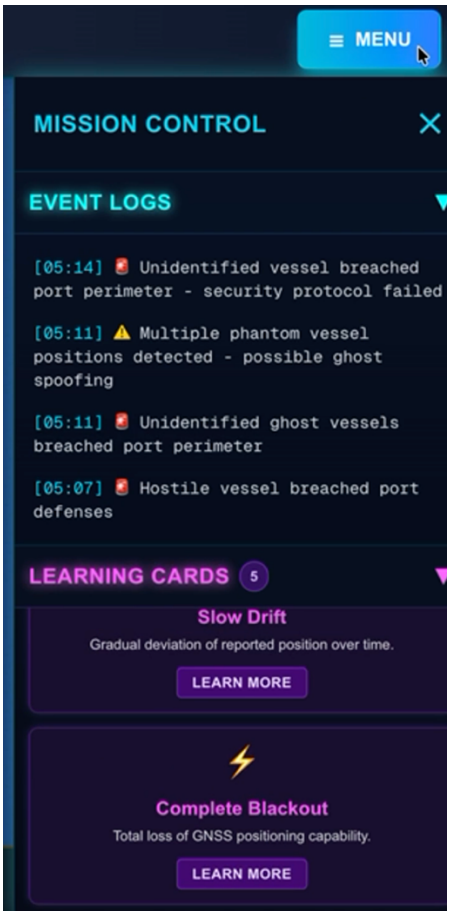

Figure 28: The Mission Control Event Log. This side-panel records every threat detection and security breach in real-time.

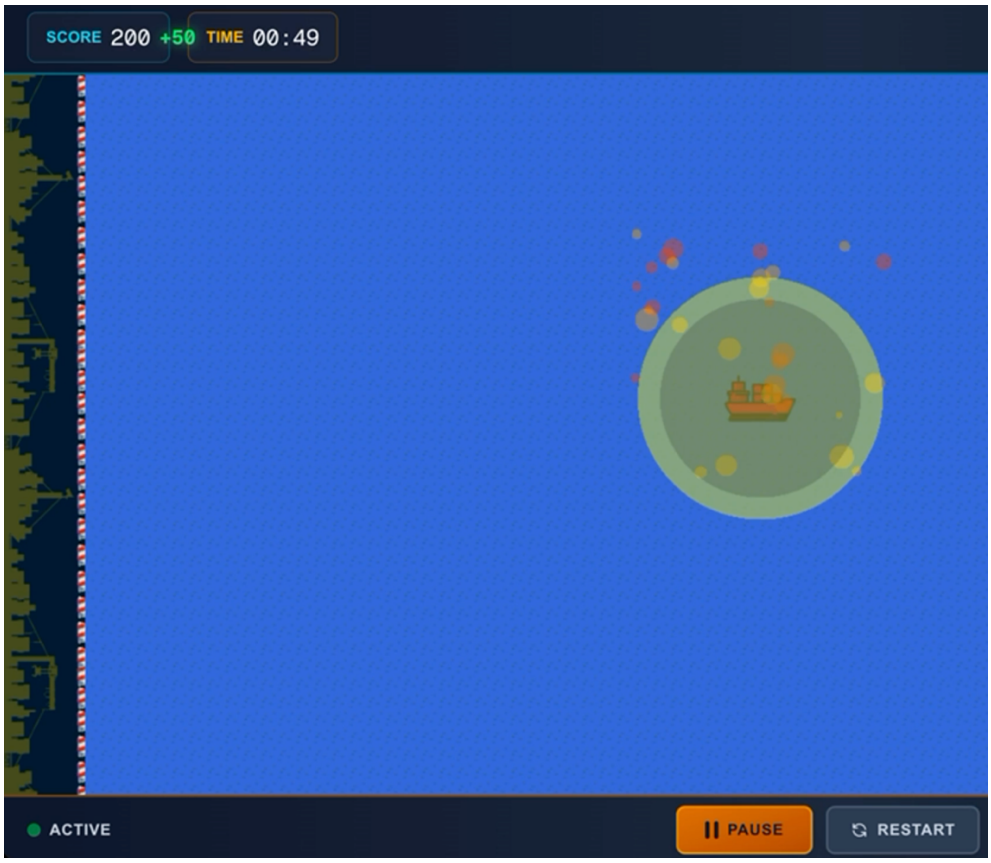

Figure 29: The Heads-Up Display (HUD). The interface highlights the score (+50) and timer, providing immediate feedback.

Figure 30: The Enemy Vessel Sprites. The game renders different effects to simulate different scenarios in order maintain a varied maritime environment.

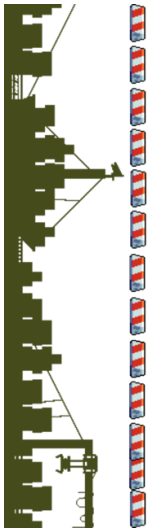

Figure 31: The Port Defense Asset.

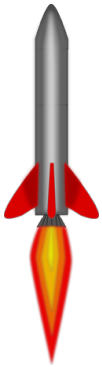

Figure 32: The Missile Defense Asset.

Game Assets

All visual assets used in the game were sourced online and were not originally created by the author.

Port and Industrial Tileset (Environment)

Asset name: Free Industrial Zone Tileset / Industrial Assets Pack

Likely Source: https://craftpix.net/freebies/free-seaport-tileset-32x32-pixel-art-for-platformer/

Disclaimer by author: You can use each product in unlimited number of free and commercial projects.

Cargo Vessel Sprite (Enemy/)

Asset name: Flat Cargo Ship Transport Icon

Likely Source: https://www.flaticon.com/free-icon/cargo-ship_870107?term=cargo+ship&page=1&position=5&origin=tag&related_id=870107

License: Flaticon License (Free for personal and commercial purpose with attribution).

Disclaimer by author: You must attribute the author if you use this image on a website or app (e.g., "Icons made by Freepik from Flaticon").

Defense Rocket Sprite (Projectile)

Asset Name: Rocket at take off vector clip art

Source: FreeSVG (https://freesvg.org/rocket-at-take-off-vector-clip-art)

License/Disclaimer: Public Domain (CC0). Free to use in personal and commercial projects. No attribution required; modification is allowed.

Emergency Light Animation (UI Alert)

Asset Name: Flashing Red Emergency Light (Thumbnail Preview)

Source: Shutterstock (https://www.shutterstock.com/shutterstock/videos/3905048149/thumb/8.jpg?ip=x480)

License/Disclaimer: Educational Fair Use / Shutterstock Standard License. Preview asset utilized strictly for non-commercial, academic demonstration purposes.

Water Surface Textures (Background)

Asset name: Seamless Blue Water Texture / Liquid Surface

Likely Source: https://craftpix.net/freebies/free-seaport-tileset-32x32-pixel-art-for-platformer/

Disclaimer by author: You can use each product in unlimited number of free and commercial projects.

Masters Program in **Geospatial Technologies**

Supported by:
Education and Culture
ERASMUS MUNDUS