

DIGITAL-ECCC-2022-CYBER-B-03-
CYBER-RESILIENCE



This project has received funding from the European Union's DIGITAL-ECCC-2022-CYBER-B-03-CYBER-RESILIENCE programme under grant agreement No 101145872.

Connected 5G-IoT Cyber Range for Training and Secure Operations



WP2 – Requirements Analysis and Architecture Definition

Deliverable D2.2 “NITRO Cyber Range Architecture, Testing and Validation Plans”

Editor(s):	IURC
Author(s):	Christos Xenakis (UPRC), Nikitas Marinos Sgouros (UPRC), George Eftymoglou (UPRC), Tsitsoula Styliani(HCSI), Antony Vamvakaris (HCSI), George Mylonas (HCSI), Christoforos Ntantogian (IURC), Emmanouil Magkos (IURC), Stylianos Karagiannis (IURC), Konstantinos Oikonomou (IURC), Markos Avlonitis (IURC) Anastasios Tzoumpas (UBI), Konstantinos Poulakakis (UBI), Ioannis Siachos (UBI), Kantikyan Araksya (UNILU)
Dissemination Level:	PU - Public
Type:	R — Document, report
Version:	1

Project Profile

Contract Number	101145872
Acronym	NITRO
Title	Connected 5G-IoT Cyber Range for Training and Secure Operations
Start Date	Jan 1 st , 2024
Duration	36 Months

Partners

1		UNIVERSITY OF PIRAEUS	University of Piraeus Research Center	Greece
2			UNISYSTEMS LUXEMBOURG SARL	Luxembourg
2.1			UNI SYSTEMS SYSTIMATA PLIROFORIKIS MONOPROSOPI ANONYMI EMPORIKI ETAIRIA	Greece
3			IONIAN UNIVERSITY	Greece
4		HCSI HELLENIC CYBERSECURITY INSTITUTE	HELLENIC CYBERSECURITY INSTITUTE	Greece
5			UBITECH LIMITED	Cyprus

Document History

VERSIONS

Table 1: Document history

Version	Date	Author	Remarks
0.1	16/10/2024	IURC	Initial ToC
0.2	23/10/2024	IURC	Updated ToC
0.3	20/10/2024	IURC	Initial Input
0.4	30/10/2024	IURC	Final ToC and assignments after partners' review and discussions
0.5	01/11/2024	IURC/UPRC	Updated section 2 and section 3
0.6	06/11/2024	UBI/IURC	Updated section 4 and section 5
0.7	07/11/2024	UPRC	Revised version
0.8	11/11/2024	IURC/UBI	Revised version
0.9	12/11/2024	IURC	Revised version
1	12/31/2024	IURC	Final version

Table of Contents

Table of Figures	6
Table of Tables	7
Table of Abbreviations	8
Executive Summary	9
1 Introduction	10
1.1 Overview of NITRO Cyber Range	11
1.2 Objectives Connected to the Architecture.....	11
1.3 Scope of the Document.....	13
1.4 Connection with other Deliverables	13
1.5 Document Structure.....	14
2 System Overview	14
2.1 5G Core and Deployment.....	16
2.2 Explanation of the NITRO Interfaces.....	17
2.3 Cybersecurity Education Modules	21
2.4 Network, Attack Simulation, Security and Privacy Modules	22
2.5 Monitoring and Evaluation	22
2.6 Workflow	23
2.7 Example Scenario: Simulating a DDoS Attack on a 5G Network.....	23
3 Technical Architecture	24
3.1 Reference Architecture.....	24
3.2 User and Control Planes	26
3.3 Components in Details	27
3.4 5G Core Network (5GC)	30
3.5 Management and Monitoring	32
3.6 Database for Storing 5G User Profiles	32
3.7 5G Radio Access Network and User Equipment (UERANSIM).....	32
3.8 Data Flows and Interactions of the 5G Core	33
3.9 NITRO Architecture Capability Blocks and Validation	35
4 Stakeholders and User Roles	39
4.1 First Trainee Group (Tier 1): Beginners.....	42
4.2 Second Trainee Group (Tier 2): Intermediate.....	43
4.3 Third Trainee Group (Tier 3): Advanced	44
4.4 Discussion on the Capabilities of the Architecture	45
5 Scalability Considerations and Integration Capabilities.....	45
5.1 Resource Allocation and Core Component Scaling	46
5.2 Isolation and Resource Partitioning for Multiple Trainees.....	46
5.3 Integration Principles	47



5.4	Distributed Deployment.....	49
5.5	Network Throughput and Latency Constraints.....	50
5.6	Database Scalability and Subscriber Management.....	50
5.7	Cybersecurity Mechanisms.....	51
6	Conclusion	51
7	References	52

Table of Figures

Figure 1. The NITRO Architecture	15
Figure 2. Explanation of the NITRO Interfaces.....	17
Figure 3. Interaction of the UERANSIM with the NITRO Platform.....	20
Figure 4. Interaction between the UE, 5G Radio Access Network, 5G Core and the Education Platform	24
Figure 5. Interaction between the Control Plane and User Plane	27
Figure 6. Details on the IMSI Structure and the Subscription to 5G Core Using the AAA Server	29
Figure 7. The 5G Core Architecture and Internal Data Flows	31
Figure 8. 5G Core Internal Network Data Flows	33
Figure 9. Trainee Groups.....	42
Figure 10. Scalability Considerations for the NITRO 5G Cyber Range	46
Figure 11. Scalability Considerations: Isolation and Resource Partitioning.....	47



Table of Tables

Table 1: Document history.....	3
Table 2. Connection of Main Objectives to the Architecture	12
Table 3. The NITRO Interfaces	16
Table 4. Main Components of the 5G and Short Explanation	28
Table 5. Integration and Validation Milestones.....	35
Table 6. NITRO 5G Cyber Range Capabilities	39
Table 7. Main Stakeholders.....	40
Table 8. Integration Principles to be Considered.....	48
Table 9. List of Cybersecurity Mechanisms to be Integrated on the NITRO 5G Cyber Range	51

Table of Abbreviations

Abbreviation	Explanation
5G	5th Generation
5GC	5G Core
6G	6th Generation
AAA Server	Authentication, Authorization, and Accounting (AAA) Server
AI	Artificial Intelligence
APTs	Advanced Persistent Threats
C&C	Command and Control
CLI	Command Line Interface
CU	Centralised Unit
DDoS	Distributed Denial of Service
DPIA	Data Protection Impact Assessment
DPO	Data Protection Officer
ENISA	European Union Agency for Cybersecurity
ES	Engineering Story
EU	European Union
EUCC	European Cybersecurity Certification Scheme
FAIR	Findable, Accessible, Interoperable, and Reusable
GANs	Generative Adversarial Networks
GDPR	General Data Protection Regulation
ICS	Industrial Control Systems
IDS	Intrusion Detection Systems
IMSI	International Mobile Subscriber Identity
IOC	Indicators Of Compromise
IoT	Internet of Things
IPS	Intrusion Prevention Systems
LMS	Learning Management Systems
MANO	Management and Network Orchestration
MCC	Mobile Country Code
MitM	Man-in-the-Middle
ML	Machine Learning
MNC	Mobile Network Code
MVP	Minimum Viable Product
NFV	Network Function Virtualization
NFVO	NFV Orchestration
NWDAF	Network Data Analytics Function
OSM	Open Source MANO
PII	Personally Identifiable Information
QoS	Quality of Service

RAN	Radio Access Network
RCE	Remote Code Execution
ROs	Research Objectives
SDN	Software-Defined Networking
SIEM	Security Information and Event Management
SOC	Security Operations Centre
TTPs	Tactics, Techniques, and Procedures
VNFs	Virtual Network Functions
AMF	Access and Mobility Management Function
AUSF	Authentication Server Function
UDM	Unified Data Management
UE	User Equipment
UDR	Unified Data Repository
SMF	Session Management Function
PCF	Policy Control Function
UPF	User Plane Function
BSF	Binding Support Function
SCP	Service Communication Proxy

Executive Summary

The D2.2 deliverable provides a comprehensive overview of the design and implementation of the NITRO Cyber Range, a cutting-edge training platform tailored for cybersecurity professionals. This document outlines the architecture of the NITRO system, emphasizing its modular structure and integration of advanced technologies to create a realistic 5G network emulation environment. By leveraging tools such as Docker containers and open-source software, NITRO offers a scalable and flexible platform that simulates real-world cyberattack scenarios, enhancing the training experience for participants.

1 Introduction

Deliverable D2.2 focuses on defining the architectural framework of the NITRO Cyber Range, alongside comprehensive testing and validation plans to ensure its effectiveness and reliability. The architecture is designed to integrate with simulated 5G infrastructure while providing the flexibility to simulate various cyber threat scenarios relevant to IoT and 5G environments [1]. It encompasses the system's architecture, its interaction with existing 5G networks, and the integration of IoT devices, illustrating the innovative nature of the NITRO platform.

- **Description of NITRO Cyber Range System:** The core functionalities and objectives of the NITRO Cyber Range are presented, highlighting how it simulates real-world cyber threat scenarios to train personnel and organizations in effective defense strategies. It encompasses the system's architecture, its interaction with existing 5G networks, and the integration of IoT devices, illustrating the innovative nature of the NITRO platform.
- **Key Concepts and Terminology:** A clear understanding of the terminology and concepts relevant to the NITRO Cyber Range is essential for stakeholders. This section defines key terms, ensuring that all participants share a common language and understanding of the system's functionalities, components, and operational paradigms.
- **Technical Architecture of the NITRO Cyber Range:** The technical architecture is fundamental to the functionality and scalability of the NITRO Cyber Range. It encompasses the design principles, components, and data flows that facilitate effective training and response to cyber threats.
- **Architecture Overview:** Presents a high-level overview of the NITRO Cyber Range architecture, illustrating its modular structure and the interplay between various components. It establishes the foundation for understanding how the system is organized to support training activities.
- **Logical Architecture:** The logical architecture delves into the abstract framework of the NITRO Cyber Range, outlining the relationships and interactions between different system elements. This section focuses on how various functions are integrated logically, supporting the overall operational objectives of the platform.
- **Logical Components:** The specific components that comprise the NITRO Cyber Range are detailed. Each component's role is clarified, highlighting its functionality and significance in the overall architecture, thus providing insights into how these components work together to facilitate effective training.
- **Data Flows and Interactions:** Understanding data flows and interactions is crucial for effective system operation. This section describes how data moves through the NITRO Cyber Range, detailing the communication pathways between components and ensuring that information is exchanged efficiently to support training scenarios.

- **Scalability Considerations:** As organizations grow and the complexity of cyber threats evolves, scalability becomes essential. This section discusses strategies for scaling the NITRO Cyber Range, ensuring that it can accommodate an increasing number of users, devices, and training scenarios without compromising performance.
- **Cybersecurity Mechanisms:** This section outlines the various cybersecurity mechanisms integrated into the NITRO Cyber Range. It details how these mechanisms protect the system from potential threats while facilitating realistic training environments where users can practice their incident response skills.
- **Integration Principles:** This section presents the principles guiding the integration of the NITRO Cyber Range with existing infrastructure and systems. It highlights the importance of interoperability and compatibility with 5G networks and IoT devices, ensuring that the cyber range can function effectively within diverse environments.

1.1 Overview of NITRO Cyber Range

The NITRO Cyber Range is an innovative platform designed to simulate and analyze cybersecurity challenges within 5G and Internet of Things (IoT) environments. It provides a controlled environment for researchers, engineers, and security professionals to conduct training, testing, and validation of security measures against a variety of cyber threats. The architecture of the NITRO Cyber Range integrates seamlessly with existing 5G infrastructure, allowing for realistic emulation of network conditions and cyberattack scenarios.

At its core, the NITRO Cyber Range aims to enhance the understanding of vulnerabilities within interconnected 5G and IoT systems. By emulating real-world scenarios, it allows users to assess the security posture of these systems, identify potential weaknesses, and develop effective countermeasures. The platform supports the simulation of various 5G network architectures, IoT device configurations, and communication protocols, facilitating in-depth analysis of diverse attack vectors.

One of the distinguishing features of the NITRO Cyber Range is its focus on adversarial AI, enabling the examination of attacks targeting artificial intelligence models deployed in 5G and IoT networks. This pioneering approach not only increases awareness of the risks associated with adversarial AI but also contributes to the development of more robust and secure AI systems.

1.2 Objectives Connected to the Architecture

The NITRO Cyber Range aims to enhance the security of 5G and IoT networks by providing a specialized environment for testing, training, and research. NITRO seeks to enhance the preparedness of cybersecurity professionals through a robust training environment. This environment will offer a range of high-stress, real-world scenarios that allow individuals, including staff in security operation centers and penetration testers, to test security technologies and methodologies. By providing hands-on

experience, NITRO will help participants develop the skills needed to detect, block, and mitigate emerging cyberattacks effectively. The cybersecurity platform features a virtualized 5G-IoT cyber range [15]. This platform will integrate existing testbeds for both 5G and IoT systems, creating a comprehensive training environment that allows cybersecurity professionals to study, practice, and develop the skills necessary to secure these interconnected technologies.

Objective	Description	Connection to Architecture
Enhance 5G and IoT Security through Testing and Training	The NITRO Cyber Range aims to improve security for 5G and IoT networks by providing a specialized environment for testing, training, and research in real-world scenarios. This robust training setting is designed for cybersecurity professionals, SOC staff, and penetration testers to test and develop effective security responses.	Virtualized 5G-IoT cyber range, incorporating real-world simulation capabilities within a modular design for adaptability.
Provide Training through Real-World Scenarios	Through high-stress simulations, NITRO enables participants to experience realistic threat scenarios and practice skills necessary for detecting, blocking, and mitigating cyberattacks.	Architecture is designed to support scenario-based training modules, data flows, and interfaces that replicate realistic attack vectors.
Integrate Existing 5G and IoT Testbeds into a Unified Platform	By unifying testbeds, NITRO creates a comprehensive environment allowing professionals to train with interconnected technologies, gaining insight into the complexities of securing 5G-IoT networks.	Modular architecture supports the integration of existing testbeds and data flows, fostering interoperability between 5G and IoT setups.
Create Central Threat Repository for 5G and IoT	NITRO will develop a common repository for attacks, threat analyses, and scenarios using open standards for interoperability. This repository will serve as a resource for data-driven threat analysis and as a knowledge base for training and research.	Logical and data architecture includes a centralized database framework designed for interoperability, supporting threat data collection and sharing.
Simulate Attack Vectors Exploiting Device Interdependencies	NITRO will simulate and analyze attack vectors that exploit interdependencies within 5G-IoT networks to uncover potential vulnerabilities and pathways for systemic failures.	Logical and technical architecture provides an adaptable framework for simulating various attack paths and assessing inter-device vulnerabilities.

Table 2. Connection of Main Objectives to the Architecture

Furthermore, a key objective is to create a common data repository that will serve as a centralized resource for attacks, threat analyses, and scenarios related to 5G and IoT networks. This repository will utilize open standards for interoperability and facilitates effective knowledge transfer and enables big data analytics. By making this information accessible, NITRO aims to foster a better understanding of the threat landscape and support ongoing research in cybersecurity.

Finally, NITRO aims to identify and simulate attack vectors that exploit interdependencies between devices in interconnected 5G and IoT networks. By investigating these vulnerabilities [8], the project seeks to uncover potential pathways for widespread system failures, thereby providing valuable

insights for improving the overall security posture of these critical infrastructures.

1.3 Scope of the Document

The primary objective of deliverable D2.2 is to establish a comprehensive architecture for the NITRO Cyber Range that includes detailed specifications of its components, interfaces, and data flows. This architecture will serve as the foundation for creating a realistic and effective simulation environment tailored to the complexities of 5G and IoT networks. Additionally, the deliverable aims to develop validation plans that set the criteria for confirming that the cyber range operates according to its intended specifications. This involves a systematic approach to validate that the simulations accurately reflect real-world conditions, thus providing meaningful training experiences.

Furthermore, a main objective of this deliverable is to provide details regarding the interactions between the NITRO Cyber Range and current 5G networks. This includes specifying how the system will interface with various network functions and IoT devices, thereby demonstrating the innovative capabilities of the NITRO platform. This includes also the creation of validation plans that outline criteria for confirming that the cyber range meets its intended specifications. This will involve a systematic approach to ensure that the simulations accurately reflect real-world conditions, providing users with meaningful and relevant training experiences.

Another important aspect of this deliverable is to provide a comprehensive description of the NITRO Cyber Range architecture. This encompasses the integration of various elements, including 5G core networks, radio access networks (RAN), and IoT devices. The document aims to illustrate how these components work synergistically to create a cohesive platform tailored for cybersecurity training and testing. By establishing a clear architectural framework, the NITRO Cyber Range sets the foundation for effective simulations and assessments of cybersecurity measures within modern network environments.

Finally, a key objective is to outline the capabilities of the NITRO Cyber Range in simulating a wide array of cyber threat scenarios. This includes the emulation of cyberattacks and vulnerabilities specific to 5G and IoT environments. By emphasizing realistic threat emulation, the NITRO Cyber Range aims to enhance the effectiveness of training and assessment exercises. This objective underscores the importance of preparing security professionals to face real-world challenges [9] by providing them with a platform to experience and respond to various cyber threats in a controlled setting.

1.4 Connection with other Deliverables

The current deliverable D2.2 is directly connected with following technical deliverables:

- **D2.1 – Technical, legal, policy requirements and use case scenarios - first version:** D2.2 will describe the architecture on top of the functional and non-functional requirements defined in D2.1.
- **D2.3 – Technical, legal, policy requirements and use case scenarios – second version:** The

new function and non-function requirements will be refined according to the architecture, data flows, and interfaces defined in the D2.2.

- **D2.4 – NITRO cyber range architecture, testing and validation plans – second version:** The final NITRO architecture in D2.4 will be built on top of the initial one provided in D2.2.
- **D3.1 – NITRO security training exercises design and development - first version:** The D3.1 will describe, analyze and implement the NITRO exercises covering several aspects of 5G-IoT security together with their accompanying manuals and guidelines on top of the architecture designed in D2.2.
- **D3.2 – NITRO data repository for threats and incidents:** The implementation of the data repository will be according to the architecture and data flow of the D2.2.
- **D4.1 NITRO scoring and gamification system - first version:** The initial design of the NITRO scoring methodology and the gamification solution will be based on the architecture defined in D2.2.

1.5 Document Structure

The remainder of this deliverable is structured as follows: Section 2 provides a comprehensive overview of the NITRO 5G Cyber Range, including the system architecture, essential concepts, and key terminology, alongside an outline of stakeholder roles and responsibilities to clarify platform engagement. Section 3 dives into the technical architecture, detailing 5G core components, data flows, and interactions, and examines scalability considerations to ensure the platform's robustness. Additionally, this section addresses the cybersecurity mechanisms designed to protect both platform integrity and simulated training environments, as well as principles for seamless system integration to enhance compatibility and interoperability. Finally, Section 4 concludes the deliverable.

2 System Overview

By providing a controlled environment, the platform allows trainees to gain hands-on experience in identifying, mitigating, and responding to cyber threats within a 5G network. The architecture (Figure 1) is composed of several interconnected modules that work in unison to simulate both defensive and offensive cybersecurity scenarios. In Figure 1 a detailed breakdown is presented of the architecture and its components (Table 3).

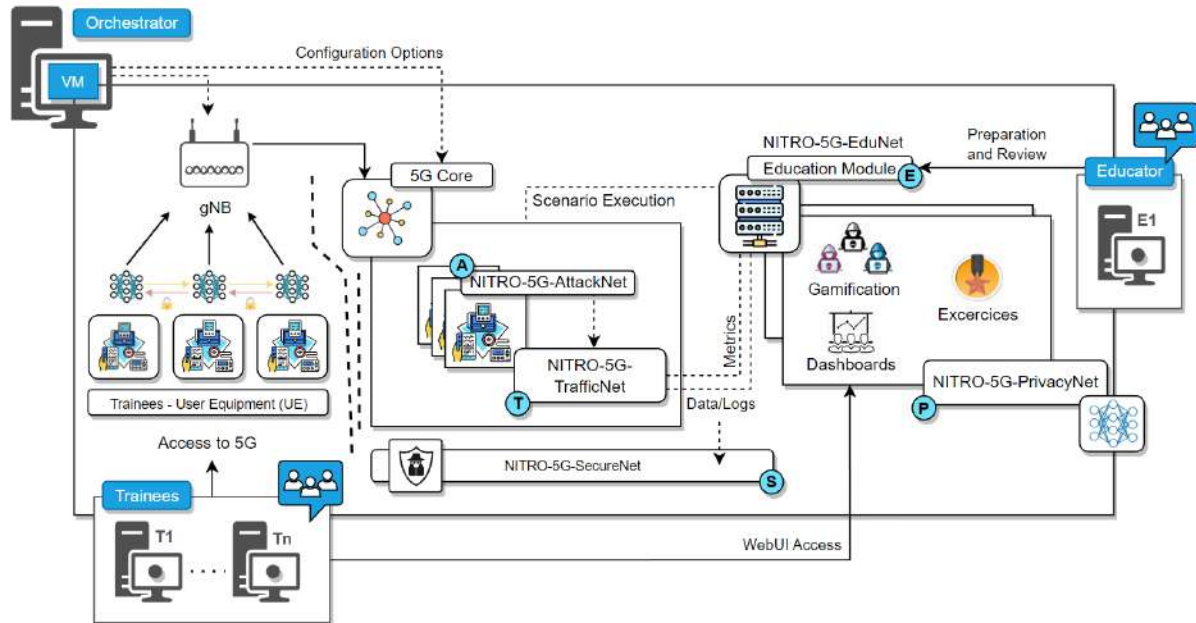


Figure 1. The NITRO Architecture

Interface	Description	Connection to Other Components
NITRO-5G-001-Orchestrator/Virtualization	Central management unit for the platform. Configures training scenarios, allocates resources, and coordinates experiments. It ensures smooth deployment and execution.	Connects with all layers to manage the allocation of resources, scenario deployment, and network coordination.
NITRO-5G-002-gNB (Next Generation Node B)	Simulates the 5G base station, providing connectivity between user equipment (UE) and the 5G core network. Handles radio access, handovers, and communication.	Interacts with the 5G Core, EduNet, and CoreNet for network connectivity, user interactions, and traffic simulation.
5G Core	Backbone of the 5G network, handling functions such as authentication, mobility management, and data routing.	Connected with CoreNet, AttackNet, TrafficNet, SecureNet, and gNB for managing core network operations and supporting network security.
NITRO-5G-003-CoreNet	Emulates 5G core functions like session and mobility management. Integrates with Open5GS to simulate realistic 5G environments.	Connects directly with the 5G Core, gNB, and other layers for simulating real-world network behavior, mobility, and session continuity.
NITRO-5G-004-AttackNet	Manages the injection of simulated threats like DDoS, fuzzing, and spoofing attacks. Enables testing of network resilience and security.	Connects with all components, especially the 5G Core, SecureNet, and CoreNet, to simulate attacks and their effects on the network.
NITRO-5G-005-TrafficNet	Controls data flow across network slices, simulating traffic patterns to replicate real-world 5G network conditions.	Interacts with the 5G Core, CoreNet, and EduNet to simulate traffic, prioritize slices, and analyze the impact

		on network performance.
NITRO-5G-006-EduNet	Facilitates user interaction and logs activity for training assessments. Provides a smooth, interactive experience during training.	Connects with all layers to monitor user activity, performance, and engagement within various network scenarios.
NITRO-5G-007-PrivacyNet	Ensures data privacy by anonymizing user data and enforcing compliance with privacy regulations like GDPR.	Works with all components, particularly EduNet and SecureNet, to ensure that data privacy is maintained across all interactions and simulations.
NITRO-5G-008-SecureNet	Focuses on enforcing security policies, detecting threats, automating responses, and ensuring data security across the network.	Connected to the 5G Core, CoreNet, AttackNet, TrafficNet, and EduNet to provide security measures, detect anomalies, and protect data integrity.

Table 3. The NITRO Interfaces

2.1 5G Core and Deployment

The core infrastructure of the NITRO 5G Cyber Range is the foundational layer that supports the simulation of a 5G network environment. This infrastructure encompasses the critical components necessary for creating a functional 5G network and enabling realistic cybersecurity training.

Orchestrator (VM): The Orchestrator acts as the central management unit for the entire platform. It is responsible for configuring training scenarios, allocating resources, and coordinating experiments. It enables the platform to run a variety of scenarios by managing the deployment of network resources and ensuring that each training exercise runs smoothly. The orchestrator's role is pivotal in ensuring that the right resources are available at the right time to facilitate seamless operations.

gNB (Next Generation Node B): gNB¹ is a crucial element in the NITRO 5G architecture, simulating the 5G base station [2]. It provides the link between the user equipment (UE) and the 5G core network, supporting essential functions like radio access, handovers, and communication between devices [3]. It mimics the operation of a real 5G base station, ensuring that trainees can experience the dynamics of base station management and network connectivity under various attack conditions.

5G Core: The 5G core is the backbone of the 5G network, responsible for handling critical network functions such as authentication, mobility management, service orchestration, and data routing [4]. It simulates the internal workings of a 5G network and acts as the central control unit for network traffic, security policies, and overall system behavior. In the cyber range, the 5G core plays a key role in simulating how attacks can impact core network functions, providing insights into network

¹ https://www.etsi.org/deliver/etsi_ts/138400_138499/138401/15.02.00_60/ts_138401v150200p.pdf

vulnerabilities and potential attack vectors.

2.2 Explanation of the NITRO Interfaces

The NITRO architecture is based on the interoperability across the 5G components. The architecture consists of multiple layers each dedicated to handling unique network tasks within the cyber range (Figure 2).

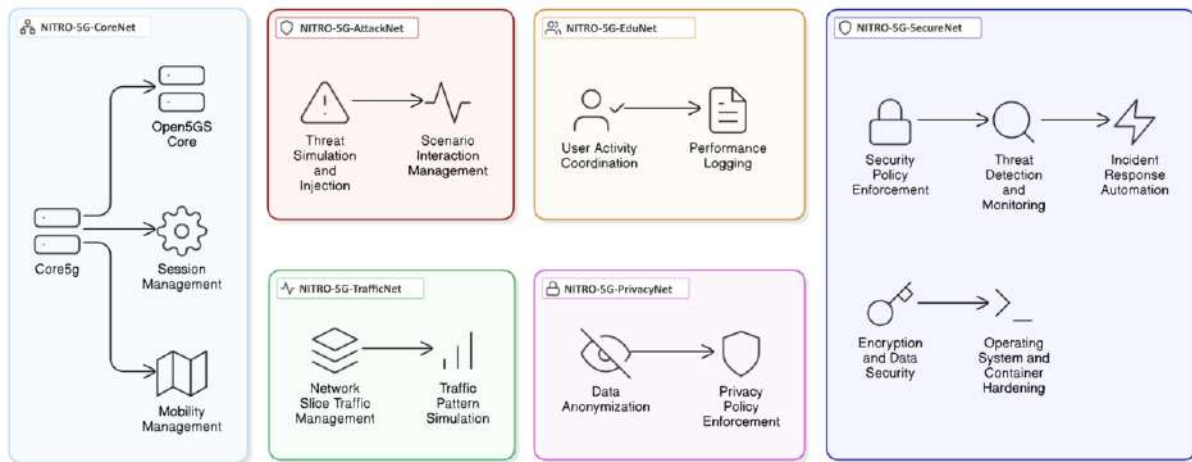


Figure 2. Explanation of the NITRO Interfaces

The layers are presented in Figure 2, namely CoreNet, AttackNet, TrafficNet, EduNet, PrivacyNet, SecureNet and are logical representations of the main functionalities and cyber range components which are responsible among others to manage the core network emulation, enable threat and attack simulations, traffic simulations, user interactions, and ensure data privacy.

NITRO-5G-CoreNet: Core5g is responsible for emulating core 5G network functions, specifically focusing on session and mobility management. It interfaces directly with the Open5GS² core to create realistic 5G environments, allowing users to experience network behavior similar to live 5G infrastructures [5]. Through this layer, the platform can manage crucial 5G core functionalities such as:

- **Session Management:** Establishing, maintaining, and terminating user sessions as users move through different network segments. It simulates how the 5G network would handle session continuity and quality across diverse scenarios.
- **Mobility Management:** Ensuring smooth transitions for users as they move between network

² <https://open5gs.org/>

cells or slices. By mimicking handovers and connectivity adjustments, CoreNet gives users insights into how mobility impacts connectivity and data flow in real-world 5G networks.

NITRO-5G-AttackNet: Designed for the controlled injection of simulated threats into the 5G training environment, enabling robust testing of network resilience and security defenses. This serves as the main interface for threat emulation, supporting a wide array of attack scenarios that target vulnerabilities specific to 5G architectures [5]. Key functionalities include:

- **Threat Simulation and Injection:** Injects various types of threats, such as Distributed Denial of Service (DDoS) attacks, protocol fuzzing, and spoofing attacks, allowing trainees to experience and respond to diverse cyber threats in a safe, controlled environment.
- **Scenario Interaction Management:** By coordinating the timing, intensity, and spread of these threats, Attack5G aligns security incidents with training objectives, offering a realistic context for participants to practice detection, mitigation, and recovery.

NITRO-5G-TrafficNet: Responsible for controlling and managing data flow across network slices, simulating realistic 5G traffic patterns to emulate user behavior and network load. This replicates traffic conditions seen in high-demand networks, helping trainees to understand the effects of different traffic loads on network performance and security [26]. Main functions include:

- **Network Slice Traffic Management:** Distributes traffic across various network slices, enabling trainees to see how network slicing can be used to allocate resources based on priority or user type.
- **Traffic Pattern Simulation:** Generates both typical and high-stress traffic patterns, such as peak-hour usage or sudden traffic spikes, simulating user behavior and device interactions in a real-world setting.

NITRO-5G-EduNet: Facilitates interaction between users and the NITRO platform, capturing user activity and maintaining logs to support real-time assessments and post-training evaluations. This is key to providing a smooth, interactive experience within training sessions and enables trainers to monitor and evaluate user performance comprehensively. Its main functions include:

- **User Activity Coordination:** Manages and logs user actions within training modules, offering trainer insights into individual and group responses during various scenarios.
- **Performance Logging:** By recording detailed logs of user interactions, EduNet enables trainers to assess participant skills, reaction times, and decision-making processes under pressure.

NITRO-5G-PrivacyNet: Dedicated to enforcing data privacy policies within the NITRO training environment, ensuring that all user data and interactions remain confidential and that training simulations adhere to data protection standards [22]. PrivacyNet is particularly important in scenarios

where data from real users may be introduced, as it ensures the responsible handling of personal information [13]. Key functionalities include:

- **Data Anonymization:** Anonymizes all user data collected during training exercises, removing personally identifiable information to protect participant privacy.
- **Privacy Policy Enforcement:** Ensures that all interactions within the NITRO environment comply with relevant privacy regulations, such as GDPR, safeguarding user data at each stage of the training process.

NITRO-5G-SecureNet: Focus on cybersecurity measures across the 5G Cyber Range environment. This layer focuses on establishing, maintaining, and reinforcing security protocols, as well as monitoring network activity for signs of threats or breaches. By providing advanced tools for security policy enforcement and continuous threat monitoring, SecureNet helps simulate real-world security defenses, offering trainees a practical experience in identifying and mitigating cyber threats within a 5G network. The SecureNet has the following functionalities:

- **Security Policy Enforcement:** Acts as the central control point for implementing security policies across all 5G network slices within the NITRO platform. These policies can include firewall rules, access controls, and encryption requirements, providing an essential layer of defense that mirrors enterprise-grade security measures.
- **Threat Detection and Monitoring:** A core aspect of the SecureNet is its continuous monitoring capabilities, which track network activity and detect unusual patterns indicative of potential cyber threats. SecureNet leverages both signature-based and anomaly-based detection techniques, enabling it to identify known attack vectors as well as emerging, less predictable threats.
- **Incident Response Automation:** Includes an Incident Response Automation module that streamlines reactions to detected threats, reducing the time to contain and mitigate security incidents. By simulating automated response protocols, SecureNet provides a realistic view of modern cybersecurity operations where rapid response is critical.
- **Encryption and Data Security:** Provides tools for enforcing encryption on data-in-transit across the 5G network slices, helping to simulate a high level of data security as seen in operational 5G environments. These tools allow trainees to configure encryption protocols.
- **Operating System and Container Hardening:** Reduces vulnerabilities, primarily by disabling unnecessary services, enforcing strict user permissions, and regularly updating software. Key steps include implementing network firewalls, file system protections, and secure logging and auditing. Furthermore, it includes securing container environments by using minimal base images, managing permissions carefully, and employing isolation techniques (e.g. AppArmor or SELinux). Finally, it can include privilege restrictions, scanning images for vulnerabilities, and managing secrets securely.

At its core, the system is built around an emulated 5G network, leveraging Open5GS for core network functions and UERANSIM [6, 7], for simulating user equipment and radio access networks (Figure 3). This emulation creates a realistic environment where trainees can explore the complexities of 5G communications, protocols, and vulnerabilities. Coupled with this is the use of Docker images, which package the necessary applications and services into isolated containers, allowing for rapid deployment and consistency across different training modules. This automation reduces the administrative burden on instructors and allows trainees to focus on engaging with the material.

Data repositories and dashboards play a critical role in the system by providing trainees with insights into their performance and the operational state of the network. The dashboards offer real-time visibility into system metrics, enabling trainees to analyze the effectiveness of their actions and make data-driven decisions during exercises. Meanwhile, the data repository stores logs and historical data for post-exercise analysis, fostering a continuous learning environment.

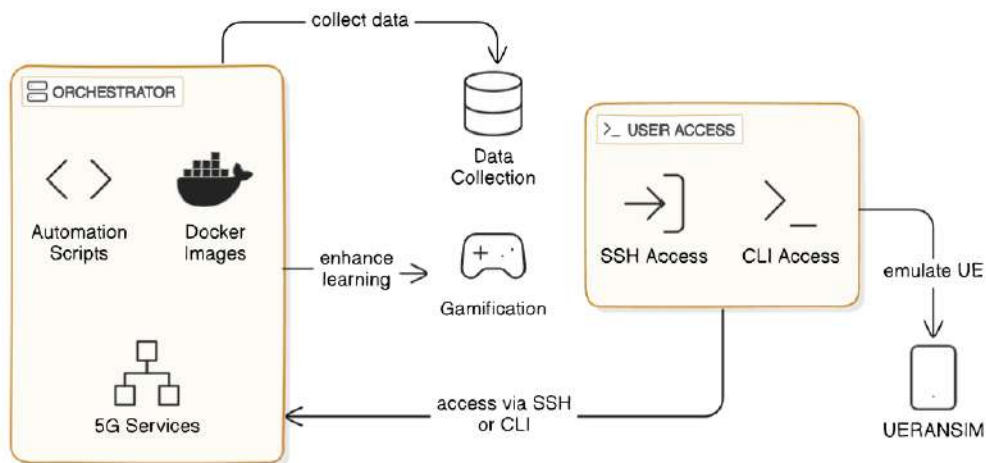


Figure 3. Interaction of the UERANSIM with the NITRO Platform

The Orchestrator (Figure 3) acts as the central control unit that manages all aspects of the training environment. Residing on a dedicated Virtual Machine (VM), the Orchestrator ensures seamless operation by automating various processes through Automation Scripts. This centralized management allows for the efficient deployment, configuration, and orchestration of multiple training modules and components.

The Orchestrator leverages **Docker Images** and **5G Services**. Docker Images package various applications and 5G services needed for the training exercises into portable containers, ensuring consistency and ease of deployment across different environments. By utilizing 5G Services, the platform emulates the core functionalities of a 5G network, including User Equipment (UE) interactions, mobility management, and session management. This emulation provides trainees with a safe and controlled space to experience real-world scenarios without the risks associated with live

networks.

Throughout the training process, the platform collects relevant data, indicated by collecting data. This continuous data collection is essential for monitoring trainee progress and performance. Participants access the NITRO platform using SSH or Linux Command Line Interface (CLI) and UERANSIM as an emulation for the UE. The training exercises are designed to be engaging and interactive, incorporating elements of Gamification to enhance the learning experience. Trainees are not only challenged by cyberattack simulations but also rewarded for their achievements and progress, fostering a competitive yet collaborative learning environment.

The integration of 5G technologies with Cyber Ranges provides a powerful platform for enhancing security training and preparedness in industrial and IoT environments. By utilizing Digital Twins [28], the architecture and deployment can ensure the simulation of 5G networks, enabling immersive and realistic training for security professionals to address potential vulnerabilities and attacks [18]. The rise of IoT devices introduces significant security challenges, making advanced training environments essential for evaluating and implementing effective countermeasures [19]. Additionally, AI-driven strategies enable these Cyber Ranges to operate dynamically, offering both offensive and defensive capabilities to address evolving threats in Beyond 5G networks [20]. These advancements also incorporate privacy-preserving measures, ensuring ethical and secure data handling in high-stakes training scenarios [21].

2.3 Cybersecurity Education Modules

The NITRO 5G Cyber Range is designed to support various types of training, from basic awareness to advanced attack and defense exercises. The training environment consists of multiple modules that provide educational content, real-time feedback, and performance evaluations.

NITRO-5G-EduNet (Education Module): This module provides educational resources and training exercises tailored to cybersecurity in 5G networks. It incorporates gamification features to enhance engagement, making the learning process interactive and dynamic. The EduNet module enables trainees to learn through a combination of theoretical knowledge and practical scenarios, ensuring a comprehensive understanding of 5G security.

Preparation and Review: Educators use this feature to design, configure, and review training scenarios. It allows instructors to create tailored exercises and refine them based on past experiences. Trainee performance can be assessed, and feedback can be provided to improve the learning process.

Educator: This represents the instructor's role in the platform. Educators are responsible for creating training sessions, managing the flow of the exercises, and monitoring the progress of trainees. They interact with the platform to ensure that the objectives of the training are met and provide guidance based on real-time results.

Trainees - User Equipment (UE): The UE represents the devices that trainees use to connect to the

simulated 5G network. These devices could be smartphones, laptops, or any other mobile device that communicates over the network. Trainees use these devices to engage with the network and perform various actions that will help them understand 5G network vulnerabilities and security procedures.

Trainees: Trainees are the individuals participating in the cyber range training. They engage with the platform, use the devices, and interact with different attack and defense scenarios. Their goal is to enhance their cybersecurity skills through practical exercises that simulate real-world security incidents in 5G environments.

2.4 Network, Attack Simulation, Security and Privacy Modules

The NITRO 5G Cyber Range offers several specialized modules that simulate different aspects of 5G network traffic and security. These modules provide in-depth analysis and hands-on experience in dealing with network anomalies, attack scenarios, and defensive measures.

NITRO-5G-AttackNet: This module hosts a comprehensive library of pre-built attack scenarios and tools designed to simulate real-world cyberattacks on 5G networks. Trainees can launch attacks such as DDoS, man-in-the-middle, or authentication bypass, providing them with hands-on experience in both offensive and defensive tactics.

NITRO-5G-TrafficNet: TrafficNet generates realistic network traffic patterns, simulating both normal and malicious activities. This enables trainees to understand the complexities of network traffic in 5G environments, including the impact of various types of traffic on performance, security, and availability.

NITRO-5G-SecureNet: This secure environment is specifically designed to test and evaluate 5G security solutions. It provides an isolated space for trainees to deploy security defenses, such as firewalls, intrusion detection systems, and encryption mechanisms, to assess their effectiveness under attack conditions.

NITRO-5G-PrivacyNet: This module focuses on privacy-related aspects of 5G networks. It allows the simulation and analysis of privacy attacks, such as data leakage or unauthorized access to user information. It provides trainees with the opportunity to understand the privacy challenges specific to 5G technologies and develop solutions to mitigate these risks [16].

2.5 Monitoring and Evaluation

Monitoring and evaluation are crucial components of the NITRO 5G Cyber Range, as they provide the necessary tools for tracking performance, identifying vulnerabilities, and improving the overall training process.

Metrics: This feature collects various performance indicators, such as response time, throughput, and attack success rate, to assess the effectiveness of different training scenarios. These metrics are essential for understanding how well trainees are performing and whether the security measures are

effective.

Data/Logs: Logs of network activities, attack events, and user actions are stored for detailed post-scenario analysis. These logs serve as a valuable resource for both educators and trainees to identify areas of improvement and refine security strategies.

Dashboards: Dashboards provide visual representations of key metrics and offer real-time feedback on the network's behavior, attack progress, and trainee performance. They are designed to give both educators and trainees a quick overview of the situation, enabling faster decision-making.

WebUI Access: The WebUI provides a user-friendly interface that allows educators and trainees to interact with the platform, configure training scenarios, monitor progress, and analyze results. It acts as a central access point for managing the overall training environment.

2.6 Workflow

The workflow within the NITRO 5G Cyber Range follows a structured process designed to maximize training effectiveness.

- a) **Scenario Configuration:** Educators design training scenarios using the Orchestrator and EduNet modules. They configure network parameters, select attack vectors, and set up the necessary conditions for each exercise. This process ensures that the training aligns with specific learning objectives.
- b) **Scenario Execution:** Once the scenario is configured, trainees connect their devices to the simulated 5G network and engage in the training exercise. They experience various attack simulations, which test their skills in a realistic environment.
- c) **Monitoring and Analysis:** During the exercise, the platform continuously collects data, which is analyzed in real-time. Educators can use the collected information to provide immediate feedback, while trainees can adjust their strategies accordingly.
- d) **Evaluation and Review:** After the scenario is complete, educators assess the trainees' performance using the collected metrics and logs. Feedback is provided, focusing on areas for improvement and reinforcement of security best practices.

2.7 Example Scenario: Simulating a DDoS Attack on a 5G Network

In this example, trainees are tasked with defending a 5G network from a simulated Distributed Denial of Service (DDoS) attack. The Orchestrator configures the network to mimic a live 5G environment, with the gNB serving as the base station and the 5G Core managing network traffic.

The trainees' devices (UE) are connected to the simulated 5G network, and they are instructed to monitor traffic using the NITRO-5G-TrafficNet module. As the attack progresses, the trainees must identify the source of the malicious traffic and implement security measures (e.g., traffic filtering, rate

limiting) to mitigate the attack's impact. Meanwhile, the NITRO-5G-SecureNet module allows trainees to deploy additional security layers, such as firewalls and intrusion detection systems, to prevent further damage.

Real-time feedback is provided through the Dashboards and WebUI, which display attack progress and network performance. After the exercise, educators review the performance metrics and provide feedback on how effectively the trainees responded to the attack, highlighting areas for improvement in their approach.

3 Technical Architecture

This section includes the technical aspects of the architecture, including the facilitation of the core 5G operations, the integration of cybersecurity training elements, and the deployment of advanced network functions. The subsections provide information regarding the specific components, design principles, and operational workflows of the 5G Cyber Range as presented in Figure 4.

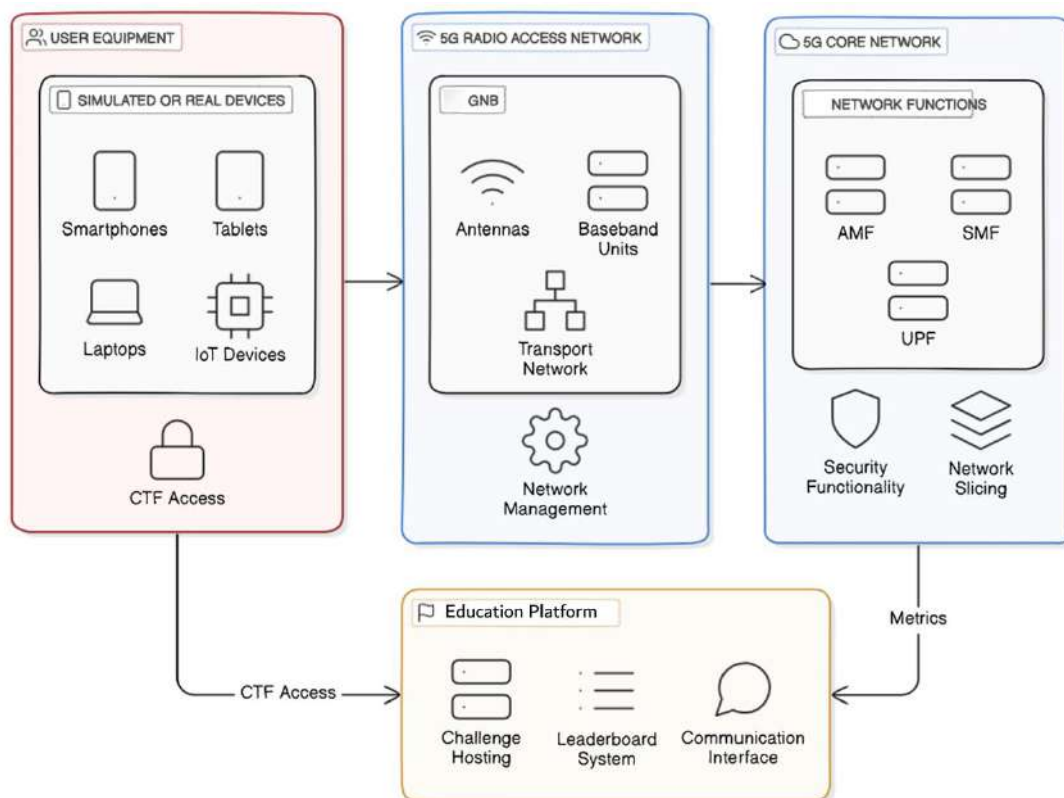


Figure 4. Interaction between the UE, 5G Radio Access Network, 5G Core and the Education Platform

3.1 Reference Architecture

The NITRO architecture is structured in a modular way to facilitate the deployment of essential

components of the 5G core, connect gNB and to host multiple UEs [14, 15]. The NITRO architecture utilizes a containerized approach, where each Core Network Function (CNF) is encapsulated within its own Docker container.

User Equipment (UE) is the entry point for users to interact with the cyber range and engage with CTF challenges. This component represents various devices, both virtualized and physical, including smartphones, tablets, laptops, and IoT devices. The flexibility of the platform allows it to incorporate simulated devices to create scalable environments for large groups, as well as real devices to provide an authentic user experience. These devices connect to the network through the 5G Radio Access Network, enabling participants to engage in cybersecurity exercises with devices that simulate real-world functionality. Access to the CTF platform is facilitated through these UEs, enabling users to solve challenges in a controlled yet realistic environment that mirrors real-world conditions.

The 5G Radio Access Network (RAN) simulates a real-world 5G radio environment, which is critical for training participants on network-specific cybersecurity issues. The RAN comprises the gNodeB (gNB), antennas, baseband units, and the transport network. The gNB acts as the 5G base station, managing radio transmission and reception to connect UEs to the network. Physical or simulated antennas enable the transmission and reception of radio signals between devices and the network. Baseband units process digital signals, managing user data traffic to ensure efficient communication. The RAN also includes a transport network that connects the gNB to the 5G Core Network, allowing for seamless data flow and high-speed connectivity between users and the core network. Additionally, a suite of network management tools is available to monitor and maintain network performance, enabling training administrators to ensure network integrity and adjust configurations as needed for specific exercises.

The **5G Core Network** represents the backbone of the cyber range, simulating essential 5G functionalities that are crucial for realistic training scenarios. It includes several key Network Functions that ensure seamless connectivity and user experience. The Access and Mobility Management Function (AMF) handles user access and mobility management, essential for training in scenarios where devices move between different network segments. The Session Management Function (SMF) establishes, modifies, and releases user sessions, a core part of data management in 5G networks. The User Plane Function (UPF) processes user data traffic, managing data routing and forwarding to enable participants to experience high-speed, low-latency connections during exercises. Security is paramount within the 5G Core Network, with dedicated functionality to protect data integrity and defend against threats. Network slicing capabilities enable the creation of multiple virtual networks over a single physical infrastructure, allowing for customized, isolated training environments for different use cases. This component also includes connection points to external networks, allowing for realistic interactions with the internet and other operator networks.

The **NITRO-5G-EduNet** is integrated within the NITRO 5G Cyber Range capable of hosting instructions and scenario information regarding the cybersecurity challenges designed maintain gamification

elements including scoreboard, leaderboard and the progress of the participants [23]. The leaderboard tracks the progress and ranking of participants, promoting a competitive atmosphere that encourages participants to enhance their skills and knowledge [25]. Furthermore, the communication interface is essential for fostering collaboration among participants, providing channels for communication between trainees and organizers [24], and enabling peer-to-peer learning. The platform is integrated with the 5G core network, allowing trainees to experience real-world constraints and network configurations while they work to complete challenges. This modularity allows for easy management, scaling, and isolation of each network component, which is critical for simulating various network scenarios and cyberattack exercises. Key features of the architecture include:

- **Modularity:** Components can be independently deployed and updated, allowing for incremental upgrades and easier maintenance.
- **Scalability:** The architecture can scale horizontally to accommodate varying loads, essential for supporting many devices and services.
- **Interoperability:** Open5GS is designed to work with other network components and systems, ensuring compatibility with existing infrastructures and third-party applications.

3.2 User and Control Planes

The logical architecture identifies key components and their roles in providing seamless connectivity and service delivery. The architecture is divided into two primary planes: **control plane** and **user plane**, each comprising specific functions that work together (Figure 5).

Control Plane: The control plane (Figure 5) manages signaling between the network and user equipment (UE). It handles subscriber data, session management, mobility, and authentication. Key components include:

- **AMF (Access and Mobility Management Function):** Manages UE registration, connection, mobility, and connection establishment for signaling.
- **SMF (Session Management Function):** Manages sessions, assigns IP addresses, and provides Quality of Service (QoS) control and session continuity.
- **AUSF (Authentication Server Function):** Authenticates subscribers, ensuring secure network access.
- **UDM (Unified Data Management):** Stores and manages subscriber data, policies, and profiles, supporting the AMF and SMF functions.
- **PCF (Policy Control Function):** Manages policy decisions for the network, including QoS management and charging.
- **NSSF (Network Slice Selection Function):** Allocates network slices to serve different user

requirements.

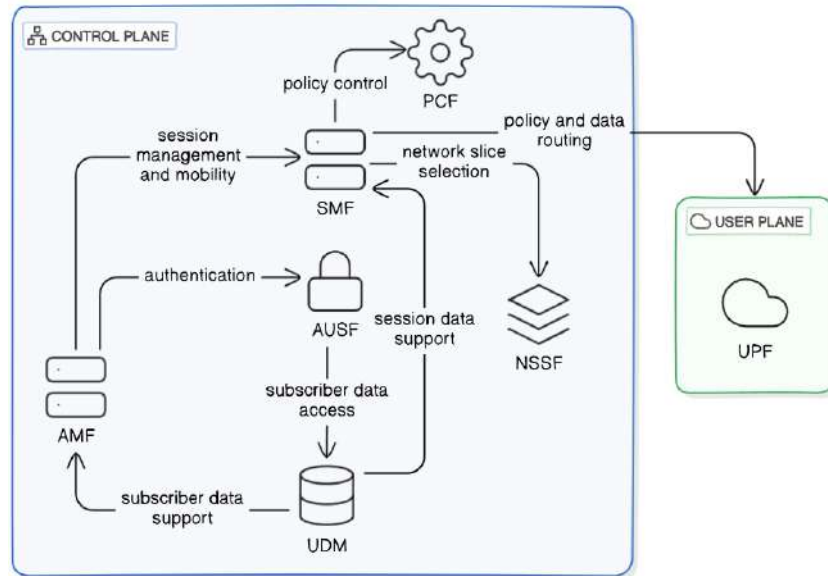


Figure 5. Interaction between the Control Plane and User Plane

User Plane: The user plane (Figure 5) handles data transfer between the UE and external data networks, such as the Internet. It primarily includes:

- **UPF (User Plane Function):** Routes and forwards user data packets, enforcing policies provided by the SMF and enabling data forwarding and QoS for different applications.

The control and user planes collaborate to ensure seamless connectivity and service delivery. The AMF and SMF coordinate to authenticate UEs and manage their connections, while the SMF provides UPF with the necessary policies and configurations to route data efficiently.

3.3 Components in Details

The NITRO (5G Nitro Cyber Range) architecture consists of several logical components that work together to create a robust and versatile training environment for cybersecurity professionals. Each component plays a crucial role in simulating, monitoring, and analyzing various aspects of the 5G network and its security.

Open5GS is an open-source implementation of the **5G Core (5GC)**, enabling the deployment and management of 5G networks. Its modular and flexible architecture supports various network functions, allowing developers and network operators to customize their deployments according to specific requirements. One of the significant advancements offered by 5G is **network slicing**, a method that enables multiple virtual networks to coexist on a single physical infrastructure. This allows for tailored services for different use cases, such as Internet of Things (IoT) applications, high-speed internet access, and low-latency services critical for real-time applications.

Component	Component
5G Core (5GC)	The backbone of the 5G infrastructure, managing data routing, user sessions, and overall network management. It includes elements like AMF (Access and Mobility Management Function), SMF (Session Management Function), and UPF (User Plane Function).
User Equipment (UE)	Devices such as smartphones, IoT gadgets, and sensors that connect to the 5G network. These interact with the gNodeB (base station) for radio communication and data transmission.
gNodeB (gNB)	Responsible for managing the radio communication between user devices, known as User Equipment (UE), and the 5G Core (5GC) network. While it includes antenna hardware for transmitting and receiving signals, it also has processing units to handle data, control signals, and mobility management tasks.
Open5GS	An open-source 5G Core (5GC) implementation that facilitates the deployment and management of 5G networks. Its modular, flexible design allows for customization in deployments to suit various requirements.
AAA Server	Handles essential AAA functions in the 5G network, such as user credential verification, policy-based permission grants, and activity tracking for billing/reporting. Ensures that only authorized users connect to and utilize the network.
IMSI	A unique identifier for each mobile subscriber, composed of the MCC (Mobile Country Code), MNC (Mobile Network Code), and MSIN (Mobile Subscriber Identification Number). It supports authentication, service provisioning, and billing.
Diameter Protocol	A protocol for Authentication, Authorization, and Accounting (AAA) that supersedes RADIUS. Used in 4G and 5G networks to secure communication between the HSS and the AAA server, it facilitates authentication, policy enforcement, and service authorization.
FreeDiameter	An open-source Diameter protocol implementation within the NITRO project, enabling flexible, extensible Diameter-based applications and services.

Table 4. Main Components of the 5G and Short Explanation

User Equipment (UE) refers to any device that connects to the 5G network, including smartphones, IoT devices, and sensors. These devices interact with the **base station (gNodeB)**, which connects the user equipment to the network and manages radio communication and data transmission. The **core network (5GC)** serves as the backbone of the 5G infrastructure, responsible for data routing, user sessions, and overall network management. It comprises various components such as the **Access and Mobility Management Function (AMF)**, **Session Management Function (SMF)**, and **User Plane Function (UPF)**.

In terms of performance metrics, latency is a critical factor in the 5G experience, representing the time it takes for data to travel from one point to another within the network. 5G aims to achieve ultra-low latency, potentially as low as 1 millisecond, which is essential for applications like autonomous driving and real-time gaming. Another important metric is throughput, which measures the amount of data successfully transmitted over the network within a given time frame, typically expressed in megabits

per second (Mbps) or gigabits per second (Gbps).

Advancements in **Network Function Virtualization (NFV)** and **Software-Defined Networking (SDN)** further enhance the flexibility and efficiency of 5G networks. NFV allows network functions to run on standard hardware instead of dedicated devices, reducing costs and improving scalability. SDN, on the other hand, enables network administrators to manage network services through abstraction of lower-level functionality, leading to a more programmable and responsive network.

The **International Mobile Subscriber Identity (IMSI)** is a unique identifier assigned to each mobile subscriber that is crucial for authentication and identification within a mobile network. The IMSI is typically stored on the **Subscriber Identity Module (SIM)** card, which is inserted into mobile devices like smartphones, tablets, and IoT devices. The IMSI (Figure 6) is composed of three main components: the **Mobile Country Code (MCC)**, the **Mobile Network Code (MNC)**, and the **Mobile Subscriber Identification Number (MSIN)**.

- **Mobile Country Code (MCC):** This is a three-digit code that identifies the country of the subscriber. For example, the MCC for the United States is 310.
- **Mobile Network Code (MNC):** This code identifies the specific mobile network operator within that country. The MNC is typically two or three digits long and, when combined with the MCC, allows for precise identification of the network being used.
- **Mobile Subscriber Identification Number (MSIN):** This is a unique number assigned to the subscriber within the mobile network, usually consisting of up to 10 digits. It is used to distinguish one subscriber from another within the same network.

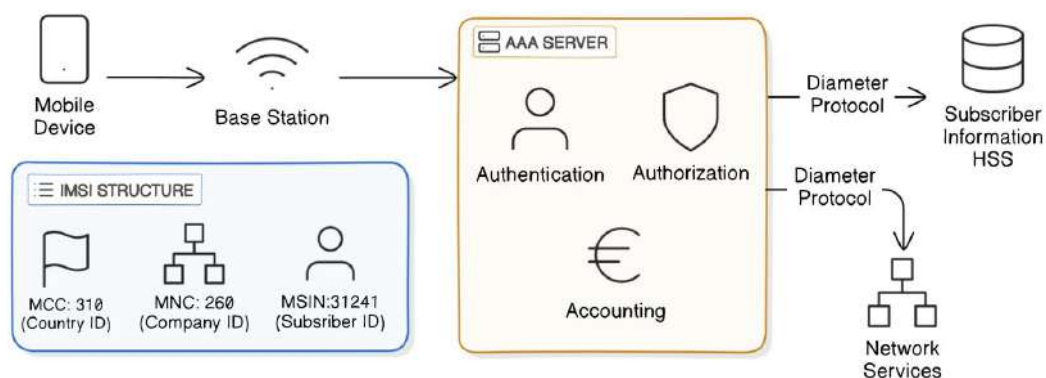


Figure 6. Details on the IMSI Structure and the Subscription to 5G Core Using the AAA Server

When a mobile device connects to a network, the IMSI is transmitted to the network to authenticate the subscriber and grant access to network services (Figure 6). The IMSI is vital for various network functions, including:

- **Authentication:** The network uses the IMSI to verify the identity of the subscriber, ensuring that only authorized users can access services.
- **Service Provisioning:** It allows the network to identify the services and plans associated with the subscriber.
- **Billing:** The IMSI is used to track usage for billing purposes, ensuring that subscribers are charged accurately based on their usage patterns.

Diameter is a protocol used for **AAA (Authentication, Authorization, and Accounting)** and is considered a successor to the older RADIUS (Remote Authentication Dial-In User Service) protocol. An **AAA server** is a server that manages user access and rights to network resources. It plays a critical role in network security by ensuring that users are properly authenticated, authorized for specific actions or services, and that their activities are tracked for accounting purposes. Diameter was designed to address the limitations of RADIUS, providing a more robust framework for AAA, particularly in the context of modern networks like 4G and 5G.

The **Diameter protocol** enables secure communication between the **Home Subscriber Server (HSS)** and the **AAA server** in 4G and 5G networks, supporting key functions like authentication, policy enforcement, and service authorization. Through **Authentication Data Exchange**, the HSS sends authentication credentials to the AAA server to verify a subscriber's identity. For **Policy Enforcement**, the HSS provides policy and profile details, allowing the AAA server to control service access based on the subscriber's plan. Finally, **Service Authorization** enables the AAA server to grant access to network services according to the permissions defined by the HSS.

Within the scope of the NITRO project **FreeDiameter** will be used as an open-source implementation of the Diameter protocol, providing a flexible and extensible framework for building Diameter-based applications and services. Open5GS includes an AAA server that implements the essential functions of authentication, authorization, and accounting within the 5G network. This is critical for managing user access and ensuring that only authorized users can connect to the network and utilize its services. The AAA server in Open5GS verifies user credentials, grants permissions based on defined policies, and tracks user activity for billing and reporting purposes.

3.4 5G Core Network (5GC)

The 5G Core Network processes, routes, and manages the data flow and control signaling between UEs and external networks. The core components (Figure 7) are responsible for managing sessions, enforcing policies, and ensuring security.

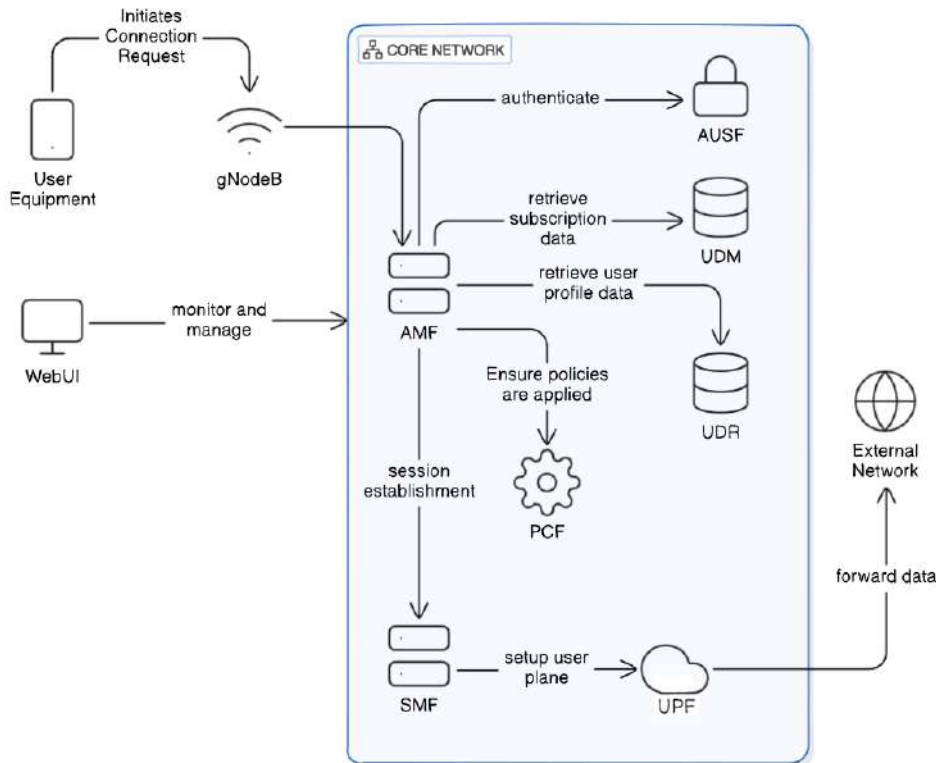


Figure 7. The 5G Core Architecture and Internal Data Flows

Access and Mobility Management Function (AMF): The AMF handles UE registration, authentication, mobility management, and session management. It is the first core network function to interact with the gNB. It communicates with various other core network components (such as AUSF, SMF, UDM) to establish and maintain connections for the UE.

User Plane Function (UPF): The UPF is responsible for forwarding user traffic between the UE and external networks (e.g., the internet). It operates at the data plane level, handling the actual data packets flowing through the network. The UPF is the key interface between the core network and external data services, enabling data routing and session continuity for the UEs.

Authentication Server Function (AUSF): The AUSF authenticates the UE when it attempts to connect to the network, ensuring that only authorized devices gain access. It uses security credentials like cryptographic keys shared by the UE and the network.

Unified Data Management (UDM) and Unified Data Repository (UDR): The UDM manages user subscription information, authentication, and authorization data. The UDR acts as a repository for subscriber and session data. These functions ensure that user profiles are stored and retrieved correctly during authentication and session establishment.

Session Management Function (SMF): The SMF is responsible for setting up and managing the data

sessions for the UE. It assigns IP addresses to UEs, controls data flows, and ensures proper routing of user traffic. It interacts with the UPF (User Plane Function) to route data packets between the UE and the external network.

Policy Control Function (PCF): The PCF enforces network policies related to Quality of Service (QoS), bandwidth usage, and session management. It ensures that traffic is managed according to predefined rules. The SMF communicates with the PCF to apply these policies during the setup and modification of data sessions.

Binding Support Function (BSF): The BSF ensures that session binding rules are applied consistently across different network slices or services. It maintains continuity for UEs as they move across different network segments or slices.

Service Communication Proxy (SCP): The SCP helps route control signaling messages between various network functions in a service-based architecture. It ensures that requests between services (such as between the AMF, SMF, and AUSF) are handled correctly and efficiently.

Network Repository Function (NRF): The NRF acts as a registry of all the available network functions. It allows other components to discover and communicate with one another as needed.

Network Slice Selection Function (NSSF): The NSSF helps allocate and select the appropriate network slice for a given service or user. Network slicing allows the 5G network to segment its resources to handle different types of traffic with specific performance or security requirements.

3.5 Management and Monitoring

WebUI: The **WebUI** provides a graphical interface for administrators to monitor and manage the 5G core network. It allows for easy access to logs, configurations, and system status, making it easier to control the network and diagnose issues.

3.6 Database for Storing 5G User Profiles

MongoDB: MongoDB is the backend database used by Open5GS components like AMF, PCF, UDM, and UDR to store user profiles, session information, and network configurations. It acts as the centralized data storage that supports various network functions.

3.7 5G Radio Access Network and User Equipment (UERANSIM)

The radio access network (RAN) and user equipment (UE) in this architecture are simulated using UERANSIM, an open-source tool that allows for the emulation of 5G base stations (gNodeB) and UE.

User Equipment - UE (Simulated by UERANSIM): UE represents devices such as smartphones or IoT devices that need to connect to the 5G network. These devices initiate the connection by communicating with the gNodeB (5G base station). Parameters like Mobile Subscriber ISDN (MSISDN), cryptographic keys, and Access Point Name (APN) are configured for each UE to define its identity and access rights in the network.

gNodeB (gNB, Simulated by UERANSIM): The gNodeB is the 5G base station that provides wireless connectivity between the UEs and the core network. It manages the radio interface, including signal strength, handovers, and communication protocols. It communicates with the core network's AMF to register the UE, initiate connections, and handle mobility-related tasks.

3.8 Data Flows and Interactions of the 5G Core

Data flows and interactions within the 5GC are essential for maintaining effective communication and service delivery. Figure 8 illustrates the data flow in a 5G core network architecture. The process begins with the User Equipment (UE) initiating a connection request. This request is then forwarded to gNodeB, which acts as a bridge between the UE and the core network.

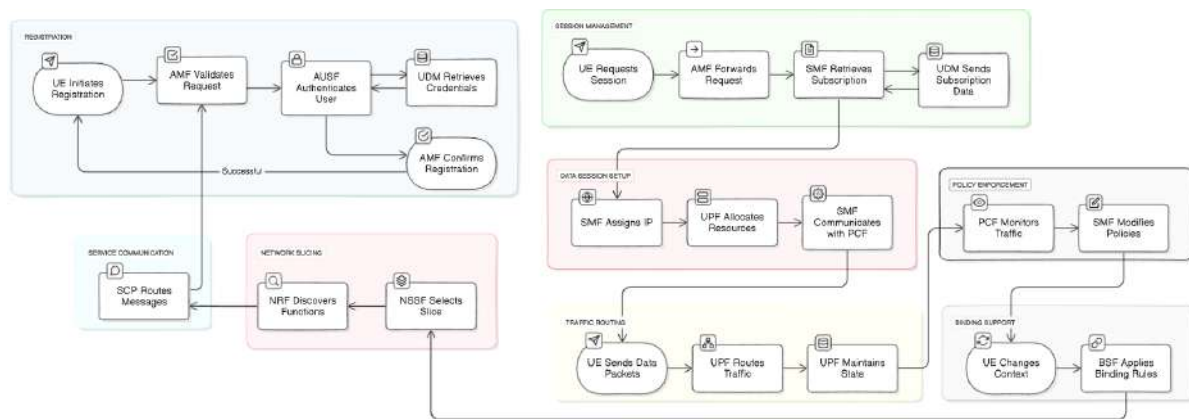


Figure 8. 5G Core Internal Network Data Flows

The gNodeB forwards the request to the Access and Mobility Management Function (AMF) within the core network. The AMF consults the Authentication Server Function (AUSF) for authentication and retrieves subscription data from the Unified Data Management (UDM). It also retrieves the user's profile data from the User Data Repository (UDR).

The AMF then ensures that the appropriate policies are applied and coordinates with the Session Management Function (SMF) for data session establishment. The SMF, in turn, sets up the user plane by communicating with the User Plane Function (UPF). Finally, the UPF forwards the data to the external network, allowing the UE to access the requested services. Meanwhile, a WebUI monitors and manages the entire process. The architecture facilitates several critical processes:

1. **User Registration and Authentication:** Upon powering on, a UE initiates the connection process by sending a registration request to the AMF. This request marks the beginning of the communication sequence between the UE and the network. In response, the AMF takes on the critical role of verifying the UE's identity. To achieve this, it queries the UDM system, which is responsible for maintaining user profiles and authentication credentials. The UDM retrieves the necessary information associated with the user, ensuring that the UE is indeed a legitimate entity

seeking access to the network. Once the UE's identity has been successfully authenticated, the AMF proceeds to establish a session context specifically for the user. This session context serves as a framework for managing the ongoing communication and data exchange, laying the groundwork for subsequent network interactions. **Example:** When a user logs into their smartphone after a restart, the device sends a registration request to the AMF, which validates the user's credentials with the UDM.

2. **Session Establishment:** Following the successful registration of the User Equipment (UE), the next step involves the UE requesting the establishment of a session. This request is forwarded by the AMF to the SMF. The SMF plays a crucial role in this process as it is responsible for allocating the necessary resources to facilitate the session. Additionally, the SMF sets up the required data paths to ensure smooth communication and data transfer. To accomplish this, it interacts with the UPF, which is essential for managing the data flow within the network. Through this interaction, the SMF ensures that the required bandwidth is available, thereby optimizing the session establishment process and allowing for efficient data transmission between the UE and the network. **Example:** In a video conferencing application, the SMF allocates sufficient resources to maintain high-definition video quality, while also managing connections for other participants.
3. **Mobility Management:** Mobility management is a critical aspect of maintaining seamless connectivity as the UE moves between different coverage areas. When the UE moves out of the coverage area of one cell and into another, the AMF takes charge of the handover process. This involves transferring the UE's session context to the new AMF that is responsible for managing the cell into which the UE has transitioned. By ensuring that the session's context is accurately and efficiently transferred, the AMF plays a vital role in maintaining an uninterrupted user experience. This handover process allows the UE to continue its data transmission and communication without any noticeable disruptions, thereby enhancing overall network reliability and user satisfaction as they move across different network environments. **Example:** A user walking through a train station will seamlessly transition from one cell to another while continuing their video call without dropping the connection.
4. **Data Transmission:** Once the session is established, the UPF takes charge of routing user data packets between the UE and the external network. This pivotal role ensures that data flows seamlessly to and from the UE, facilitating effective communication and connectivity. In addition to routing, the UPF is responsible for applying QoS policies that have been established by the PCF. These QoS policies are essential for managing network resources and ensuring that critical traffic receives prioritized handling. By implementing these policies, the UPF can optimize network performance, enhance user experience, and maintain the integrity of important data transmissions, ensuring that time-sensitive or high-priority communications are treated with the necessary urgency and reliability. **Example:** During a video call, the UPF ensures that video packets are prioritized over non-critical data, such as background application updates, to maintain call

quality. In a scenario where multiple users are streaming video in a crowded area, the PCF might lower the resolution for some users to ensure others can maintain a quality experience.

When a user wants to stream a live video: a) The user registers with the AMF, b) The AMF communicates with the UDM to authenticate the user, c) The user initiates a session, and the SMF establishes it by coordinating with the UPF to route data to the video server, d) The UPF manages the data flow to ensure the user experiences smooth streaming.

3.9 NITRO Architecture Capability Blocks and Validation

The validation methodology for the NITRO 5G Cyber Range focuses on systematically assessing the platform's capabilities to ensure they meet their intended objectives. This process evaluates both individual features and the overall system performance, emphasizing reliability, scalability, and security. Each capability block undergoes rigorous testing aligned with predefined success criteria and failure handling mechanisms. The methodology ensures that all features operate seamlessly, even under challenging conditions, and provides actionable insights for improvement.

Phase	Milestone	Description
M21	First Prototype	Initial development and testing of the first prototype. Focus on validating core features and identifying areas for improvement.
M27	Assessment	Comprehensive evaluation of the platform's performance, focusing on reliability, scalability, and security. Adjustments and refinements based on predefined success criteria.
M33	Second Prototype	Development of the second prototype, incorporating feedback from the first prototype and the assessment phase. Testing of enhanced features and new functionalities.
M36	Final Assessment	Final validation of the platform, ensuring all features operate seamlessly under challenging conditions. Last opportunity for improvements before deployment.

Table 5. Integration and Validation Milestones

The first phase of the validation process is planned for M21 (Table 5). It involves the development and testing of the first prototype of the NITRO Cyber Range. During this phase, initial testing focuses on verifying the basic functionalities of the platform. It is an opportunity to assess the core architecture and ensure that the platform's foundational features work as expected. Additionally, this phase helps identify any areas for improvement that can be addressed in later stages.

At M27, the platform is planned to proceed to a comprehensive assessment phase, where the features are evaluated against predefined success criteria. This stage is critical in determining how well the platform performs in terms of reliability, scalability, and security in real-world conditions. Based on the outcomes of this assessment, necessary adjustments and refinements are made to the platform

to ensure that it meets performance standards and is ready for further testing.

The M33 phase involves the development and testing of the second prototype. Building on the feedback and insights gained from the first prototype and the earlier assessment phase, the second prototype incorporates improvements and new functionalities. This phase tests the platform's enhanced features and evaluates whether the modifications made are effective. It ensures that the platform continues to meet the required standards for performance, scalability, and security.

Finally, at M36, the platform undergoes a final assessment. This phase focuses on confirming that all features operate seamlessly, even under challenging conditions. It is the last opportunity to make any final improvements or adjustments before the platform is considered ready for deployment. The results from this final validation phase help ensure that the NITRO 5G-IoT Cyber Range is fully functional, secure, and reliable, ready to be used in real-world 5G-IoT environments.

The primary objectives of the validation process include verifying the platform's ability to simulate realistic 5G network scenarios, enable effective cybersecurity mechanisms, and support dynamic scalability. Performance, reliability, and security are assessed under various conditions, including high traffic loads and simulated cyberattacks. The process also evaluates the user experience, focusing on parameters such as latency, throughput, and data accuracy to optimize the training environment for both administrators and trainees.

Each capability block (Table 6) has dedicated test cases designed to validate its functionality. For example, NITRO-ARCH-01 involves simulating realistic 5G traffic patterns while ensuring minimal jitter and verifying rapid deployment times. NITRO-ARCH-02 focuses on configuring cybersecurity mechanisms and testing their effectiveness in blue team scenarios. For NITRO-ARCH-10, varying user loads are simulated to evaluate the system's dynamic scaling capabilities and its ability to maintain performance under stress. Similarly, NITRO-ARCH-12 assesses bandwidth allocation and rerouting efficiency during periods of high network traffic.

ID: Title	NITRO-ARCH-01: Realistic 5G Traffic Simulation
Description	The platform emulates realistic 5G traffic patterns with minimal jitter.
Short summary	This use case focuses on providing a realistic training environment for network performance testing.
Criteria for success	Fast deployment times with minimal downtime
Failure conditions	Network congestion or disconnectedness
Failure handling	Traffic shaping and rerouting techniques

ID: Title	NITRO-ARCH-02: Cybersecurity Mechanisms
Description	Essential cybersecurity features are integrated to monitor threats.
Short summary	This use case focuses on enabling features for supporting blue team scenarios within the cyber range.

Criteria for success	Successful deployment and configuration
Failure conditions	Missing rules, or incapability to integrate
Failure handling	Rule generation, integration testing and adaption

ID: Title	NITRO-ARCH-03: Database Management
Description	The system efficiently manage high-volume subscriber and device profiles.
Short summary	This use case centers on the management of subscriber data in a scalable way.
Criteria for success	Database access parameters
Failure conditions	Data corruption, or incapability to submit or retrieve data
Failure handling	Database recovery procedures, configurations

ID: Title	NITRO-ARCH-04: End-to-End Encryption
Description	The system ensures data confidentiality through encryption.
Short summary	This use case ensures that data transmitted across the network remains secure.
Criteria for success	High level of data confidentiality achieved
Failure conditions	Encryption failure
Failure handling	Alternative encryption pathways activated

ID: Title	NITRO-ARCH-05: User Equipment Interaction with 5G Core
Description	User Equipment (UE) interacts seamlessly with the 5G Core network.
Short summary	This use case focuses on ensuring that UEs can communicate effectively with the 5G Core for service access and network functionalities.
Criteria for success	Successful communication and service access for UEs with the 5G Core.
Failure conditions	Communication failures between UEs and the 5G Core.
Failure handling	Log analysis for troubleshooting; reconfiguration of UEs if necessary.

ID: Title	NITRO-ARCH-06: Support the Addition for Multiple User Equipment
Description	The system supports the addition of multiple User Equipment (UEs) without degradation of performance.
Short summary	This use case focuses on the scalability of the network to accommodate multiple UEs simultaneously.
Criteria for success	Capable of adding new UEs.
Failure conditions	Integration issues with increased UE numbers.
Failure handling	Scale resources dynamically; investigate bottlenecks in network performance.

ID: Title	NITRO-ARCH-07: Retrieve and Inspect 5G Network Traffic
Description	Retrieve and inspect the 5G network traffic for analysis and troubleshooting.
Short summary	This use case enables network administrators to access and analyze traffic data for performance and security assessments.
Criteria for success	Comprehensive access to real-time traffic data with analytical capabilities.

Failure conditions	Inability to retrieve or inspect network traffic.
Failure handling	Log errors and review monitoring tool configurations.

ID: Title	NITRO-ARCH-08: Scoreboard and Submission Capability
Description	Submission of flags or other approach to retrieve the progress of the trainees is supported.
Short summary	This use case facilitates the engagement of trainees in challenges by allowing flag submissions for validation.
Criteria for success	Flags are submitted correctly.
Failure conditions	Incorrect flag submissions or system errors during submission.
Failure handling	Provide error messages and resubmit options; log submissions for review.

ID: Title	NITRO-ARCH-09: Retrieval of Trainee Metrics
Description	Trainee metrics and actions are retrievable from the Cyber Range for assessment and feedback.
Short summary	This use case allows instructors to analyze trainee performance metrics for evaluation and improvement.
Criteria for success	Accurate and timely retrieval of metrics for all trainees.
Failure conditions	Inability to retrieve metrics or inaccurate data.
Failure handling	Log errors and review data collection processes; notify system administrators.

ID: Title	NITRO-ARCH-10: Dynamic Scaling of Core Network Components
Description	The system supports dynamic scaling of core 5G components to handle varying user loads and network traffic.
Short summary	The use case enables the cyber range to adaptively scale resources based on demand.
Validation Test Case	Simulate different traffic loads and verify automatic scaling of core network components.
Criteria for success	Core network components adapt to increased traffic without performance degradation. Increased user satisfaction and performance efficiency
Failure conditions	Resource limits reached
Failure handling	If scaling fails, trigger manual scaling and verify alerting mechanisms to administrators. Alerts sent to the administrator, and auto-scaling triggers initiated

ID: Title	NITRO-ARCH-11: Isolation of Network Slices
Description	The cyber range provides the capability to isolate network slices for distinct environments.
Short summary	This use case allows for simultaneous teams and user activities in separated virtual environments.
Validation Test Case	Deploy isolated network slices for separate teams and run concurrent simulations.
Criteria for success	No cross-contamination between slices; each operates in its virtual environment. Successful simulation sessions with zero cross-contamination
Failure conditions	Misconfigured slices
Failure handling	Log slice configurations, adjust isolation settings, and alert administrators to configuration issues. Automatic alerts to administrators, manual configuration options

ID: Title	NITRO-ARCH-12: Network Configuration, Bandwidth Allocation and Rerouting
Description	The system intelligently allocates network bandwidth and support automatic rerouting to optimize performance under variable network load and congestion.
Short summary	Adjust bandwidth dynamically and reroute traffic to avoid bottlenecks, ensuring reliable connectivity during high-traffic periods.
Criteria for success	Efficient bandwidth utilization, improved network stability, and enhanced user experience
Failure conditions	Failure to apply rerouting
Failure handling	Configuration changes

ID: Title	NITRO-ARCH-13: Container Orchestration Integration
Description	The system integrates with Kubernetes or similar to allow distributed deployment.
Short summary	This use case focuses on deploying the cyber range in a containerized environment.
Criteria for success	Fast deployment times with minimal downtime
Failure conditions	Deployment failures
Failure handling	Logs reviewed for issues; redeployment initiated

Table 6. NITRO 5G Cyber Range Capabilities

Failure handling mechanisms are tested by simulating adverse scenarios for each capability. For instance, traffic congestion (Table 6 - NITRO-ARCH-01) is used to evaluate traffic shaping techniques, while misconfigured rules in NITRO-ARCH-02 test the system's ability to adapt and integrate new configurations. Resource exhaustion scenarios in NITRO-ARCH-10 are used to validate both manual and automated scaling procedures. These tests ensure the robustness of failure handling protocols and help refine the system's resilience.

The validation process follows a structured approach, beginning with preparation, where isolated environments are created for controlled testing conditions. During execution, the defined test cases are implemented, and real-time data is captured to monitor performance, reliability, and security. The analysis phase involves comparing observed results with the success criteria to identify deviations, bottlenecks, and potential areas for improvement. Comprehensive documentation of results, including logs and performance graphs, facilitates transparency and supports decision-making.

4 Stakeholders and User Roles

The primary stakeholders in the NITRO project include **academic institutions, industry partners, government agencies, and training organizations (Table 7)**. Academic institutions, such as universities and research centers, play a vital role by providing theoretical knowledge and practical expertise in cybersecurity and network technologies. These institutions have experience in curriculum development, ensuring that training content aligns with current industry standards and practices. Additionally, their research capabilities are used to identify emerging threats and vulnerabilities in 5G and IoT environments [17], contributing valuable insights to the training programs.

Stakeholders	Description
Academic Institutions	Simulation capabilities for research and training, incorporating practical exercises in cybersecurity and network technology courses. Integration with curriculum and conducting research on emerging threats, vulnerabilities, and defense strategies in 5G and IoT environments.
Industry	Create realistic training modules reflecting real-world scenarios, tools, and challenges. By collaborating with academic institutions, they help design training exercises that simulate current industry demands, equipping trainees with practical skills for industry-specific cybersecurity roles.
Government Agencies	Ensure training aligns with regulatory standards and promotes best practices in cybersecurity. They may also use the project to foster collaboration with other sectors, enhancing national and international security measures for critical infrastructure protection.
Training Organizations	Create engaging, hands-on exercises and simulations for various skill levels. They apply adult education methods to ensure the training is accessible, effective, and aligned with industry needs, thus helping to improve the overall quality and impact of cybersecurity education.
Trainee Groups	Engage in hands-on experience in cybersecurity, tailored to beginner, intermediate, and advanced levels. The exercises support both offensive and defensive practices, helping trainees build practical skills in a controlled, realistic environment.

Table 7. Main Stakeholders

Industry partners, including telecommunications companies, cybersecurity firms, and technology vendors, are integral to the NITRO project. They provide experience regarding real-world scenarios, technologies, and tools that are essential for creating a realistic training environment. These partners will be able to collaborate with academic institutions to develop training modules that reflect current industry challenges, ensuring that trainees gain hands-on experience with relevant technologies.

Government agencies in collaboration with universities play a significant role in the NITRO project by establishing regulations and guidelines for cybersecurity practices. Their indirect involvement ensures that the training programs adhere to national and international standards, promoting best practices in cybersecurity. These agencies may also provide resources or support training initiatives, fostering collaboration between the public and private sectors to enhance the overall security posture of critical infrastructure.

Training organizations can use the results from NITRO and utilize or extend simulation tools, hands-on exercises, and real-world scenarios to engage trainees and enhance their learning experiences.

Their expertise in adult education and instructional design ensures that training is effective, relevant, and aligned with industry requirements.

In the context of the NITRO project and Open5GS, developing tailored exercises for each trainee group—beginner, intermediate, and advanced—is crucial for effective learning in cybersecurity. These exercises allow trainees to gain hands-on experience in both offensive and defensive practices, leveraging the capabilities of the cyber range. Below are detailed examples of exercises designed for each group. In the following subsection, the capabilities of NITRO are explained since the architecture can support those exercises. More details on the exercises and their implementation will be provided in D3.1 – NITRO security training exercises design and development - first version and D3.3 in the second version.

Administrators in the context of the NITRO Cyber Range are responsible for managing the technical infrastructure that supports the scenarios regarding the 5G-IoT. The role of the administrators includes setting up and maintaining virtual environments that simulate real-world 5G IoT networks, including high-bandwidth connections, low-latency requirements, and large-scale device deployments. Administrators must configure network slices, manage virtual network functions (VNFs), and ensure interoperability between IoT devices and 5G systems. They also oversee the deployment of realistic cyber-attack scenarios that mimic threats specific to IoT ecosystems, such as Distributed Denial-of-Service (DDoS) attacks, malware propagation, and device exploitation.

Trainers and educators leverage the NITRO Cyber Range to design and deliver hands-on exercises that reflect the complexities of 5G IoT security. They create scenarios where trainees can engage in offensive and defensive practices, such as securing IoT devices, detecting anomalous behaviors, and mitigating 5G-specific threats like signaling storms or protocol vulnerabilities. For beginner trainees, exercises may involve fundamental IoT security practices, such as securing device authentication and encryption. Intermediate and advanced trainees may work on detecting and responding to coordinated attacks targeting 5G network slices or vulnerabilities in IoT communication protocols. Trainers also incorporate real-world 5G IoT case studies to ensure the exercises remain relevant and practical.

Managers play a strategic role in aligning the capabilities of the NITRO Cyber Range with the needs of organizations operating in 5G IoT ecosystems. They ensure that training objectives address critical areas such as securing IoT devices, ensuring 5G network reliability, and protecting sensitive data transmitted over 5G connections. Managers coordinate resources, schedule training sessions, and define success metrics to evaluate the effectiveness of the exercises. They also emphasize compliance with cybersecurity standards and regulations relevant to 5G IoT, such as GDPR, NIS2, or ETSI standards (e.g. EN 303 645), to ensure that the training supports the broader organizational goals of security and reliability.

4.1 First Trainee Group (Tier 1): Beginners

For beginner trainees, an effective learning path involves the **Basic Network Security (Figure 9)**. In a simulated environment, trainees will learn about essential network protocols such as TCP/IP, HTTP, and DNS. A solid understanding of IP routing within the 5G core network is essential for beginners. In this section of training, trainees will learn about the architecture of the 5G core network, including its components, such as the gNB and the UE.

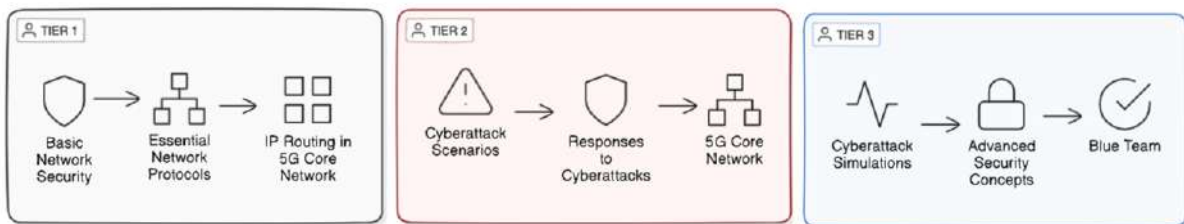


Figure 9. Trainee Groups

The gNB serves as the base station, providing wireless connectivity to the UE, while the UE represents the devices that connect to the network, such as smartphones or IoT devices. Trainees will explore the overall networking principles, including how data flows through the core network and the role of various network functions like the UPF for data routing, the SMF for session establishment, and the AMF for handling user authentication and mobility management. They will learn about the concept of slicing in 5G networks, where resources are partitioned to provide tailored services for different types of users and applications. Furthermore, trainees will engage in practical exercises that involve **configuring IP routes** within the Open5GS environment. This includes understanding how to manage network traffic, setting up IP addresses for different network functions, and ensuring that data is routed efficiently from the UE through the gNB and into the core network.

5G Core Network Architecture and Components: Trainees will delve into the architecture of the 5G core network, exploring its key components and how they interact to facilitate communication between user devices and the broader network. They will learn about the gNB and the UE, which are fundamental to the 5G infrastructure. Below are detailed descriptions of the potential tasks:

- **Understanding Network Slicing:** A deep understanding of network slicing technology, which enables multiple isolated virtual networks (or "slices") to run over the same physical 5G network. Each slice can have different performance requirements and be isolated from others, but this isolation can be compromised through attacks.
- **IP Routing and Configuration:** Set up IP addresses for different network components and manage network traffic flow efficiently. This exercise will help them understand how data is routed from the UE through the gNB and into the core network, ensuring that traffic is directed correctly and efficiently. For example, trainees will set up and configure IP addresses for the AMF, SMF, and UPF, ensuring proper communication between these network functions. This involves the

configuration of routing paths for user data, ensuring that data from a UE is routed correctly through the network infrastructure. Furthermore, the trainees will get familiar with resource management and get information on the status of the 5G components including traffic management configurations.

- **Introduction to Security Concepts:** Introduction to basic security concepts relevant to 5G networks, such as authentication, encryption, and access control. These concepts will help them understand the importance of securing network traffic and maintaining the integrity of data transmitted over the network.

4.2 Second Trainee Group (Tier 2): Intermediate

In the advanced training module of the NITRO project focused on Open5GS, trainees will explore various cyberattack scenarios targeting the 5G core network, specifically assessing the responses of critical components such as the Access and Mobility Management Function (AMF) and the User Plane Function (UPF). Below are detailed descriptions of key attack types that trainees will simulate, focusing on their impact on these components.

- **5GReplay Attacks:** The 5GReplay attack [27] involves capturing valid signaling messages exchanged between the User Equipment (UE) and the 5G core network, particularly during the authentication and connection setup phases. Once these messages are captured, attackers can replay them to the AMF to gain unauthorized access or impersonate legitimate users. The AMF is responsible for handling the registration and authentication of UEs. In a 5GReplay attack, if the AMF fails to implement strong mechanisms to detect and block replayed messages, it may inadvertently allow unauthorized access, leading to potential data breaches or service disruption. Trainees will analyze how the AMF responds to replayed authentication requests and assess its effectiveness in preventing such attacks.
- **Denial of Service (DoS) Attacks:** In a Denial-of-Service attack, trainees will simulate overwhelming the AMF by sending an excessive number of authentication requests from the UE in a short period. This flood of requests can saturate the processing capacity of AMF, leading to service degradation or complete unavailability for legitimate users. Under a DoS attack, the AMF may struggle to differentiate between legitimate authentication requests and malicious ones, causing delays in processing or failure to authenticate valid UEs. Trainees will observe how the performance of AMF is affected, as well as the potential cascading effects on other network functions due to the increased load.
- **Data Flooding Attacks:** In a data flooding attack, trainees will generate an excessive amount of data traffic directed at the UPF, which is responsible for data routing between the user plane and the core network. This exercise will simulate scenarios where the UPF is overwhelmed with data packets, impacting its performance and the overall network. The role of UPF in managing user data sessions makes it a critical component in the 5G core architecture. When subjected to data flooding, the UPF may experience increased latency, reduced throughput, and potential packet loss. Trainees will evaluate how effectively the UPF maintains data flow under heavy load and

whether it can implement traffic shaping or quality of service (QoS) measures to mitigate the impact of such attacks.

- **Eavesdropping Attacks:** Eavesdropping attacks involve intercepting communications between the UE and the 5G core, aiming to capture sensitive information transmitted over the network. Trainees will simulate this attack to understand the vulnerabilities in communication channels. The AMF and UPF play pivotal roles in managing signaling and user data. If attackers can eavesdrop on the signaling messages between the UE and AMF, they may gain access to authentication credentials and session information. Similarly, intercepting data traffic flowing through the UPF could lead to unauthorized access to user data. Trainees will analyze how these components can implement encryption and secure protocols to protect against eavesdropping.

4.3 Third Trainee Group (Tier 3): Advanced

The third tier is intended for advanced trainees who possess significant knowledge and experience in cybersecurity and network management. This group will focus on hands-on simulations of cyberattacks, assessing the resilience of 5G networks, and understanding advanced security concepts. This involves the execution of cyberattack simulations and the monitoring of the responses from the system.

- **Vulnerability Assessment:** Trainees will be introduced to advanced techniques for assessing vulnerabilities in 5G network components. They will learn how to scan and identify weaknesses in network configurations, system architectures, and software implementations, with a specific focus on 5G-specific components. This knowledge will be vital in recognizing areas that adversaries could exploit and proposing remediation steps.
- **Incident Response:** Trainees will develop effective incident response strategies once an attack has been detected. This includes understanding the steps required to contain the attack, mitigate its effects, and recover from the security breach. The focus will be on real-time decision-making, isolating compromised elements of the network, and implementing defensive tactics such as rate-limiting, traffic filtering, or blackholing malicious traffic. Additionally, they will work on post-incident analysis, where they will examine the attack's footprint, review logs, and generate reports that outline the timeline of events, key findings, and recommendations to prevent future incidents. This element of the training emphasizes quick identification of vulnerabilities, precise attack attribution, and effective recovery protocols.
- **Adversarial AI:** Adversarial AI involves generating specific inputs, known as adversarial examples [11], that are designed to corrupt or create mistakes on the machine learning models. These inputs are crafted in such a way that they appear normal to the human eye or to standard network analysis tools, but they trigger incorrect responses from the AI-based IDS. A key exercise for intermediate-level trainees involves attacking the AI model of an IDS, focusing on how adversarial inputs can be crafted to deceive or evade machine learning algorithms used in network security [12].

4.4 Discussion on the Capabilities of the Architecture

Each 5G core network component within the NITRO 5G Cyber Range architecture is validated to ensure it can support a range of cyberattack simulations and defensive exercises. These validations cover the critical functions of connectivity, authentication, data routing, and policy enforcement. The platform's modular architecture [10] allows trainees to explore component interactions, identify vulnerabilities, and deploy real-time defensive measures, ensuring a comprehensive training environment that supports network security learning across all tiers.

5 Scalability Considerations and Integration Capabilities

The main scalability considerations (Figure 10) arise from the need to accommodate a large number of users, emulate realistic network conditions, and support a high volume of connected devices and traffic streams. Below, the primary scalability issues in a cyber range context are provided.

The technical and operational constraints of deploying Open5GS within a 5G cyber range do not just present challenges; they introduce valuable learning opportunities that enhance the depth and realism of Red and Blue Team training scenarios. These limitations allow participants to engage with real-world issues of scalability, resource allocation, and system resilience, making the cyber range a more authentic environment for practicing network security strategies. For example, when DDoS attacks are launched by Red Teams, they place significant strain on the network's core functions, challenging participants to manage limited resources under high-stress conditions. Blue Teams must learn to make strategic decisions on resource prioritization, such as allocating more power to critical nodes (e.g., UPF) to keep data flowing to essential services or rate-limiting non-essential traffic.

However, for a cyber range to be effective as a training platform, it must accommodate multiple trainees simultaneously, allowing Red and Blue Teams to practice offensive and defensive tactics in a collaborative and realistic setting. Hosting multiple trainees introduces additional challenges, such as isolation between exercises, resource sharing, and managing network performance, which must be carefully orchestrated to ensure a meaningful training experience.

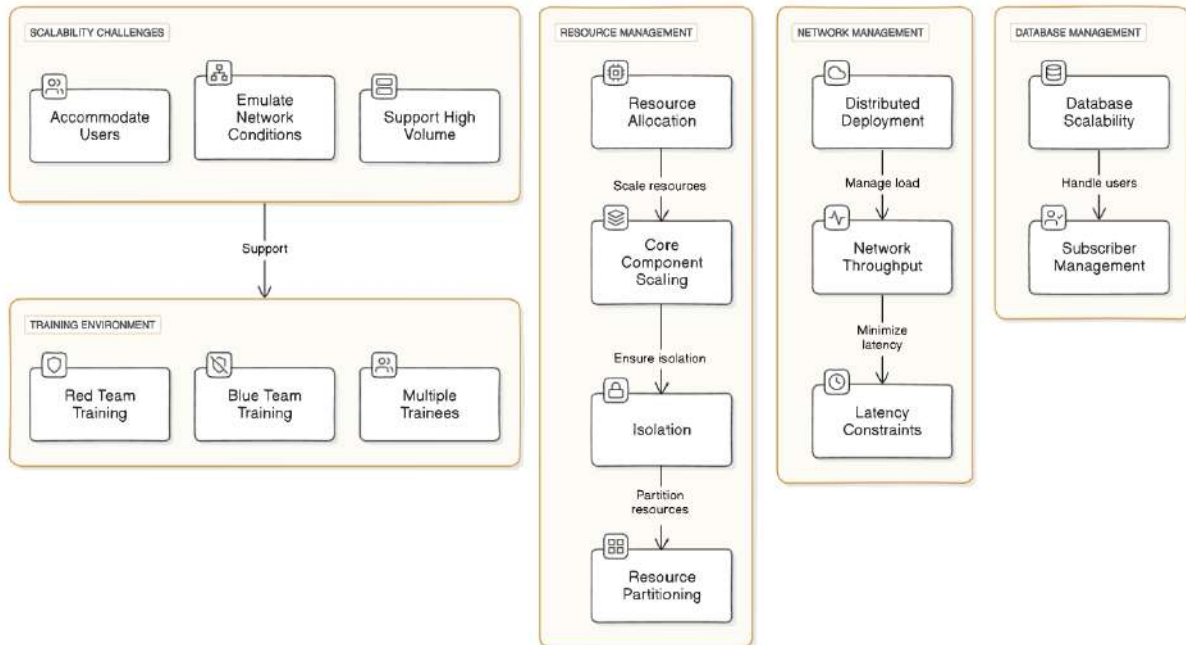


Figure 10. Scalability Considerations for the NITRO 5G Cyber Range

5.1 Resource Allocation and Core Component Scaling

The core network components, including the AMF, the SMF, and the UPF, are the most important microservices for the NITRO 5G operations. These components are tasked with processing complex, resource-intensive 5G traffic simulations. As the number of connected devices and concurrent user sessions increases, these core functions require dynamic resource allocation to scale efficiently. This scaling typically involves adding more computational resources or deploying additional instances of core components to handle the load, which may strain available resources within the cyber range.

5.2 Isolation and Resource Partitioning for Multiple Trainees

The cyber range must isolate sessions to allow concurrent activities without interference. This requires creating multiple virtual network slices within Open5GS, where each slice operates independently, simulating a multi-tenant 5G architecture.

For trainees, these isolated slices offer a realistic model of resource partitioning within actual 5G networks, where various operators share infrastructure (Figure 10). Deploying multiple isolated 5G instances enables each trainee or team to operate in a dedicated environment, minimizing interference and providing a realistic platform for simulating 5G network security scenarios. By implementing separate instances, Red or Blue Team can practice offensive and defensive techniques in their own network slice, which is especially beneficial for simulating complex and resource-intensive scenarios like DDoS attacks, network misconfigurations, or segmented intrusion attempts.

Another approach includes assigning each trainee a dedicated UE and gNB within the same Open5GS

instance. Each trainee receives their own UE and gNB pair (Figure 11), ensuring that network traffic and activities are isolated at both the device and access points. This setup enables Red Team trainees to launch targeted attacks or network exploits, such as signalling storms or malformed packet injections, directly from their own UE, impacting only their designated gNB.

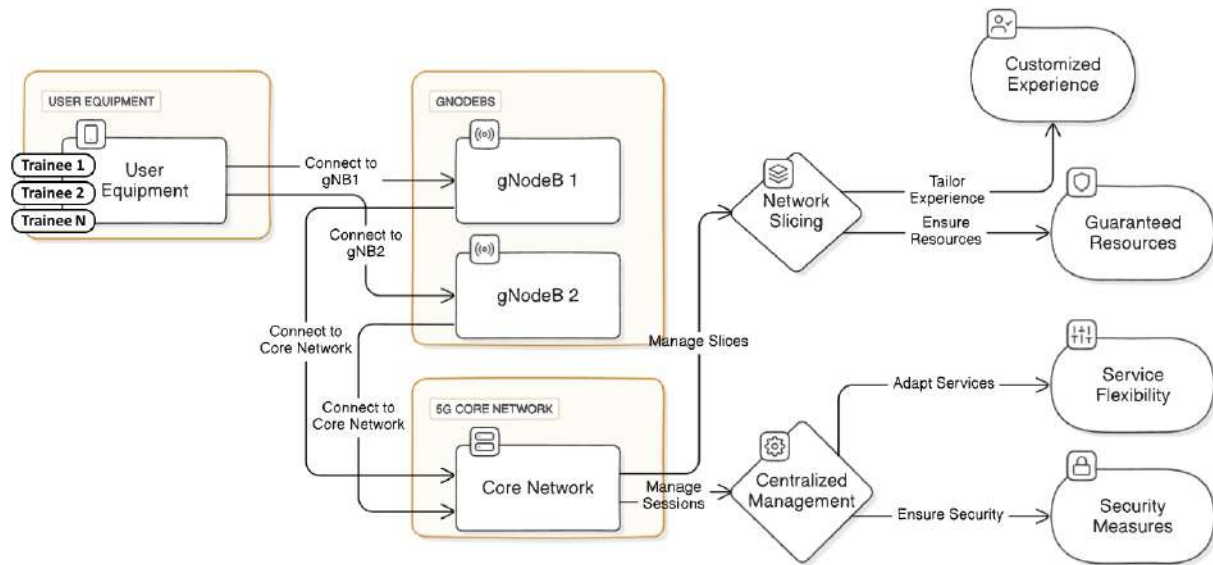


Figure 11. Scalability Considerations: Isolation and Resource Partitioning

Although multiple gNBs can offer isolation, they share the same Open5GS core network resources, which may lead to performance bottlenecks during high-demand scenarios. While isolation is a primary goal, the shared core environment can inadvertently create situations where one team's training activity affects another's learning outcomes. For example, if a Red Team successfully overwhelms the UPF with a coordinated attack, the resulting service degradation could hinder the Blue Team's ability to respond and practice their defensive strategies effectively. Balancing the need for realism in attack scenarios with the educational objectives for all trainees will be a critical challenge.

5.3 Integration Principles

The NITRO 5G Cyber Range aims to provide a comprehensive framework for simulating, testing, analyzing, and refining security in 5G and IoT networks. The integration principles outlined on Table 8 focus on creating a sophisticated cyber range that not only accommodates realistic testing environments but also ensures compliance with privacy regulations such as GDPR. These principles facilitate modular design, seamless orchestration, and specific feature development, such as cascading attack analysis and adversarial AI exercises. By adhering to these principles, NITRO is positioned to advance the understanding of vulnerabilities and enhance the resilience of 5G and IoT systems.

Principle	Requirement	Implementation Details	Alignment
Simulated Testing Environment	Establish a robust cyber range	Scenario-based testing with SPIDER 5G and CTF platforms	Modular design for isolated testing
Compliance and Privacy	Incorporate a privacy toolbox	GDPR compliance and personal data safeguarding	Centralized management of data flows
Cascading Attack Analysis	Facilitate cascading attack simulations	Use UBI's infrastructures for interconnected scenarios	Interoperability for accurate vulnerability analysis
Adversarial AI Exercises	Implement adversarial AI training	Simulate AI-targeted attacks using real-world datasets	Control and privacy measures in scenario management
Data Repository and Incident Tracking	Develop the NITRO Data Repository	Real-time tracking and analysis using automated traffic generation tools	Unified dashboard for incident data management

Table 8. Integration Principles to be Considered

The requirement for a robust cyber range entails the establishment of an environment that supports scenario-based testing to conduct real-world vulnerability assessments and risk validations. This simulated testing environment utilizes the SPIDER 5G [29] cyber range along with UPRC's Capture The Flag (CTF) platforms, including CTFd, CTFlib, and FaustCTF, to gamify and score the testing processes. This modular environment is designed to provide isolated modules for different protocols, device configurations, and network structures, thus enabling comprehensive testing and risk analysis in a controlled setting.

Cascading attack analysis is crucial for identifying vulnerabilities stemming from interdependencies in 5G and IoT systems. By leveraging SPIDER H2020 and specifically the MATILDA orchestration framework and the MouseWorld 5G setup, the NITRO cyber range enables users to simulate interconnected scenarios. This feature reveals weak points across supply chains, device protocols, and infrastructure components. The modular and interoperable structure supports isolated testing of interconnected components, ensuring accurate analysis and communication between diverse systems.

The NITRO platform aims to implement adversarial AI exercises focusing on attack and defense strategies. This module simulates AI-targeted attacks within 5G and IoT environments to enhance model resilience against adversarial techniques. By utilizing datasets such as "DeepSlice" and "WSN-DS" provided by IURC, the platform can create realistic scenarios for interdisciplinary cybersecurity training. The integration of centralized orchestration ensures effective control over adversarial scenarios while maintaining privacy measures for secure data handling.

A critical component of the NITRO framework is the establishment of a comprehensive Data Repository for managing security incidents, vulnerabilities, and threats. This repository facilitates real-time incident tracking and historical analysis, employing automated tools from the SANCUS project to simulate realistic 5G traffic flows. The centralized orchestration enables efficient organization and management of incident data from a unified dashboard, while automation supports modularity, allowing individual components to simulate incidents for streamlined data collection and threat

analysis.

5.4 Distributed Deployment

Having multiple trainees use a cyber range in a distributed deployment setting is essential for effective training and realistic simulation of cyber defense and attack scenarios. Distributed deployments enable the cyber range to be scaled across multiple virtual machines or containers, making it accessible to many users at once without performance degradation. This setup is particularly important in scenarios where trainees need to collaborate on complex tasks, compete in Capture the Flag (CTF) challenges, or simulate incident response in a dynamic and shared environment.

A distributed deployment allows each trainee to have access to isolated environments, providing them with individual instances or unique roles within a shared scenario. For example, in a CTF event, each trainee or team can interact with their own instance of vulnerable systems or services, allowing them to experiment without affecting others. At the same time, having a shared, distributed infrastructure lets the cyber range host complex simulations that span multiple virtual networks and environments, giving trainees exposure to scenarios they are likely to encounter in real-world cybersecurity operations.

For trainers, distributed deployment also brings operational benefits. It enables easy scaling to accommodate many users, regardless of whether they are in the same location or distributed globally. Through orchestration tools like Kubernetes or OpenStack, trainers can spin up multiple instances of network services, applications, or entire environments, providing quick recovery, enhanced fault tolerance, and efficient resource management. Each trainee's activities can be isolated within containerized instances, making it possible to monitor their actions, track their learning progress, and assess their response to different security scenarios.

For containerized deployment, Docker is commonly used to create isolated environments for each Open5GS function. Docker Compose or Kubernetes can be used to manage multiple containers, allowing for orchestration, scaling, and load balancing of the different components. Kubernetes, in particular, offers advanced features like automatic scaling and self-healing, ensuring that if a container or service fails, it is automatically restarted or replaced. This setup also allows for the efficient use of resources, as each container can be dynamically scaled based on the demand from the cyber range training sessions.

Alternatively, Open5GS can be hosted on virtual machines (VMs) for more comprehensive isolation and dedicated resource allocation. Each Open5GS network function can be deployed on separate VMs, providing more stringent network and resource isolation between different trainees or teams. Virtual machines are particularly useful when creating separate environments for each trainee, which allows for secure and independent interactions with the system.

For large-scale deployments, the distributed nature of Kubernetes allows Open5GS components to be

easily scaled across multiple nodes in a cluster, providing high availability and fault tolerance. Trainee environments can be isolated within Kubernetes namespaces or assigned dedicated VMs, ensuring that different teams or trainees do not interfere with each other's testing. This makes it possible to run multiple independent training scenarios, each with their own instance of Open5GS, in parallel.

Furthermore, hosting Open5GS in a distributed manner allows for the use of advanced monitoring and orchestration tools to track system performance. Kubernetes integrates with Prometheus and Grafana for real-time monitoring of the Open5GS environment, while centralized logging solutions like ELK Stack provide insights into trainee activities and system performance. These capabilities ensure that trainers can manage and evaluate each trainee's actions efficiently while maintaining the integrity of the overall system.

5.5 Network Throughput and Latency Constraints

Handling increased traffic volumes often means high packet processing loads on the UPF, which routes data between devices and the internet. In a cyber range, this function must simulate conditions with minimal jitter and packet loss, replicating real 5G scenarios for applications like autonomous driving or industrial IoT. A solution is to introduce rate limiting on the UPF to prevent overloading by controlling the packet flow rate. By shaping the traffic based on predefined profiles, the system can simulate realistic data flows without overwhelming network resources. Another option is to enforce QoS policies to manage bandwidth allocation dynamically based on application needs, ensuring critical tasks maintain high throughput while less critical ones are throttled. Ensuring sufficient bandwidth, optimizing network infrastructure, and using tools like QoS policies are key to maintaining high throughput, especially when accommodating multiple trainees in a cyber range.

Latency is the delay between data transmission and reception, which is crucial for real-time applications. In Open5GS, additional network hops, virtualization overhead, and long-distance deployments can increase latency. To minimize delays, network functions should be placed as close together as possible within a data center, and edge computing can be used to reduce latency for time-sensitive applications. Edge computing and 5G network slicing are effective strategies to mitigate throughput and latency issues. By deploying network functions closer to users or devices, edge computing reduces the need for long-distance communication, cutting latency. Network slicing helps allocate dedicated resources for critical tasks, ensuring that high-priority functions maintain optimal performance despite network congestion.

NITRO 5G Cyber Range will include exercises that address the above including the network throughput and latency constraints, providing trainees with hands-on experience in managing real-world 5G network conditions. These exercises will encompass a variety of scenarios, such as optimizing performance under high traffic, mitigating latency impacts, and defending against cyberattacks.

5.6 Database Scalability and Subscriber Management

In a large-scale cyber range simulation, where potentially thousands of devices and user profiles are

active, managing this database becomes increasingly challenging. The database must support rapid read and write operations for authentication, session establishment, and handover processes as devices move through different network areas. Scaling this database horizontally to manage more users and achieve high availability can be complex and may require sharding techniques to prevent bottlenecks in read/write operations.

5.7 Cybersecurity Mechanisms

The NITRO platform integrates a suite of advanced cybersecurity measures and comprehensive access management protocols. These mechanisms (Table 9) provide real-time monitoring, threat detection, and incident response capabilities, ensuring that the integrity and confidentiality of network operations are maintained. Additionally, the implementation of network slicing allows for the segmentation of services, enhancing security by isolating different applications and user groups. The training content will leverage simulated environments that reflect the complexities of 5G networks, allowing learners to explore various attack vectors and defense strategies in a controlled setting.

Security Mechanism	Description	Implementation in NITRO
Firewall	Filters network traffic, allowing or blocking data packets based on predefined security rules.	Network firewalls implemented at entry and exit points to monitor traffic.
Intrusion Detection & Prevention System (IDPS)	Detects and responds to unauthorized activities or potential threats by monitoring network traffic for known attack patterns or anomalies.	Integrated to monitor Open5GS network traffic for real-time threat alerts.
Security Information & Event Management (SIEM) Log Monitoring	Collects and analyzes security logs and events to detect potential threats, ensuring compliance and facilitating forensic analysis.	Logs from Open5GS to a SIEM system for central monitoring and analysis.
Access Management	Ensures that only authorized users have access to critical network resources, reducing unauthorized access risks.	Implements role-based access control and authentication protocols in Open5GS.
Network Slicing	Isolates network slices to prevent cross-slice attacks, allowing each slice to have dedicated security policies and configurations.	Allows secure, isolated services within Open5GS for different application needs.
Network Rate Limiting	Controls the flow of data packets to prevent network overloads and mitigate DDoS attack impacts.	Rate-limiting rules can be configured to throttle excessive traffic in Open5GS.
End-to-End Encryption	Encrypts data packets from sender to receiver, protecting data confidentiality in transit.	Open5GS supports encryption mechanisms (e.g., IPsec) to secure data transmission.
DDoS Protection	Detects and mitigates distributed denial of service attacks by filtering malicious traffic and rate-limiting.	DDoS protection involves traffic filtering and automated response.

Table 9. List of Cybersecurity Mechanisms to be Integrated on the NITRO 5G Cyber Range

6 Conclusion

In conclusion, in this Deliverable the architecture for the NITRO 5G Cyber Range has been presented,

ensuring its effectiveness and reliability in simulating cybersecurity scenarios specific to 5G and IoT environments. The deliverable provides a detailed overview of the system architecture, highlighting its seamless integration with existing 5G infrastructures while offering the flexibility to simulate various cyber threat scenarios. This framework ensures that stakeholders can effectively assess the security posture of interconnected systems, facilitating the identification of vulnerabilities and the development of robust countermeasures. By emphasizing the modularity and scalability of the NITRO Cyber Range, the deliverable aims to support diverse training scenarios and user requirements.

A key component of the deliverable is its focus on the core functionalities of the NITRO Cyber Range, which include simulating real-world cyber threat scenarios and conducting vulnerability assessments. By creating a controlled environment, the platform enables researchers and security professionals to train on effective defense strategies tailored to 5G and IoT systems. The deliverable describes how the cyber range can emulate different network architectures and IoT device configurations, providing in-depth analyses of various attack vectors. This focus on realistic simulations not only enhances training outcomes but also contributes to a deeper understanding of the interconnected vulnerabilities inherent in modern digital ecosystems.

The scope of Deliverable D2.2 also addresses the integration principles essential for ensuring the NITRO Cyber Range's compatibility with current infrastructures, particularly regarding interoperability with 5G networks and IoT devices. It discusses the importance of effective data flows and interactions among system components, as well as the strategies for scaling the platform to accommodate an increasing number of users and devices without compromising performance. Additionally, the deliverable outlines integrated cybersecurity mechanisms designed to protect against potential threats during training exercises, creating a secure environment for users. Overall, this deliverable serves as a foundational document, establishing a clear roadmap for the implementation and future development of the NITRO Cyber Range in the evolving landscape of cybersecurity training and testing.

7 References

- [1] Farao, A., Ntantogian, C., Karagiannis, S., Magkos, E., Dritsa, A., & Xenakis, C. (2024, July). NITRO: an Interconnected 5G-IoT Cyber Range. In *Proceedings of the 19th International Conference on Availability, Reliability and Security* (pp. 1-6).
- [2] Kaur, G., Goyal, R. K., & Mehta, R. (2024, March). Impact of Inter-Next Generation Node B (gNB) Distance on End-User Applications in 5G Networks. In *International Conference on Power Engineering and Intelligent Systems (PEIS)* (pp. 289-298). Singapore: Springer Nature Singapore.
- [3] Goshi, E., Jarschel, M., Pries, R., He, M., & Kellerer, W. (2021, October). Investigating inter-nf dependencies in cloud-native 5g core networks. In *2021 17th International Conference on Network and Service Management (CNSM)* (pp. 370-374). IEEE.
- [4] Silveira, L. B., de Resende, H. C., Both, C. B., Marquez-Barja, J. M., Silvestre, B., & Cardoso, K. V. (2022). Tutorial on communication between access networks and the 5G core. *Computer Networks*, 216, 109301.

- [5] Santos, G. A., da Costa, J. P. J., & da Silva, A. A. S. (2023, November). Towards to Beyond 5G Virtual Environment for Cybersecurity Testing in V2X Systems. In 2023 Workshop on Communication Networks and Power Systems (WCNPS) (pp. 1-7). IEEE.
- [6] A. Güngör, "UERANSIM: Open source 5G UE and RAN (gNodeB) implementation." [Online]. Available: <https://github.com/aligungr/UERANSIM>
- [7] K. Gokarlan, Y. S. Sandal, and T. Tugcu, "Towards a urllc-aware " programmable data path with p4 for industrial 5g networks," in 2021 IEEE International Conference on Communications Workshops (ICC Workshops). IEEE, 2021, pp. 1–6
- [8] Fonyi, S. (2020). Overview of 5G security and vulnerabilities. The Cyber Defense Review, 5(1), 117-134.
- [9] Sullivan, S., et al. "5G security challenges and solutions: a review by OSI layers." IEEE Access 9 (2021): 116294-116314.
- [10] Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." Computers & Security 88 (2020): 101636.
- [11] Zolotukhin, Mikhail, et al. On attacking future 5g networks with adversarial examples: Survey. Network 3.1 (2022): 39-90.
- [12] Apruzzese, G., Colajanni, M., Ferretti, L., Guido, A., & Marchetti, M. (2018). On the effectiveness of machine and deep learning for cyber security. In 2018 10th International Conference on Cyber Conflict (CyCon) (pp. 371-390). IEEE.
- [13] Chicaiza, Janneth, et al. "Application of data anonymization in Learning Analytics." Proceedings of the 3rd International Conference on Applications of Intelligent Systems. 2020.
- [14] Attaran, Mohsen. "The impact of 5G on the evolution of intelligent automation and industry digitization." Journal of ambient intelligence and humanized computing 14.5 (2023): 5977-5993.
- [15] Basu, Deborsi, Raja Datta, and Uttam Ghosh. "Softwarized network function virtualization for 5g: Challenges and opportunities." Internet of Things and Secure Smart Environments (2020): 147-192.
- [16] Sicari, Sabrina, Alessandra Rizzardi, and Alberto Coen-Porisini. "5G In the internet of things era: An overview on security and privacy challenges." Computer Networks 179 (2020): 107345.
- [17] Zhang, Chuan, et al. "Artificial intelligence for 5G and beyond 5G: Implementations, algorithms, and optimizations." IEEE Journal on Emerging and Selected Topics in Circuits and Systems 10.2 (2020): 149-163.
- [18] Vakaruk, S., Mozo, A., Pastor, A., & López, D. R. (2021, July). A digital twin network for security training in 5G industrial environments. In 2021 IEEE 1st International Conference on Digital Twins and Parallel Intelligence (DTPI) (pp. 395-398). IEEE.
- [19] Butun, I., Österberg, P., & Song, H. (2020). Security of the internet of things: Vulnerabilities, attacks, and countermeasures. IEEE Communications Surveys & Tutorials, 22(1), 616-644.
- [20] Benzaid, Chafika, and Tarik Taleb. "AI for beyond 5G networks: A cyber-security defense or offense enabler?." IEEE network 34.6 (2020): 140-147.
- [21] Chicaiza, Janneth, et al. "Application of data anonymization in Learning Analytics." Proceedings of the 3rd International Conference on Applications of Intelligent Systems. 2020.

- [22] Jones, Kyle ML, et al. "'We're being tracked at all times': Student perspectives of their privacy in relation to learning analytics in higher education." *Journal of the Association for Information Science and Technology* 71.9 (2020): 1044-1059.
- [23] van Steen, T., & Deeleman, J. R. (2021). Successful gamification of cybersecurity training. *Cyberpsychology, Behavior, and Social Networking*, 24(9), 593-598.
- [24] Khairallah, Obay, and Ma'moun Abu-Naseer. "The effectiveness of gamification teaching method in raising awareness on Email Phishing: Controlled Experiment." (2024).
- [25] Tseng, Shih-Lun "Allen, et al. "Rethinking Gamification Failure: A Model and Investigation of Gamified System Maladaptive Behaviors." *Information Systems Research* (2023).
- [26] Yadav, R.; Sousa, E.; Callou, G. Performance comparison between virtual machines and docker containers. *IEEE Lat. Am. Trans.* 2018, 16, 2282–2288
- [27] Salazar, Z.; Nguyen, H.N.; Mallouli, W.; Cavalli, A.R.; Montes de Oca, E. 5Greplay: A 5G network traffic fuzzer—application to attack injection. In *Proceedings of the 16th International Conference on Availability, Reliability and Security*, Vienna, Austria, 17–20 August 2021; pp. 1–8.
- [28] Glas, Magdalena, Gerhard Messmann, and Günther Pernul. "Complex yet attainable? An interdisciplinary approach to designing better cyber range exercises." *Computers & Security* (2024): 103965.
- [29] Rebecchi, F., Pastor, A., Mozo, A., Lombardo, C., Bruschi, R., Aliferis, I., ... & Xenakis, C. (2022, June). A digital twin for the 5G era: The SPIDER cyber range. In *2022 IEEE 23rd International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)* (pp. 567-572). IEEE.