B5G/6G Cyber Security Testbed

Alessandro Carrega*† Franco Davoli*† Ramin Rabbani†

* Department of Electrical, Electronic and Telecommunications Eng., and Naval Architecture (DITEN)
University of Genoa (UniGe), Italy {*name*}.{*surname*}@unige.it

† National Laboratory of Smart and Secure Networks (S2N) of the
National Inter-university Consortium for Telecommunications (CNIT), Genoa, Italy {*name*}.{*surname*}@cnit.it

***Abstract*—The evolution of mobile communication technologies to Beyond 5G (B5G) and Sixth-Generation (6G) introduces significant advancements but also new cybersecurity vulnerabilities. This paper details the National Inter-university Consortium for Telecommunications (CNIT) National Laboratory of Smart and Secure Networks (S2N) testbed in Genoa, Italy, a state-of-the-art facility for research and development in B5G/6G technologies with a focus on cybersecurity. The testbed's modular architecture, including isolated "*islands*" and advanced HardWare/SoftWare (HW/SW), enables the simulation and analysis of cyber threats like Application Programming Interface (API) exposure, and Distributed Denial of Service (DDoS) attacks. It supports the testing of security measures, including Artificial Intelligence (AI)/Machine Learning (ML)-based solutions, and facilitates comprehensive vulnerability assessments and penetration testing for next-generation networks.**

***Index Terms*—B5G, 6G, Cybersecurity, Testbed, Network Security**

I. Introduction

The evolution of mobile communication technologies has progressed from the First-Generation (1G) to the anticipated Sixth-Generation (6G). Each generation has introduced significant advancements in terms of speed, capacity, and connectivity. Fifth-Generation (5G) and 6G technologies are poised to revolutionize the telecommunications landscape by enabling ultra-reliable low-latency communications, massive machine-type communications, and enhanced mobile broadband. These advancements are driven by the increasing demand for high-speed data transmission, the proliferation of Internet of Things (IoT) devices, and the need for seamless connectivity across various platforms.

Beyond 5G (B5G) and 6G technologies are characterized by their use of higher frequency bands, including millimeter waves and terahertz frequencies, which facilitate higher data rates and lower latency. The integration of Artificial Intelligence (AI) and Machine Learning (ML) into network management and operations is also a hallmark of these technologies, enabling more efficient resource allocation and improved user experiences.

As the complexity and interconnectivity of networks increase, so do the vulnerabilities and potential attack vectors. Cybersecurity has become a paramount concern in the deployment of 5G and 6G networks. The integration of diverse technologies, such as IoT devices, autonomous systems, and cloud computing, introduces new challenges in safeguarding sensitive data and ensuring the integrity of network operations.

Cyber threats can manifest in various forms, including denial-of-service (DoS) attacks, data breaches, and Advanced Persistent Threats (APTs). The consequences of such attacks can be catastrophic, leading to service disruptions, financial losses, and reputational damage. Therefore, robust cybersecurity measures are essential to protect the integrity, confidentiality, and availability of network services.

The National Inter-university Consortium for Telecommunications (CNIT) - National Laboratory of Smart and Secure Networks (S2N) has established a state-of-the-art testbed designed to facilitate research and development in 5G and 6G technologies, with a particular focus on cybersecurity. This test-bed provides a controlled environment for testing new protocols, applications, and security measures, enabling researchers to simulate real-world scenarios and evaluate the performance of various technologies.

The CNIT – S2N Testbed (CST) is equipped with advanced HardWare (HW) and SoftWare (SW) components, allowing for the emulation of complex network topologies and the integration of various cybersecurity frameworks. This infrastructure supports a wide range of use cases, from testing the resilience of network components to evaluating the effectiveness of security protocols in mitigating cyber threats.

II. B5G/6G Testbed Architecture

The CST in Genoa, Italy, serves as a comprehensive facility for experimenting with B5G and 6G, Edge, and Cloud Computing technologies. This multi-layered HW and SW platform, shown in Figure 1, is specifically designed to host multiple isolated environments, known as "*islands,*" which can emulate complete B5G/6G network setups. The testbed is also part of different European Horizon 2020 (H2020) projects like Holistic, Omnipresent, Resilient Services for future 6G wireless and computing Ecosystems (HORSE)[1], A Lightweight Software Stack And Synergetic Meta-Orchestration Framework For The Next Generation Compute Continuum (NEPHELE)[2], Programmable, Modular and Disaggregated Security Plane for 6G Ecosystems (MARE)[3] [1], and Scientific LargeScale Infrastructure for Computing/Communication Experimental Studies (SLICES) [2].

[1]horse-6g.eu
[2]https://nephele-project.eu
[3]https://mare6g.eu/

Figure 1: Testbed installation.

The architecture of the CST is designed to be modular and scalable, accommodating a variety of research needs. Key components of the testbed include:

Network Infrastructure
: The testbed features a high-speed backbone network that supports multiple access technologies, including fiber optics, millimeter-wave links, and wireless connections. This infrastructure enables the simulation of diverse network scenarios and the evaluation of performance metrics.

Computational Resources
: High-performance computing resources are integrated into the testbed to support data-intensive applications and complex simulations. These resources facilitate the execution of AI algorithms and machine learning models for network optimization and security analysis.

Security Frameworks
: The testbed incorporates various cybersecurity frameworks, including intrusion detection systems (IDS), firewalls, and encryption protocols. These components are essential for testing the resilience of network services against cyber threats.

The testbed's infrastructure integrates both general and special-purpose equipment to create underlying B5G/6G network foundations and related slices, alongside edge-cloud computing resources. Its HW capabilities include 35 servers, 8 high-speed switches, various base stations such as 2x Amarisoft Callbox 5G[4] gNodeB (gNB) Multiple Input Multiple Output (MIMO) 4x4 and Open RAN (O-RAN) units, an Amarisoft 5G User Equipment (UE) Emulator[5], *NVIDIA* A100 Graphical Processing Units (gpus)[6], a *P4*[7] (*Tofino*[8]-enabled) switch, power monitors, HW traffic generators, HW firewalls, and 12 UE devices. For SW, the testbed utilizes OpenStack (OS)[9], Open Source MANO (OSM)[10], Kubernetes (k8s)[11], Fourth-Generation (4G)/5G and networking Virtual Network Functions (VNFs), Data Plane Development Kit (DPDK)[12]-based delay and packet loss emulation, and an Open Network Operating System (ONOS)[13] Software-Defined Networking (SDN) Controller [3]. An observability stack, including *Prometheus*[14] and Elasticsearch, Logstash and Kibana (ELK)[15], is also in place for monitoring. The physical topology, illustrated in Figure 2, uses a network of switches with speeds from $10\,\mathrm{Gbit}ps$ to $100\,\mathrm{Gbit}ps$. Connectivity for each isolated island is managed through dedicated Virtual Routing and Forwarding (VRF) instances, with an internal firewall preventing traffic exchange between islands. An external firewall manages connectivity to the public Internet. A direct link to the national research network (Gruppo per l'Armonizzazione della Rete della Ricerca (GARR)[16]) will also be established to interconnect the testbed with external facilities [4].

The testbed is managed flexibly using a Metal as a Service (MaaS) approach, supporting OS and k8s instances. A meta-orchestrator, comprising the Metal Convergence Layer (MetalCL) and the NFV Convergence Layer (NFVCL), handles the creation and lifecycle management of these isolated environments. MetalCL uses Canonical MaaS [5] for bare-metal server provisioning and Ansible [6] for SW installations and operating system reconfiguration. A Python service called Network Convergence Layer (NetCL) automates the discovery of the physical topology and configures overlay networks using Virtual LANs (VLANs) to ensure seamless hosting and isolation for OS and k8s. MetalCL's capabilities extend to managing federated infrastructures as "*zones,*" each with different programmability levels, as depicted in Figure 3.

The NFVCL provides a high-level abstraction for orchestrating network services, VNFs, and Parallel Network Functions (PNFs) within the 5G infrastructure, allowing for the dynamic creation and management of complete network environments like a B5G/6G core network [7]. It utilizes *blueprints* as deployment templates and can instantiate network services, select computing facilities, and attach network functions [8]. The entire procedure involving both MetalCL and NFVCL is shown in Figure 4.

The design and capabilities of the CST make it highly suitable for cybersecurity projects [9], especially in the context of B5G/6G networks [10]. The fundamental concept of "*isolated islands,*" as illustrated in Figure 5, is crucial, as it allows researchers to deploy and test cybersecurity solutions within a confined and secure environment without impacting other experiments. The internal firewall directly ensures this isolation by preventing inter-island traffic. The ability to commission

[4]https://www.amarisoft.com/test-and-measurement/device-testing/device-products

[5]https://www.amarisoft.com/test-and-measurement/network-testing/network-products

[6]https://www.nvidia.com/it-it/data-center/a100

[7]https://p4.org

[8]https://www.intel.com/content/www/us/en/products/details/network-io/intelligent-fabric-processors/tofino.html

[9]https://www.openstack.org

[10]https://osm.etsi.org

[11]https://kubernetes.io

[12]https://www.dpdk.org

[13]https://opennetworking.org/onos

[14]https://prometheus.io

[15]https://www.elastic.co/elastic-stack

[16]https://www.garr.it/en

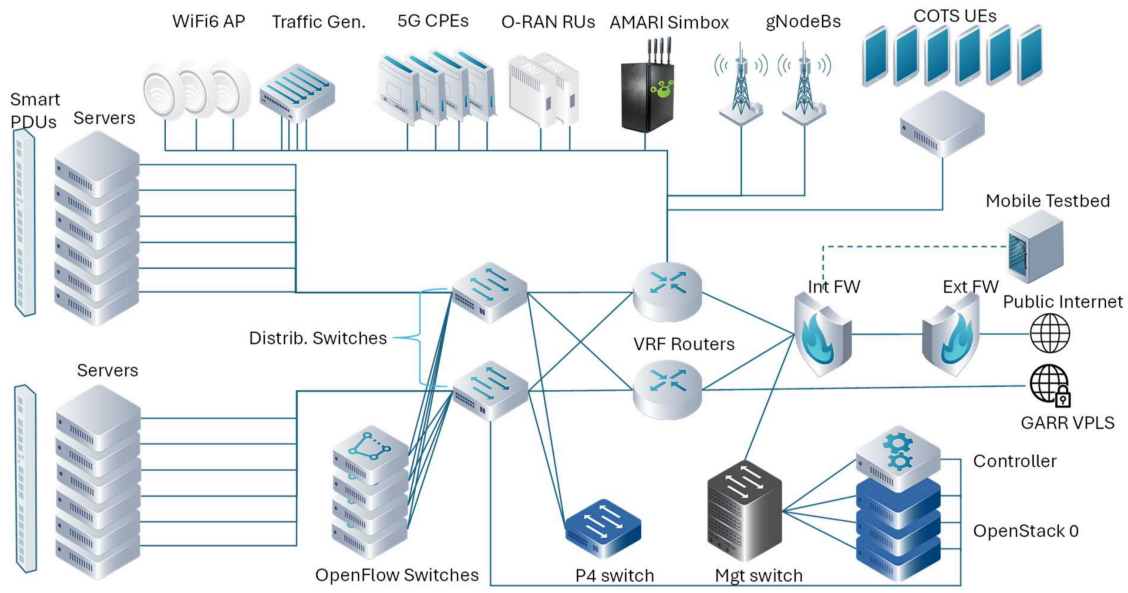

Figure 2: The physical infrastructure of the CST.

and configure bare-metal resources through MetalCL offers maximum programmability, essential for setting up specific test scenarios for security vulnerabilities or deploying custom security tools.

Furthermore, the NFVCL's capacity to build and manage complete network environments, including a 5G core as expanded in Figure 6 enables the deployment and testing of security functions as VNFs. The CST's support for Bring Your Own Network Function (BYONF) allows cybersecurity researchers to develop and integrate their own custom security network functions (xNFs), providing a flexible platform for innovation in network security. The presence of HW traffic generators and the observability stack (*Prometheus*, ELK) is vital for cybersecurity research, enabling the simulation of various attack types and the real-time monitoring of network behaviour and security events. This allows for thorough testing of intrusion detection systems, firewalls, and other security mechanisms. The *P4* switch offers programmability at the data plane, which can be leveraged for implementing advanced security policies and real-time threat mitigation directly within the network. Lastly, the availability of site-to-site and client-server Virtual Private Networks (VPNs) ensures secure remote access for researchers, which is paramount when dealing with sensitive cybersecurity experiments [11].

The CST is designed to seamlessly integrate with existing cybersecurity frameworks, allowing researchers to evaluate the effectiveness of different security measures in real-time. This integration enables the testing of various security protocols, such as Transport Layer Security (TLS), Secure Socket Layer (SSL), and Advanced Encryption Standard (AES).

Moreover, the testbed supports the implementation of ML-based security solutions, which can adapt to evolving threats and enhance the overall security posture of the network. By leveraging AI and ML, researchers can develop predictive models that identify potential vulnerabilities and recommend proactive measures to mitigate risks.

Therefore, from the point of view of cybersecurity, the CST supports a wide range of use cases and applications, including:

Vulnerability Assessment
Researchers can conduct comprehensive assessments of network components to identify potential vulnerabilities and evaluate the effectiveness of security measures.

Penetration Testing
The testbed allows for controlled penetration testing, enabling researchers to simulate cyber-attacks and assess the resilience of network services against various threat vectors.

Performance Evaluation
The testbed facilitates the evaluation of network performance under different conditions, including varying traffic loads and attack scenarios. This information is crucial for optimizing network configurations and enhancing security measures.

III. Use Cases of the CST in Cybersecurity

The CST is designed for a wide range of use cases, from vulnerability research to testing new network functions. Its core strength is its flexibility and ease of use for experimenters. Through a MaaS approach, the testbed automates the entire setup process. A user simply declares the HW and SW they need, and the testbed management application automatically provisions the resources, installs the OS, and configures the required software components. This allows for rapid and reproducible deployment of complex environments, such as those involving VNFs, SDN switches, and radio devices. Users can then interact with the provisioned testbed using standard

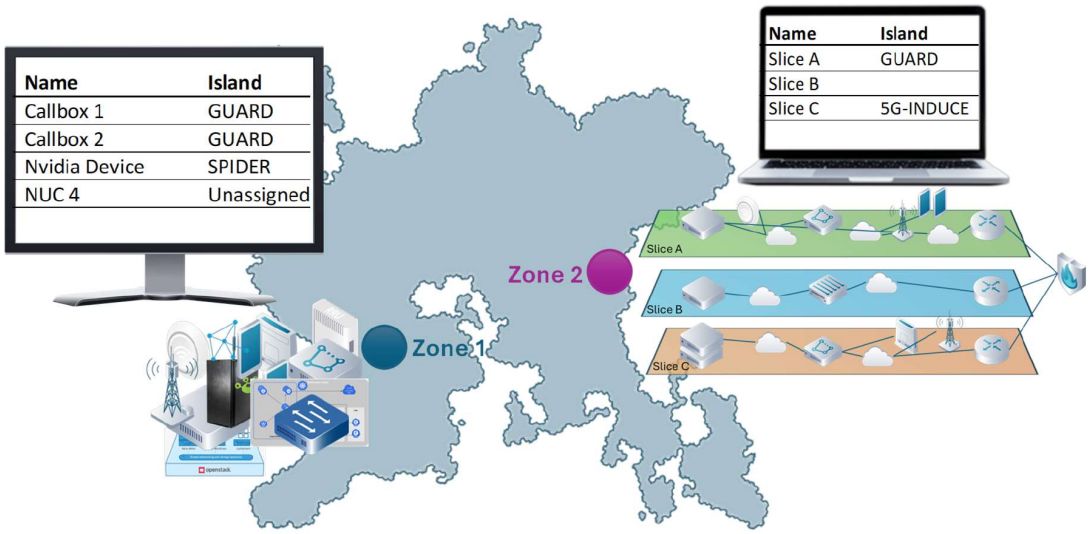

Figure 3: Example of two zones over a geographical area with different programmability levels, Zone 1 exposing programmability at MaaS level and Zone 2 exposing a catalogue of slices.

interfaces, including web-based user interfaces for manual control and REST-based Application Programming Interfaces (APIs) for automated testing. This streamlined process reduces the complexity and time typically required to set up such environments, making it easy for researchers and developers to focus on their experiments. The testbed's design allows for dedicated, isolated instances for each experiment, ensuring that different research projects do not interfere with each other. This is critical for reliable and repeatable results, whether the goal is to assess the security of a 5G core network, evaluate AI-based threat detection mechanisms, or simulate new types of cyber-physical attacks.

The CST is evolving to meet the security challenges of 5G and 6G by focusing on a holistic approach that bridges the gap between cyber and physical domains. The core of this evolution lies in the integration of new technologies and methodologies. To handle the increased complexity and data traffic, the testbed is incorporating advanced capabilities like digital twins for central coordination and control, and improving spectrum aggregation for faster data access. It is moving towards a more open and programmable infrastructure to reflect the future of 6G networks. Key areas of focus for the testbed include the development of new authentication and cryptography systems to address emerging threats, such as those posed by quantum computing. It is also expanding its capacity for security assurance and vulnerability research, with a strong emphasis on testing AI and machine learning-based solutions for threat detection and mitigation. The testbed's modular design, which allows for isolated experiments, is crucial for simulating and analyzing new types of cyber-attacks, including those that target the new interfaces and APIs that will be common in 6G. By focusing on these areas, the testbed aims to stay ahead of the curve, ensuring that future network infrastructure is resilient and secure.

Two illustrative use cases, API Exposure and Distributed Denial of Service (DoS) attacks, demonstrate how the testbed simplifies the detection and mitigation of complex threats.

A. *API Exposure*

In modern network architectures, especially within B5G/6G, APIs are exposed to enable various services and functionalities, such as those provided by the Network Exposure Function (NEF). However, these exposed APIs can become targets for malicious actors seeking to retrieve sensitive information, like user traffic routing, device location, or mobility events. Such information gathering is often the initial phase of an eavesdropping attack, which is particularly critical and dangerous in industrial scenarios. In particular, the HORSE framework, validated on the CST, considers brute-force-based attacks on these APIs as a threat that can be identified by a Detector and Mitigation Engine (DEME).

The CST facilitates the simulation and analysis of API exposure attacks by providing a controlled and isolated environment. Researchers can deploy realistic B5G/6G core network components, including the NEF, within a dedicated "*island*". The Smart Monitoring (SM) module within the HORSE framework, operating on the CST, continuously collects log data related to API interactions. This data is then pre-processed and fed to the DEME, which is responsible for detecting anomalies indicative of brute-force attacks or unauthorized access attempts. The testbed's programmability allows for the dynamic configuration of network functions

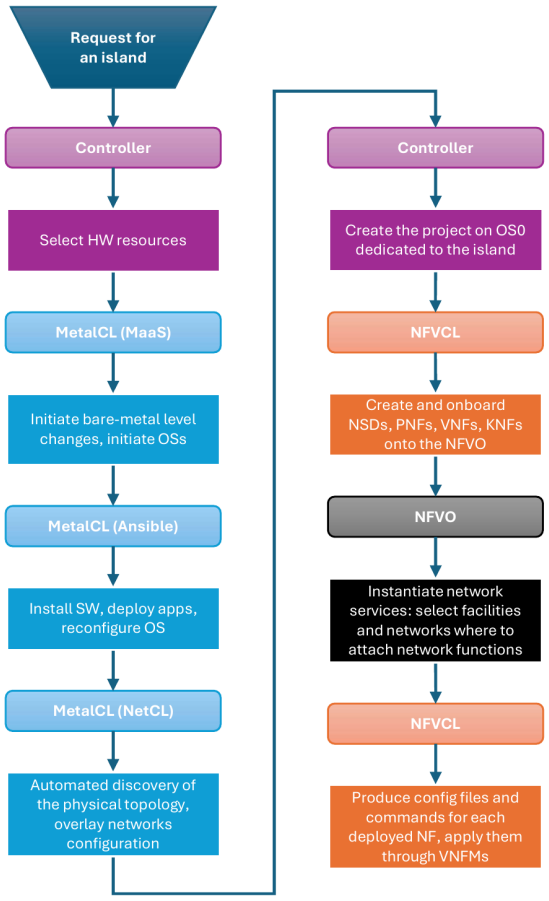

Figure 4: Flow diagram representing the steps performed by the MetalCL and the NFVCL to setup the infrastructure component and networking of an island in the CST.

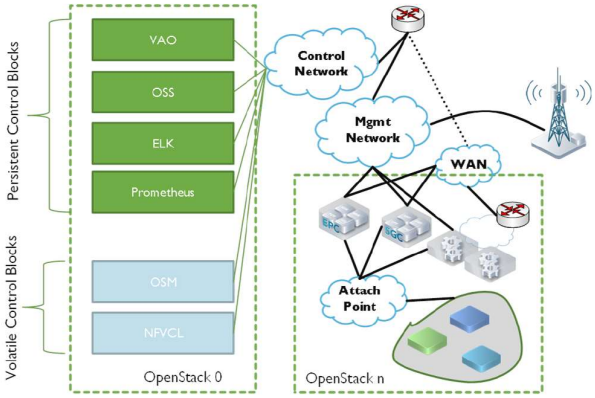

Figure 5: Example of an island architecture and interfaces.

and API endpoints, enabling precise replication of attack vectors. Once an API exposure is detected, the Distributed Trustable AI Engine (DTE) can generate intents for prevention or mitigation, which are then translated into actionable commands by the Intent-Based Interface (IBI). The CST ability to

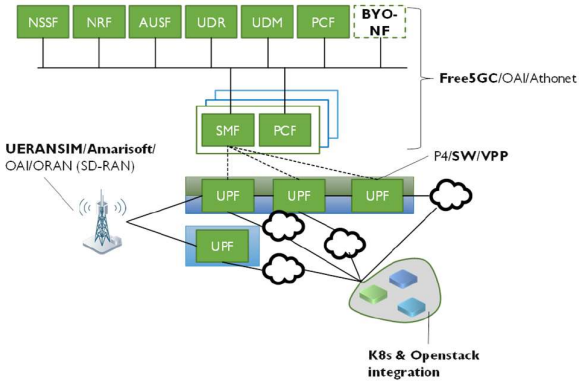

Figure 6: Deployment of a core in the example island.

enforce these actions, such as filtering malicious API requests or modifying access policies, is crucial for validating the effectiveness of the deployed cybersecurity solutions.

The CST, when combined with the HORSE framework, allows for the precise evaluation of cybersecurity solutions against API exposure threats. Measurable results, as exemplified in Figure 7, can include the detection accuracy of brute-force attacks on exposed APIs, quantifiable by metrics like true positives, false positives, and detection latency. In more detail, Figure 7 shows a graph comparing the number of requests over time with and without the HORSE framework. The blue line, representing the scenario without HORSE, exhibits a steady increase in requests before peaking and remaining consistently high. In contrast, the lighter blue line, representing the scenario with HORSE, shows the number of requests dropping significantly after reaching a certain threshold, demonstrating the framework's effectiveness in mitigating the attack. This visual example illustrates how the testbed can provide measurable results, such as detection accuracy and the effectiveness of security solutions.

Researchers can observe the effectiveness of proposed mitigation strategies, such as the reduction in unauthorized API calls post-intervention, and measure the residual impact on legitimate API traffic. Furthermore, the overhead introduced by the security mechanisms on network performance can be assessed. This comprehensive validation ensures the robustness and efficiency of security countermeasures before deployment in real-world B5G/6G environments, providing concrete evidence of the testbed's utility.

In addition to the qualitative observations, the CST combined with the HORSE framework also enables quantitative evaluation of mitigation strategies. Table I summarizes representative results from an API exposure attack scenario against the NEF. During the attack, the number of API requests surged from a normal rate of 50 requests/s to 1000 requests/s, while the request success rate dropped to 10%. Once the DEME intervened, legitimate traffic recovery was observed, with the request success rate improving to 90% and malicious requests being effectively blocked. The average detection time of the

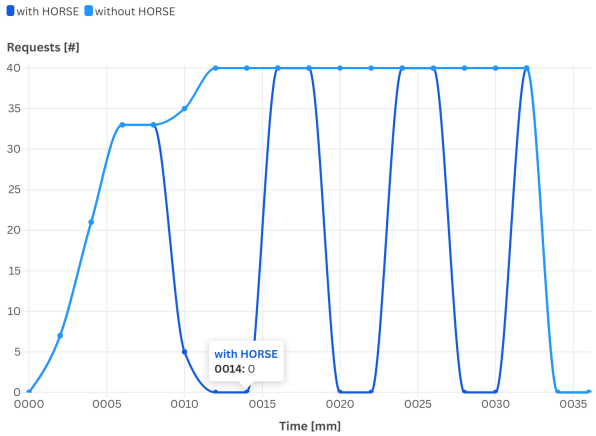

Figure 7: Example of possible results from API Exposure attack detection and mitigation in HORSE using the CST.

attack was approximately 3 seconds. Performance evaluation further indicated a false positive rate of 5% and a false negative rate of 2%, demonstrating both high detection accuracy and timely response.

TABLE I: Representative metrics for API exposure attack mitigation.

Metric	Normal Traffic	During Attack	After Mitigation
API Requests (per second)	50	1000	55
Request Success Rate (%)	100%	10%	90%
Blocked Requests (per second)	0	900	950
Average Detection Time	N/A	3 seconds	N/A
Performance			
False Positive (%)	5%		
False Negative (%)	2%		

These results highlight the testbed's ability not only to reproduce realistic attack conditions but also to provide measurable insights into the effectiveness of detection and mitigation mechanisms. In this way, the testbed contributes concrete evidence of how cybersecurity solutions perform under stress before their deployment in operational B5G/6G networks.

B. Distributed Denial of Service (DoS) Attack

DDoS attacks aim to overwhelm network resources, disrupting legitimate services. Examples include Network Time Protocol (NTP) DDoS attacks, Domain Name System (DNS) DDoS prediction and impact analysis, and multi-domain DNS DDoS attacks [12][13][14]. These attacks can originate from within the 5G network (e.g., from compromised User Equipment (UEs)) targeting external servers, or from external attackers directed towards UEs within the network. The impact can range from lowering bandwidth for malicious UEs to completely filtering out their traffic.

The CST offers a robust environment for simulating and managing DDoS attacks due to its comprehensive HW and SW stack and its isolation capabilities. The testbed's network of high-speed switches and dedicated VRF instances for each "*island*" allows for realistic traffic generation and precise attack emulation without affecting other experiments. HW traffic generators can simulate large-scale malicious traffic, while the SM module collects crucial network traffic data (e.g., Packet CAPture (PCAP) files) and system metrics for analysis. This data is then processed and fed to the Prediction and Prevention Digital Twin (P&P-DT) and Impact Analysis Digital Twin (IA-DT).

The HORSE framework, leveraging the CST, can predict DDoS attacks and analyze their potential impact using digital twin capabilities. The testbed's ability to host VNFs allows for the dynamic deployment and testing of security functions designed to detect and mitigate DDoS attacks. For instance, the DEME identifies and classifies the DDoS attack, and the DTE generates mitigation or prevention intents. These intents can lead to countermeasures like lowering bandwidth for malicious UEs or completely filtering their traffic, which are applied on routers within the infrastructure. The observability stack (Prometheus and ELK) provides real-time monitoring of network behaviour and security events, allowing researchers to assess the effectiveness of mitigation strategies. The testbed's programmability, including the *P4* (*Tofino*-enabled) switch, further enables the implementation of advanced security policies at the data plane for real-time threat mitigation. This comprehensive approach simplifies the process of testing, validating, and refining DDoS detection and mitigation actions.

TABLE II: Representative metrics for DDoS attack mitigation.

Metric	Normal Traffic	During Attack	After Mitigation
Traffic Volume (Gbps)	0.5	5	0.8
Connection Requests (per second)	500	150,000	800
Successful Connections (per second)	480	10	750
CPU Utilization on Target Server (%)	15%	95%	30%
Packet Loss (%)	1%	75%	2%
Performance			
False Positive (%)	6%		
False Negative (%)	3%		

As shown in Table II, the DDoS attack increased traffic volume tenfold (from 0.5 to 5 Gbps) and caused connection requests to surge from 500 to 150,000 per second. This led to a dramatic drop in successful connections (from 480 to just 10), while CPU utilization on the target server spiked to 95% and packet loss rose to 75%. After applying mitigation strategies within the testbed, traffic was stabilized at 0.8 Gbps, successful connections recovered to 750 per second, CPU utilization dropped to 30%, and packet loss was reduced to only 2%. These results demonstrate the testbed's effectiveness in both reproducing the severe impact of volumetric DDoS attacks and validating the efficiency of mitigation mechanisms.

IV. Practical Use Cases of the Testbed

To better illustrate the flexibility and real-world applicability of the proposed testbed, this section presents three representative use cases in distinct domains: education, industry,

and healthcare. These examples demonstrate how the testbed supports experimentation, training, and validation activities in a controlled yet realistic environment.

A. Educational Use Case: Teaching Cybersecurity Concepts

The CST provides an effective learning environment for teaching students and young researchers the fundamentals of cybersecurity in B5G/6G networks. Leveraging the concept of isolated islands, instructors can design practical exercises without interfering with other users. For instance, a class exercise may focus on Distributed DDoS attacks. Using the testbed's MetalCL and MaaS approach, the instructor deploys an isolated 5G/6G network instance, complete with servers, switches, and a core network. Hardware traffic generators simulate a large-scale DDoS originating from compromised devices, while students monitor the attack using the observability stack (Prometheus, ELK). Students are then tasked with detecting and mitigating the attack by programming advanced data-plane rules on the P4 switch or deploying custom VNFs. The real-time feedback loop offered by the observability tools allows students to evaluate the effectiveness of their countermeasures. This hands-on approach provides invaluable experience in managing and defending modern network infrastructures.

B. Industrial Use Case: Securing Smart Factories

The CST also serves as a training and validation platform for industry practitioners tasked with protecting critical infrastructures. Consider a smart factory where robots, sensors, and control systems operate over a B5G private network. A digital twin of the factory's network can be deployed on the testbed, enabling security teams to train in realistic attack-defense scenarios. One example involves simulating an API exposure attack against a production robot, requiring the team to detect and contain the threat using SDN-based mitigation strategies. Another scenario may replicate a denial-of-service attack against Automated Guided Vehicles (AGVs), disrupting supply-chain operations. Using machine learning tools integrated into the testbed, the security team can automatically classify malicious traffic and reroute legitimate flows to maintain production continuity. By reproducing these complex cyber-physical scenarios in a risk-free environment, the CST equips industrial operators with the skills to safeguard next-generation manufacturing systems.

C. Healthcare Use Case: Protecting Telemedicine Services

In healthcare, where ultra-reliable low-latency communication is critical, the CST enables the exploration of security strategies for telemedicine and remote surgery. A representative scenario involves a Man-in-the-Middle (MitM) attack on a remote surgery session, where a surgeon's console communicates with a robotic arm over a B5G/6G connection. Within the testbed, this environment can be fully emulated as an isolated island. An automated adversary attempts to intercept and manipulate data flows, while the trainees monitor anomalies using the SM module. They must then coordinate a response, such as enforcing stronger encryption protocols or dynamically rerouting traffic through secure paths. The testbed's digital twin functionality further allows "what-if" analysis, enabling trainees to test the effectiveness of different countermeasures before applying them. This approach provides healthcare IT professionals with critical skills for ensuring the safety and reliability of future telemedicine applications.

These use cases highlight how the CST testbed bridges the gap between academic training, industrial readiness, and healthcare resilience, ultimately reinforcing its role as a versatile platform for advancing cybersecurity in B5G/6G environments.

V. Conclusions

The CNIT testbed serves as a vital resource for advancing research in B5G and 6G technologies, particularly in the realm of cybersecurity. The findings underscore the importance of robust security measures in safeguarding next-generation networks against evolving cyber threats.

As B5G and 6G technologies continue to evolve, ongoing research will be essential to address emerging cybersecurity challenges. The integration of AI, the focus on IoT security, and collaboration with industry stakeholders will play crucial roles in shaping the future of cybersecurity in next-generation networks. The CNIT testbed will remain at the forefront of this research, facilitating the development of innovative solutions to enhance the security and resilience of B5G and 6G networks.

Acknowledgment

This research was supported by the H2020 HORSE (grant agreement number 101096342), NEPHELE (grant agreement number 101070487), and MARE (grant agreement number 101191436) projects.

References

[1] R. Bolla et al., "A multi-tenant system for 5/6g testbed as-a-service," in *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 2023, pp. 768–773. DOI: 10.1109/COMSNETS56262.2023.10041360

[2] S. Fdida et al., "Slices, a scientific instrument for the networking community," *Computer Communications*, vol. 193, pp. 189–203, 2022.

[3] D. Kreutz et al., "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2015. DOI: 10.1109/JPROC.2014.2371999

[4] A. Chouman, D. M. Manias, and A. Shami, "A modular, end-to-end next-generation network testbed: Toward a fully automated network management platform," *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5445–5463, 2024. DOI: 10.1109/TNSM.2024.3416031

[5] Canonical. "MAAS (Metal-as-a-Service)," Accessed: Sep. 3, 2025. [Online]. Available: https://canonical.com/maas

[6] Red Hat, Inc. "Ansible Documentation," Accessed: Sep. 3, 2025. [Online]. Available: https://docs.ansible.com

[7] I. Trrad, "5g and beyond: Evolution of wireless communication technologies," in *2025 International Conference on Frontier Technologies and Solutions (ICFTS)*, 2025, pp. 1–9. DOI: 10.1109/ICFTS62006.2025.11031933

[8] ETSI, "Network Functions Virtualisation (NFV) Release 2; Protocols and Data Models; NFV descriptors based on YANG Specification," ETSI GS NFV-SOL 006 V2.7.1, Tech. Rep., Dec. 2019.

[9] M. O. Basurto Guerrero and J. Guaña-Moya, "Cybersecurity in 5g networks: Challenges and solutions," *Revista VICTEC*, vol. 4, no. 7, 2023. DOI: 10.61395/victec.v4i7.114

[10] E. A. Kadir et al., "B5g and 6g: Next generation wireless communications technologies, demand and challenges," in *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, 2021, pp. 1–6. DOI: 10.1109/ICOTEN52080.2021.9493470

[11] A. Al-Fuqaha et al., "Internet of things: A survey on enabling technologies, protocols, and applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347–2376, 2015. DOI: 10.1109/COMST.2015.2444095

[12] K. B. Adedeji, A. M. Abu-Mahfouz, and A. M. Kurien, "Ddos attack and detection methods in internet-enabled networks: Concept, research perspectives, and challenges," *Journal of Sensor and Actuator Networks*, vol. 12, no. 4, 2023, ISSN: 2224-2708. DOI: 10.3390/jsan12040051

[13] V. Patil and S. Deore, "Ddos attack detection: Strategies, techniques, and future directions," *Journal of Electrical Systems*, vol. 20, pp. 2030–2046, Jul. 2024. DOI: 10.52783/jes.4808

[14] A. Alfatemi et al., "Advancing ddos attack detection: A synergistic approach using deep residual neural networks and synthetic oversampling," *arXiv preprint arXiv:2401.03116*, 2024. DOI: 10.48550/arXiv.2401.03116