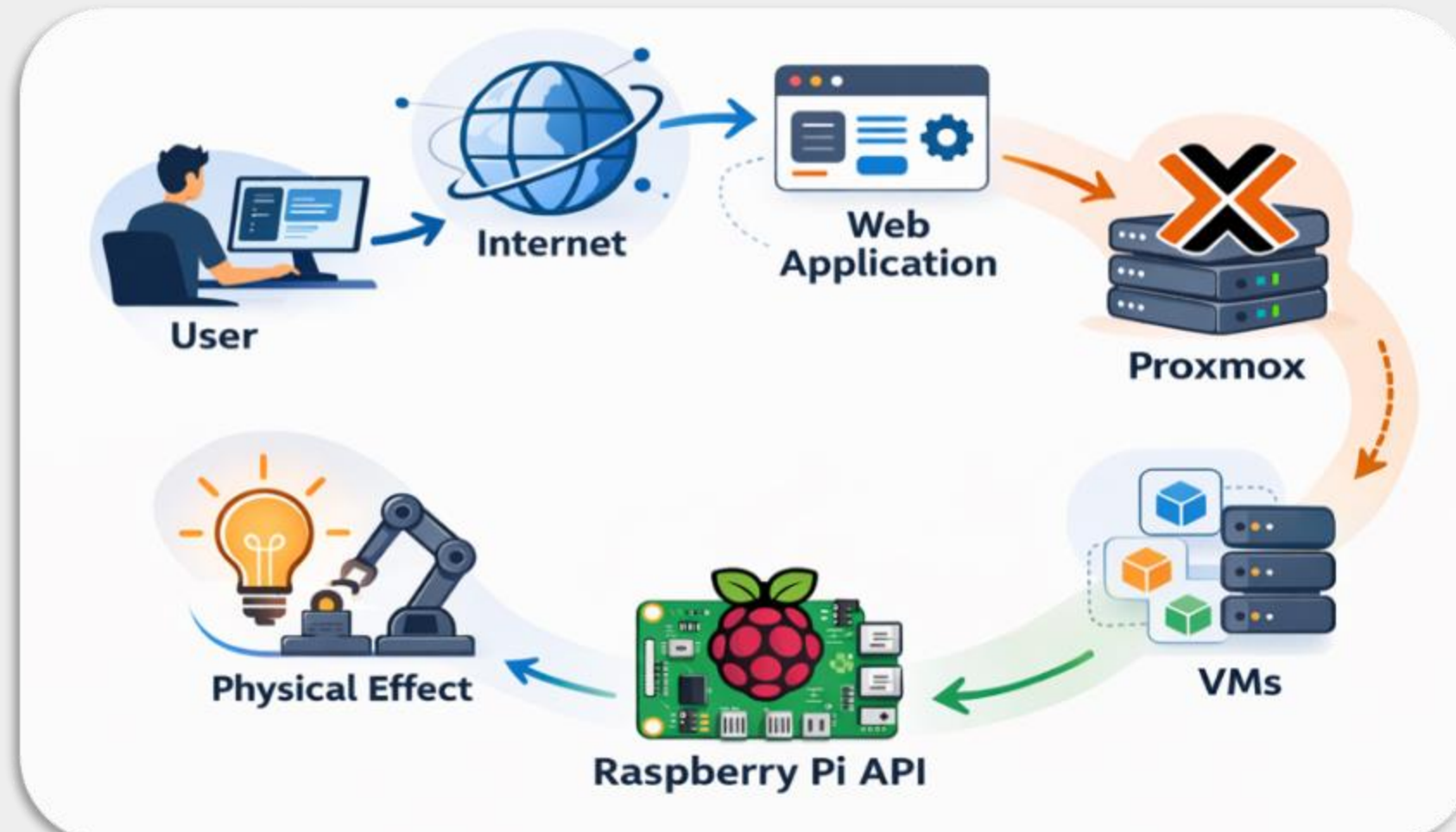


CYBER RANGE

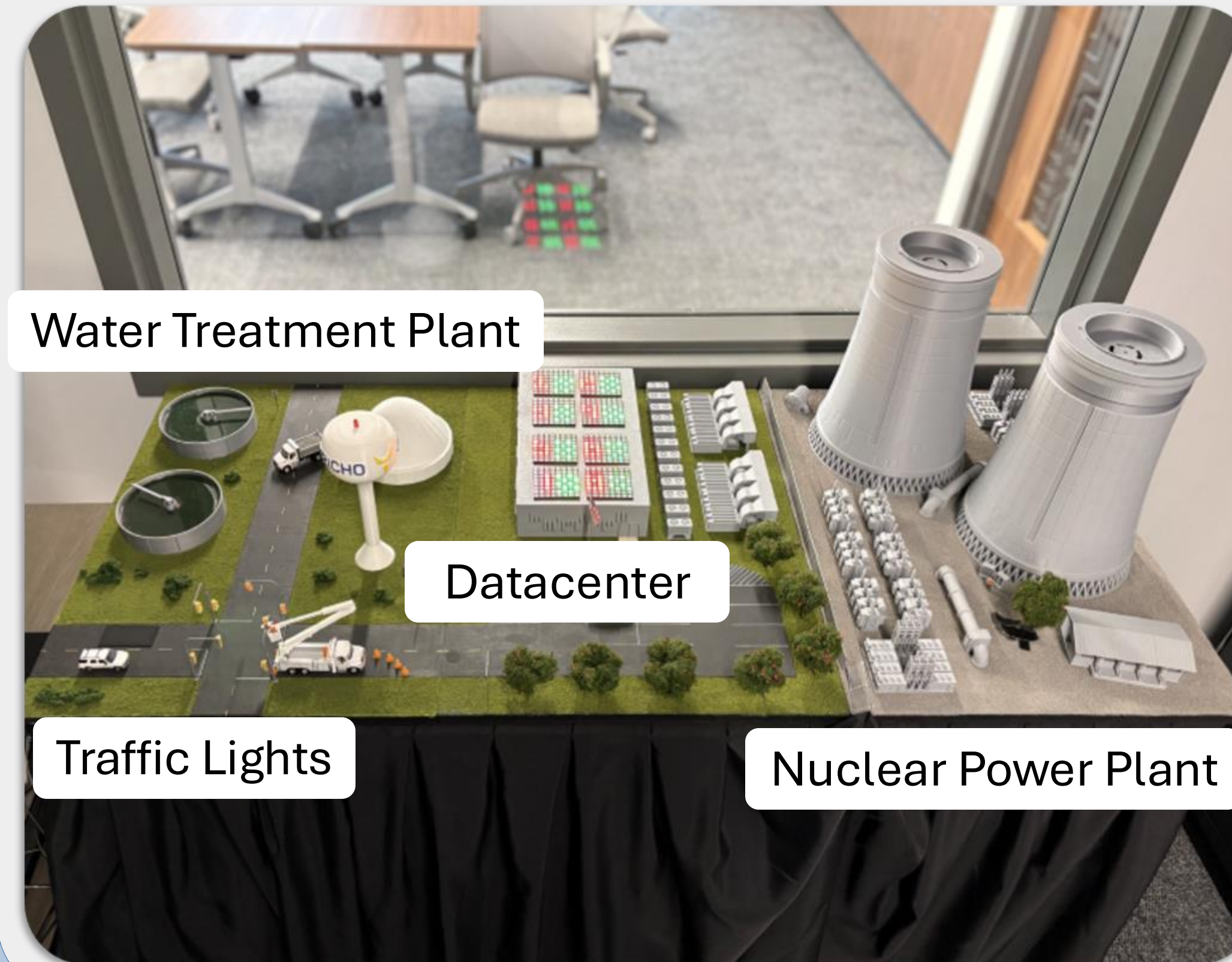
Jericho utilizes multiple layers of technology to enable users to access each of the scenarios with ease.



INFRA AUTOMATION	LUDUS CYBER RANGES
HYPERVERSOR	PROXMOX
BLADE SERVER	Lenovo



PHYSICAL INFRASTRUCTURE



ABSTRACT

Traditionally, educational institutions have conducted cybersecurity exercises exclusively in virtual environments, reducing student awareness of the profound impacts cyberattacks can have in physical space and on critical infrastructure. The Jericho project targets students from secondary education to advanced undergraduate level. Jericho drives home the potential physical space effects of cyberattacks by blending virtual computer networks with a physical city model. Other cyber-physical sandbox environments exist, but they are prohibitively expensive and found only at a few select institutions. Jericho is an affordable and scalable cyber city built using inexpensive wooden crates, Raspberry Pis, 3D printed structures, and low-cost model railroad artifacts. Additionally, Jericho's hacking scenarios are accessed through an intuitive web application ensuring that students of all ages and technical experience can master core cybersecurity competencies. Jericho's web application includes a Kali Linux virtual machine web console, a question-and-answer scoring system, and a livestream of the physical city fed by strategically placed cameras. With these features, students can complete custom-designed scenarios while simultaneously observing the effects their actions have on the physical infrastructure. Scenarios can be spun up and torn down on demand in a traditional cyber range environment that is ultimately networked with Raspberry Pis in the city capable of creating physical effects.

SCENARIOS

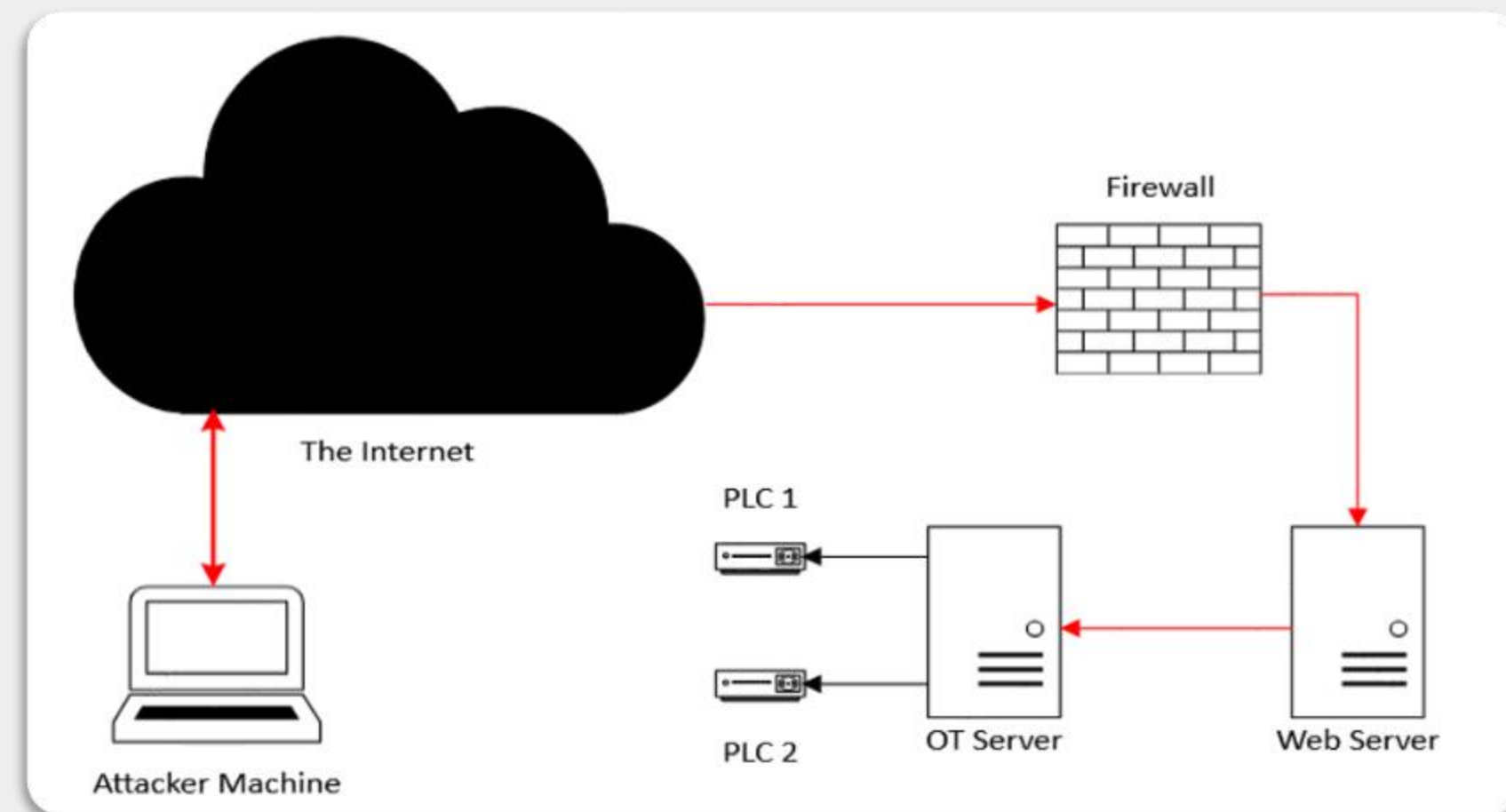
Jericho is a unique cyber education tool that allows instructors to easily create their own cyber-physical training environments and assessment tools. Through Jericho, instructors can create realistic training exercises to help their students attain specific competencies that align with their classroom instruction.

Jericho makes use of an infrastructure automation tool called Ludus, which gives instructors the capability to utilize YAML configuration files and Ansible roles to deploy fully fledged cyber ranges.

```

3 ludus:
4   - vm_name: "{{ range_id }}-demo-kali"
5     hostname: "{{ range_id }}-attacker-box"
6     template: kali-x64-desktop-template
7     vlan: 10
8     ip_last_octet: 100
9     ram_gb: 4
10    cpus: 2
11    linux:
12      packages:
13        - nmap
14        - seclists
15        - hydra
16        - curl
17        - burpsuite
18        - tmux
19        - man

```



WEB APPLICATION

Features

Kali Web Console • Live Stream • Multiple Scenarios • Scoreboard • Question & Answer • Competency Assessment

