Safe, Predictable Robot Behavior Starts With Securing Every Layer

AI-enabled robots rely on three core capabilities: perception of their environment, intelligent decision-making, and precise physical action. When any of these layers is compromised through cyberattacks or vulnerabilities, robot behavior becomes unpredictable and potentially dangerous to people, property, and operations.

Lab R7

The Robot's Five-Layer Attack Surface

Physical Layer

Exposed debug ports, USB interfaces, and unsecured firmware enable direct hardware tampering and unauthorized access to core systems.

Perception Layer

Laser attacks, acoustic noise injection, and spoofed GPS signals can distort what robots see, hear, and sense about their environment.

AI Model Layer

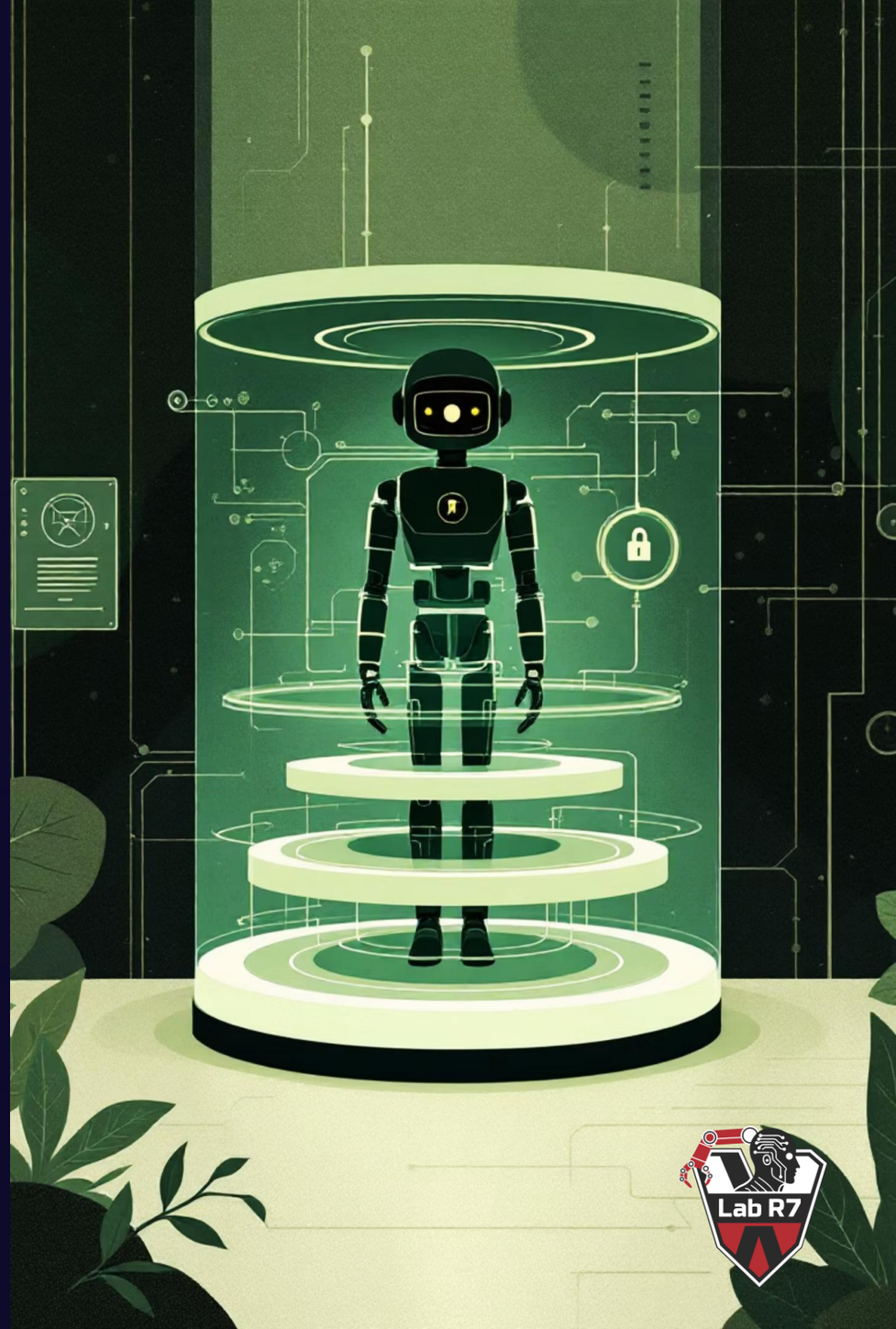
Adversarial images, poisoned training data, and backdoored models can fundamentally corrupt the robot's decision-making capabilities.

Wireless Layer

Weak Bluetooth pairing, man-in-the-middle attacks, and tampered over-the-air updates can disrupt control signals and hijack communications.

Software & Cloud Layer

ROS 2 vulnerabilities, exposed APIs, and compromised cloud services can impact entire robot fleets simultaneously across organizations.



What Causes Unpredictable or Unsafe Robot Behavior

Network Attacks

Exploiting communication protocols to intercept or manipulate robot commands.

Sensor Spoofing

Feeding false environmental data to perception systems.

Adversarial Examples

Crafted inputs designed to fool AI vision and recognition models.

Prompt Injection

Manipulating natural language interfaces to override safety controls.

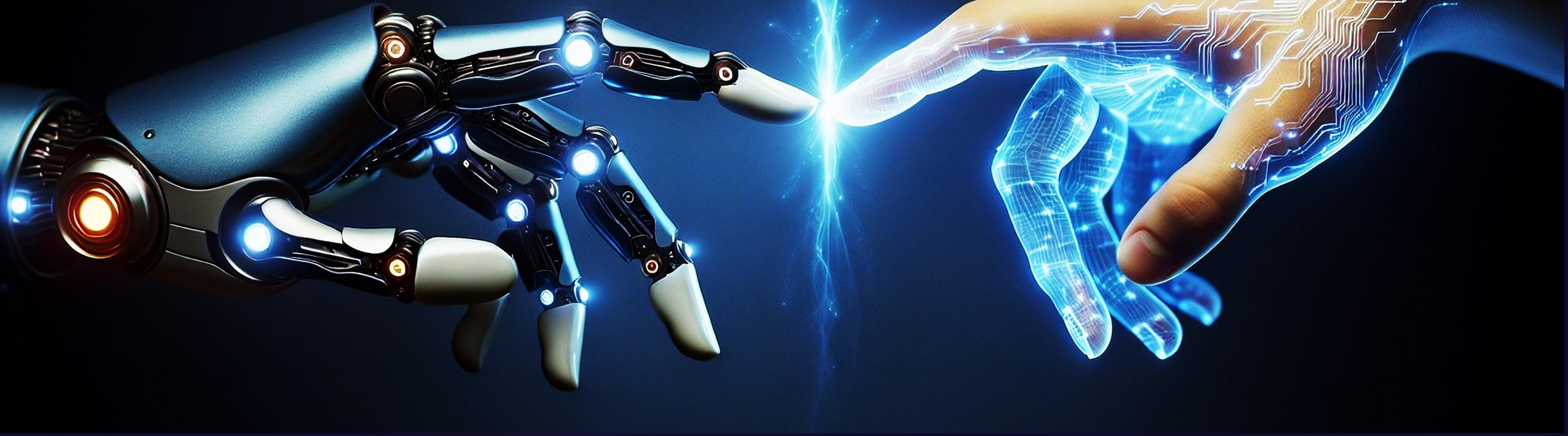
Data Poisoning

Corrupting training datasets to embed malicious behaviors.

Model Stealing

Extracting AI models to discover exploitable weaknesses.

Lab R7



The Cost of Security Gaps: Are You Prepared?

Regulatory Fines

Non-compliance with emerging regulations like the EU Cyber Resilience Act can result in market access bans and substantial financial penalties.

Brand Damage

A single high-profile cyber incident can permanently erode customer confidence and destroy partnerships that took years to build across your entire market.

Operational Disruption

Just one successful cyberattack can halt AI robot operations across facilities, cascading into supply chain failures and massive revenue losses.

Your Comprehensive Defense Strategy Awaits

Discover how our white paper equips you with:

- ✓ A Complete AI Robotic ATT&M Matrix
- ✓ A Deep Dive into the Attack Surface
- ✓ Defense Strategies for Evolving Attacks

Master Your Robotic Security

Download the full white paper today and equip your team with the knowledge to build secure, trustworthy AI robot deployments.

Download the White Paper

Lab R7