Adversarial Attacks

	Perception	Decision & Planning	Execution & Interaction
Optimization	Object / Behavior Triggers	Data Poisoning	Data Poisoning
Deployment	Role-Playing Sensor Delay Representation Hijacking	Adversarial Suffixes Visual Perturbations	Adversarial Suffixes Visual Perturbations Multimodal Perturbations

Perception
Put apple in bowl
Decision & Planning
Execution & Interaction
Multi-Stage Closed-Loop Embodied AI Systems

	Perception	Decision & Planning	Execution & Interaction
Optimization	Adversarial Training	Safety Fine-Tuning Explicit Modeling	None
Deployment	Anomaly Detection Information Augmentation	Structural Augmentation Safety Filtering	Safety Verification Secondary Control

Adversarial Defenses