KINAITICS

# Cyber-kinetic attacks using Artificial Intelligence

## CONTEXT

**Artificial intelligence (AI)** is profoundly **modifying products and systems** in various sectors. On the one hand, its adoption creates **new opportunity for services and protection**, on the other hand, it creates **new risks for systems with an increased attack surface.**

It is well-known that attacks or malfunctions in the cyber world can **have critical impacts on the physical world**, especially in critical infrastructures. Conversely, intentional perturbations of physical systems, through e.g., attacks on sensor measurements, can have disastrous consequences on digital control mechanisms, and consequently on physical processes.

## OBJECTIVES

KINAITICS objectives towards a European strategic autonomy in **human-aware cyber-physical security** are threefold:

### 1. ATTACK SIDE

- **Demonstrate** new kind of attacks,
- **Consider** legal and ethical aspect,
- **Explore** new attack opportunities.

### 2. DEFENCE SIDE

- **Offer innovative tools and methodologies** to protect against the new threats.

### 3. VALIDATION BY REAL-WORLD SCENARIOS

- Healthcare
- Uncertainty in Critical Systems Design
- Chemical, Biological, Radiological & Nuclear
- Web Application Firewall

Funded by European Union

The KINAITICS has received funding from Horizon Europe under Grant Agreement 101070176

# MAIN OUTCOMES

- Improve the **scientific knowledge** on AI in cybersecurity
- Provide wider **societal** and **economic impact**
- Improve **EU knowledge** and policies on AI legal and ethical requirements
- Complete **7 tools** for AI attacks and defences, integrating cyber-range issues
- Provide the **demonstration of a cyber-defence platform** with a set of potential attacks on AI in physical systems

# TOOLS AND USES CASES

The KINAITICS partners are developing around 10 different attack and/or defence tools to be tested and demonstrated in the **5 proposed use cases** mentioned below:

1. **Attacks on simulation codes** to design nuclear facilities
2. **Phishing email** to steal Electronic Health Record data
3. **Image tampering** in healthcare
4. **Bot detection** in web application
5. **Structural health** monitoring

seer box
by Pluribus One

## EXAMPLE OF A TOOL:

The Seer Box tool, developed by Pluribus One, is a web application security manager, which is a **product to monitor and protect web applications and services.** Seer Box offers a broader perspective than **web application firewalls** by collecting and **analyzing real traffic data** from production websites **to detect and protect against bot attacks.**

## PROJECT FIGURES

**DURATION**
36 MONTHS

**EU GRANT**
4M€

**CONSORTIUM**
7 PARTNERS

**EUROPE**
5 NATIONALITIES


Funded by European Union

The KINAITICS has received funding from Horizon Europe under Grant Agreement 101070176