KINAITICS

Launch of EU-funded project KINAITICS

Press release - November 2, 2022

KINAITICS aims to bring robustness, resilience and responsiveness capabilities to systems involving cyberspace exposure, connections with the physical world through sensors or actuators, and in which Artificial Intelligence (AI) is used to sense, process or control. This research and innovation project funded by the European Union started on the 1st of October 2022.

The launch of KINAITICS (Cyber-kinetic attacks using Artificial Intelligence) was officially marked the 11th October 2022 at a kick-off meeting held at CEA (The French Alternative Energies and Atomic Energy Commission) in Saclay, France. The project gathers 7 members from 5 European countries.

AI is profoundly modifying products and systems in various sectors. On the one hand, its adoption creates new risks for systems, while 60% of companies adopting AI acknowledge that the cybersecurity risks generated by AI are among the most critical. On the other hand, AI has an impact on cyber-physical security practices, both on the attack and defence sides.

As a new paradigm emerges from the ubiquitous use of AI in cyber-physical systems, threat and risk assessments on systems need to be redefined to take into account the interconnection of the cyber and physical worlds and the dual use of AI. KINAITICS addresses this challenge by undertaking in-depth technical research to understand the emerging risks, and by adopting innovative defence approaches to protect systems from attack and ensure their robustness and resilience. The ambition of the KINAITICS project is to develop tools adapted to these requirements while taking into account the highest ethical standards. The project, which will take into account existing EU laws and regulations, aims to foster cross-fertilisation between technical and legal stakeholders in order to position itself beyond the current expectations of the European Commission.

Examples on the attacker side:

- Let’s imagine an attacker able to steal a factory digital twin. This enables him to obtain advanced knowledge of the physical behavior of the system. Therefore he may be able to identify the highest impacting, in terms of timing and locations, software attacks.
- In a similar factory, an attacker with access to the factory digital twin may also be able to identify behavioral cycles of the production, with advanced knowledge of the role of physical sensors in factory operations. He thus could use this knowledge to introduce perturbed measurements (aka adversarial attacks) with the most detrimental impact on a command-control AI.

Expectations on the defender side:

- In cyber-physical interconnected systems, a precise knowledge and the monitoring of the physical behaviors of the systems will be extremely valuable to add a secondary protection layer, in case firewalls and intrusion detection systems are not able to block a cyber attack.

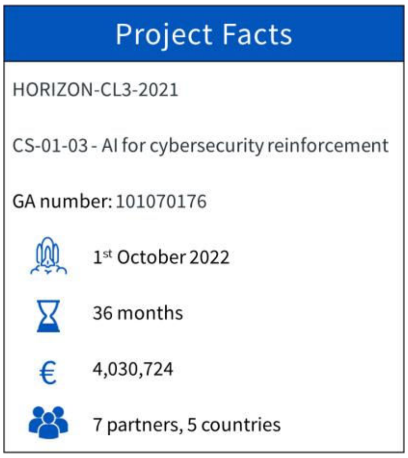
The specific targets in KINAITICS are:

- Design an integrated framework for legal, ethical and technical requirements to ensure human-aware cyber-physical security
- Go beyond the state of the art in evaluating the risk of physical attacks Design, research and develop an advanced attack exploitation framework leveraging AI, providing effective attacks to compromise either physical systems or AI-enabled ones

- Go beyond the state of the art in defense strategies in the context of cyber-physical systems security
- Advance capabilities of advanced simulators, enabling accurate training on realistic contexts

Partner’s Name	Short Name	Country
1. Commissariat à l’Energie Atomique et aux Energies Alternatives	CEA	France
2. Centre for Research & Technology, Hellas	CERTH	Greece
3. Vicomtech	VICOM	Spain
4. Engineering Ingegneria Informatica	ENG	Italy
5. Katholieke Universiteit Leuven	KUL	Belgium
6. Fondazione Toscana G.Monasterio	FTGM	Italy
7. Pluribus One	PLURI	Italy

KINAITICS
KU LEUVEN
cea
vicomtech
MEMBER OF BASQUE RESEARCH & TECHNOLOGY ALLIANCE
ENGINEERING
Pluribus One
Fondazione Toscana Gabriele Monasterio
CERTH
CENTRE FOR RESEARCH & TECHNOLOGY HELLAS



Project Facts

HORIZON-CL3-2021

CS-01-03 - AI for cybersecurity reinforcement

GA number: 101070176

1st October 2022

36 months

€ 4,030,724

7 partners, 5 countries

Contact: cedric.gouy-pailler@cea.fr
For more information about the KINAITICS project, visit https://cordis.europa.eu/project/id/101070176

Funded by the European Union

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