Assegno di Ricerca annuale su fondi PE7-Serics-Ecocyber

Title: Cyber-Risk Propagation on networks.

Months: 12

Finanziato dall'Unione Europea - NextGenerationEU a valere sul Piano Nazionale di Ripresa e Resilienza (PNRR) – Missione 4 Istruzione e ricerca – Componente 2 Dalla ricerca all'impresa - Investimento Investimento 1.3 , Avviso D.D. 341 del 15/03/2022, dal titolo: SEcurity and RIghts in the CyberSpace, codice proposta PE0000014 - CUP J33C22002810001

Committee Members:

Prof. Daniele Tantari; Dott. Davide Pastorello; Prof. Gabriele Sicuro.

Research Project in brief:

The advent of the cyber-physical ecosystem will open novel service and business opportunities but also severe risks in terms of security, resilience, privacy, and even safety. The EcoCyber project proposes original methods and solutions to exploit future opportunities and not being penalized by related issues. The four work packages aim to offer original models and solutions that represent useful inputs to the design and implementation of secure and resilient systems in different cyber-physical contexts including themanagement of legal and political issues and practices.

The research activity related to this call concerns the theoretical work-package of the project PE7 Serics-Ecocyber, in particular the WP1, Task 1.3 on Quantitative cyber-risk models and measures of cyber-physical systems.

The activity will be focused on finding unconventional and multidisciplinary ideas for cybersecurity dynamics and cyber-physical systems modeling. The goal is to understand cybersecurity dynamics, cyber and resilient risks through first principles modeling. These models aim to derive macroscopic phenomena or properties from microscopic cyber-attack/defense interactions through mathematical, AI or simulation methods.

The starting point will be the setup of a game-theoretical framework for optimal security investments against strategic attacks in networks with cyber-risk propagation. The task is comparing different optimal defending strategies as a function of the attacker preferences on which nodes (or part of the network) toreach and the network topology.