November 18, 2019 *Master of Science in Cybersecurity – Prof. Luigi V. Mancini*

CYBERSURE

CYBERsecurity at Sapienza University of Rome Events

Machine learning and Autonomous Agents: Future and Challenges for a Secure Cyberspace

Fabio De Gaspari

Affiliation: Postdoctoral Researcher at the Department of Computer Science of Sapienza University of Rome.

Abstract: Advancements in machine learning (ML), and in particular deep neural network, are pushing us towards an increasingly automated cyberspace. Intelligent systems are applied throughout all fields of IT and, in recent years, also to cybersecurity. Intelligent cyber defense agents promise to replace human experts in the cyber security domain, providing near instant incident response and adaptive security for the systems. However, while extremely successful, machine learning techniques are not designed to work in adversarial settings. Several works show how it is possible to hijack machine learning classifiers to evade classification or leak sensitive information. This talk discusses applications of ML to the cyberspace and the challenges of using ML techniques in adversarial settings.

November 18, 2019, from **14:00** to **16:00**

Aula 303 (CU002, III Floor of Scienze politiche), Piazzale Aldo Moro 5, Rome (RM)

Partecipation if free. However, registration is required on **Eventbrite** at the following link: "Machine learning and Autonomous Agents: Future and Challenges for a Secure Cyberspace".

Upcoming Events and Seminars: https://cybersecurity.uniroma1.it/cybersecurity-seminars
For any questions or further info, please write to cybersecurity_info@uniroma1.it

Website: https://cybersecurity.uniroma1.it

LinkedIn: Master of Science Cybersecurity Sapienza