Collaborative Doctoral Partnership Agreement No. 35452
between the Joint Research Centre (JRC) of the European Commission and Università degli Studi di Bari Aldo Moro (UNIBA)

Call for Expression of Interest

Applications are invited for PhD traineeships on **AI and Cybersecurity** at Joint Research Centre (JRC) of the European Commission, at Ispra Italy, under the Collaborative Doctoral Partnership programme (CDP Agreement No 35452) and within the PhD Programme in Computer Science and Mathematics of Università degli Studi di Bari Aldo Moro (UNIBA). Traineeships are expected to start on **1st October 2022**, and will last from **12 up to 18 months**, as authorized by the PhD Academic Board according to the regulations for the Doctorate Programme of UNIBA.

Number of positions

1

Title

AI and Cybersecurity

Research area and project description

Nowadays, problems with security and privacy regarding digital infrastructures, services, and products are continually increasing. Attacks against computer networks and systems continue to advance at a rate outpacing the ability of cybersecurity experts to write and deploy new signatures to detect emerging attacks. In this context, advances in AI algorithm development offer a rich opportunity to apply AI approaches to cybersecurity controls, such as Intrusion Detection and Prevention Systems, in order to detect new variants of attacks.

The recent trend of research is recognising deep learning as a definitely relevant approach in cybersecurity: since many new cyber-attacks occur because of the addition of various protocols, and most of them are variations of previously known cyber-attacks. Such a situation indicates that even advanced mechanisms, such as conventional machine learning systems, face the difficulty of detecting these small variations of attacks over time. The properties of deep neural networks may actually facilitate the discovery of effective patterns over time under drifting conditions.

Under these premises, the project will investigate one of these two main areas, namely, the application of Adversarial Machine Learning in malware detection or Time Series for anomaly detection.

a. **Adversarial Machine Learning in malware detection**

Although advances in deep learning demonstrate unprecedented levels of performance in cybersecurity applications, their vulnerability to attacks is still an open question. Adversarial examples are small modifications of legitimate inputs, which can cause misclassification at inferencetime in operational conditions. Adversarial machine learning algorithms deal with adversarial sample generation, which is creating altered input data that are capable of deceiving machine learning models. For instance, attributes of a goodware can be added to a malware executable to make the classifier incorrectly identify it as benign. Due to the critical nature of the applications of AI in cybersecurity, it is important to model the adversary and their strategies to attack the decision-making algorithms, in order to represent a realistic adversary in a cyber scenario. Explainable Artificial Intelligence (XAI) may cover a crucial role both in modeling adversaries and in developing cyber-protecting solutions.

b. **Time series analysis for anomaly detection**

One of the key aspects in the analysis of cybersecurity data is the role of the time dimension since data are typically labeled with a timestamp. This information is crucial since i) the type of attacks evolve over time and ii) the attacks can require some sequence of actions to be conducted. This means that AI methods have to take into account both past and recent events, be able to consider the sequence of events, as well as continuously adapt to the new data. For this purpose, time series analysis methods that are naturally able to take into account the changes in the underlying data distribution (concept drift) will be investigated. The purpose is to apply adaptive and time series analysis algorithms, which require a continuous training phase (lifelong learning) for anomaly detection, that is identify anomalies in the network traffic in an unsupervised manner. Such anomalies can then be used to generate alerts.

This project will explore how to take advantage of modern machine learning paradigms such as adversarial learning, XAI, time series analysis, in order to develop cyber-attack detection systems for malware or intrusion detection that are robust against possible malicious actions.

The PhD student will:

1. Carry out quantitative syntheses of the scientific literature investigating machine learning, including deep learning, adversarial learning, XAI, time series analysis algorithms recently synthesized in machine learning for cybersecurity tasks.
2. Understand the main vulnerable characteristics of cyber-data that mainly help attackers to fool any machine learning model.
3. Explore, using adversarial learning methods and time series analysis methods, the potential of defensive practices to improve the security and resilience of machine learning-based cybersecurity controls
4. Use benchmark and real data to explore the effectiveness of the new developed methods.

This stage project is an international collaboration between UNIBA and JRC. The prospective candidates are PhD students regularly enrolled in the PhD Programme in Computer Science and Mathematics with UNIBA. Selected candidate(s) will spend 18 months at JRC, Ispra (Italy). The exact plan will be settled after enrolment. The JRC in Ispra will apply the Grantholder 20 contract and working conditions reported at:

https://ec.europa.eu/jrc/en/working-with-us/jobs/temporary-positions/grantholders/contract-and-working-conditions

Eligibility criteria

Candidates should, prior to the start of the employment contract, have the nationality of a Member State of the EU or a country associated with the Research Framework Programs (Horizon Europe). Candidates from other countries may also apply. However, only the Director-General of the JRC may allow their recruitment, following the security clearance before and derogation procedure for non-EU country nationals in force at the JRC.

JRC will ask the selected candidate to provide the following supporting documents:

- Updated CV - signed
- A valid and original criminal record extract from the national database
- if applicable: Visa
- Copy of the passport or identity card
- Legal entity form and financial identification form duly filled in, signed and dated
- If relevant, marriage certificate and birth certificate of children
- Studies / Experience certificates
- Copy of the university degree/s and
- Proof of enrolment in a university doctoral studies programme. This proof must be provided before the Grant-holder contract may start and within six months from the date of the position's offer.

The JRC reserves the right to request additional documents in order to ensure the compliance with all requirements and specific rules applicable to JRC sites.

The selected candidate(s) must also be recognized as medically fit to carry out the work activities foreseen. To this end the candidate must undergo, in advance and independently, the medical checks specified by the JRC.

Selection process

The selection process is composed of two phases: a first selection is made by UNIBA resulting in a short list of two to five candidates and then a second selection is made by JRC.

UNIBA will inform the short-listed candidates about the results of the selection and that it will send their application (CV and motivation letter) to the JRC.

A short list of applications will be shared between UNIBA and JRC during the selection process.

JRC will collect the applications sent by UNIBA and will check the eligibility of the applications according to the Grantholder rules (CV included). JRC will appoint a panel and all successful applicants will be invited to an interview. The panel will establish a short list by ranking successful applicants and sending negative answers to the non-successful applicants.

The request for confirmation of interest for the traineeship position(s) will be sent by JRC, according to the above-mentioned ranking and the number of positions.

Qualifications and specific competences:

- You have a Master in Computer Science, Cybersecurity, Data Science, Computer Engineering, Mathematics (or a related field).
- You have a strong interest in machine learning and cybersecurity.
- You have experience with the design and analysis of machine learning experiments.
- You have experience with machine learning and deep learning models, big data analytics.
- You have programming skills in Python and/or Scala for data manipulation and visualization, and for performing machine learning analysis.
- You work proactively and independently and have good communication skills.
- You have a very good knowledge of English, both spoken and written.
- You are highly motivated, ambitious and result-oriented.
- You highlight relevant publications in peer review journals, if you have them.

Place of employment and place of work:

The place of the stage is the European Commission – Joint Research Centre (JRC), Via Enrico Fermi, 2749, 21027 Ispra (VA), Italy.

Contacts:

Applicants seeking further information are invited to contact:

- Prof. Annalisa Appice, annalisa.appice@uniba.it
- Prof. Michelangelo Ceci, michelangelo.ceci@uniba.it
- Prof. Donato Malerba, donato.malerba@uniba.it

How to apply:

Application must be submitted to protocollo.dib@uniba.it, clearly indicating in the subject the following text: “Application for the Collaborative Doctoral Partnership Agreement No. 35452”. Applications must be submitted before **15 April 2022 23:59 CET**.

Applications should include:

- Updated Europass CV - signed
- Copy of the passport or identity card
- Motivation letter, including a (1-2 pages) perspective project

All interested candidates are encouraged to apply, regardless of their personal background. We view equality and diversity as assets, and we welcome all applicants.