CYBER AI Module

# **Lesson design**

## ***Main Components / Key Topics***

1. Flwr module on collab
2. Custom fed-learn module on collab
3. Larger fed-project on Jupyter HPC
4. Large scaled project on slurm

## ***Objectives***

Objectives for workshop:

* Go over fundamentals of training and parameters of NN
* Go over fed learning
* Go over attacks
* Give overview of project scaling and environments

## ***Prerequisites***

* Basic understanding of python, notebooks, and setting up environments.

## ***Summative & formative assessments***

**Summative assessments:** After this workshop, participants will be able to:

**Formative assessments:**

## ***Ideals (TODO)***

# **Datasets**

# **Hands-on Development**

## ***Approach***

## ***Jupyter Notebooks***

For learners, as a supplement to the lesson

# **Lesson Outline (module)**

## ***Datasets***

## ***Approach***

## ***Conventions***

## ***Episodes:***

# **Key Resources**

<https://github.com/UMBCvision/Universal-Litmus-Patterns>

[[2007.08745] Backdoor Learning: A Survey](https://arxiv.org/abs/2007.08745)

# **OPEN ISSUES/FEEDBACK**