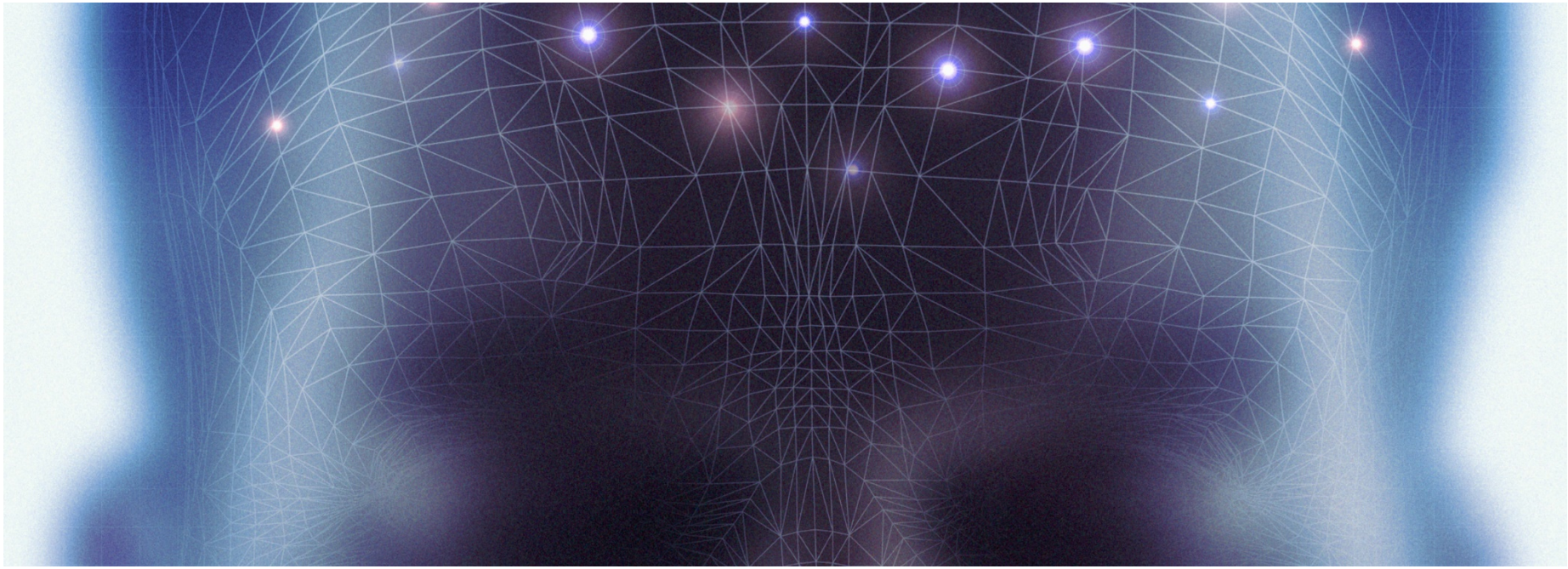
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confedraziun svizra

Swiss Confederation

Federal Department of Defence,
Civil Protection and Sport DDPS
armasuisse
Science and Technology



ACM SOSP

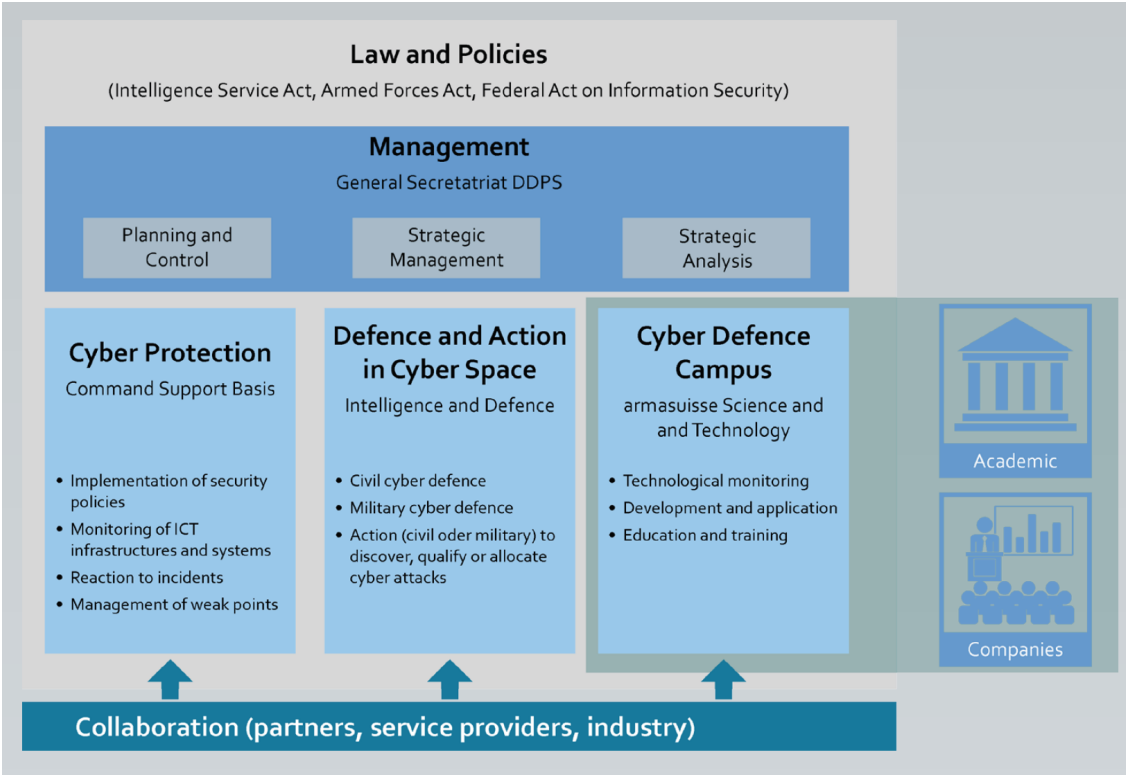
Resilient Federated Learning

Dr. Gérôme Bovet, 25.10.2021
gerome.bovet@armasuisse.ch

Introduction

Head of Data Science at Swiss DoD

- 10 scientific project managers
- 5 interns at master level
- Portfolio of 25-30 research projects with academia (Switzerland + Europe)



The Cyber-Defence Campus (CYD) was created in 2019 to conduct

- technology monitoring
- research & development
- education and training
- consulting and testing

Focussing on following domains

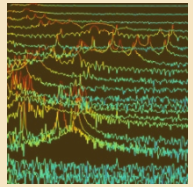
- Cyber Threat Intelligence
- Intelligence
- ICT security

Research focus

Data protection

Adversarial ML/DL
Federated learning

Data acquisition



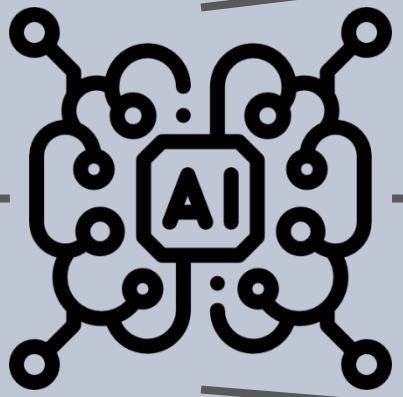
IoT
*Crowd**
ADINT
OSINT

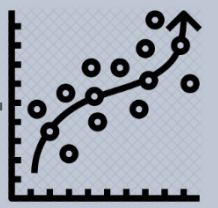
SIGINT
COMINT
SOCMINT

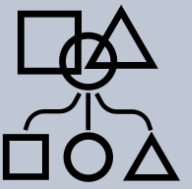
Data management

Data lake
Lambda architecture
Kappa architecture

Data processing & analysis







Statistical learning
Machine learning
Deep learning

Classification
Prediction
Anomaly detection

What are the top one or two topics in resilient FL where we are working and we are making progress?

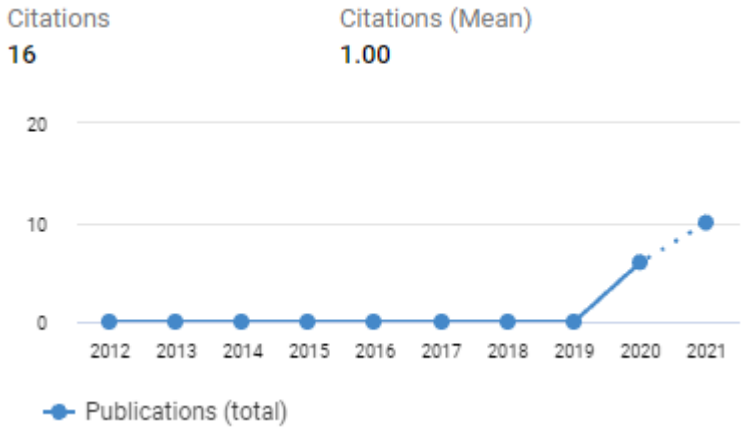
- Federated learning as **privacy preserving** approach
  - Analysis of network traffic for intrusion detection
  - Definition of behavior patterns of IoT devices for anomaly detection

  BUT…

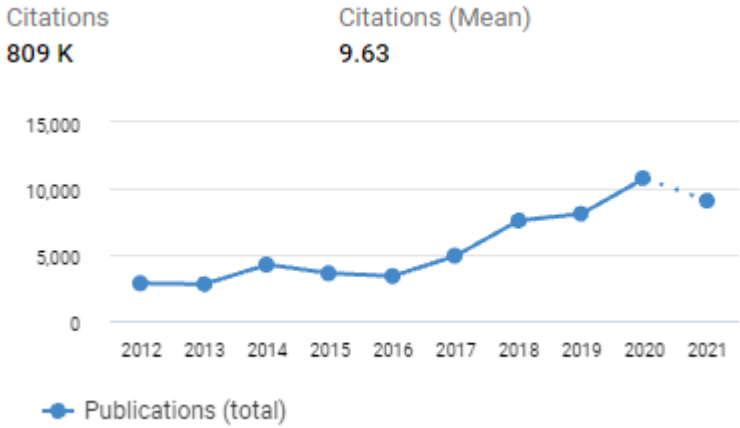
  - **Model poisoning attacks** can have a large impact on classification and anomaly detection results
  - The federator remains a **single point of failure**, although considered to be trustworthy or running in a trusted environment (contrary to the worker nodes)

What are the top one or two topics in resilient FL where we have learned important lessons from existing literature?

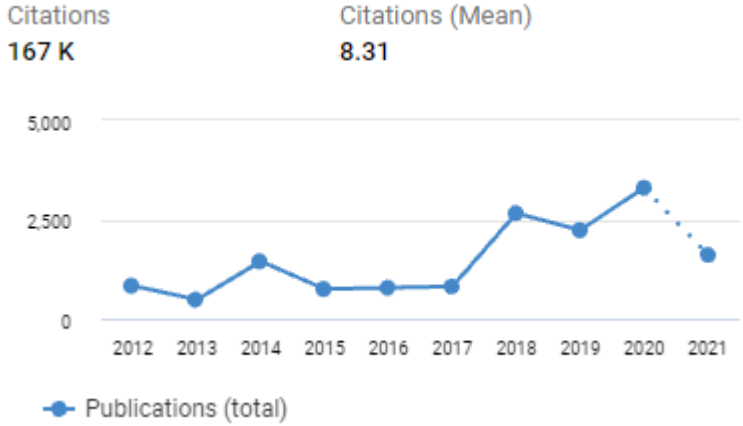
"resilient federated learning"



federated learning



resilient federated learning



What are the top one or two topics in resilient FL which we should be working on but are not?

- Get rid of the federator and target a **fully distributed/collaborative learning** → *Towards peer-to-peer learning*

- **Secure multi-party computation** seems really promising, but usually limited to a **small number of participants** → *Towards peer-to-peer secure multi-party ML*