EDF-2021-DIGIT-R: Artificial intelligence

Proposals are invited against the following topic:

EDF-2021-DIGIT-R-FL: Frugal learning for rapid adaptation of AI systems.

Budget

The Union is considering a contribution of up to EUR 18 500 000 to support proposals addressing the abovementioned topic and its associated specific challenge, scope, targeted activities and main functional requirements.

Several actions, addressing different solutions, may be funded under this call.

Specific challenge

In times of real-time information availability and exchange, and increasing complexity of situations, artificial intelligence (AI) has become an essential driver for new competitive system solutions. Future military capabilities will include a significant share of systems that will make massive use of AI techniques.

Modern AI systems based on Machine Learning and especially Deep Learning techniques usually require many labelled data points to reach acceptable performance. Furthermore, they can suffer from inconsistent behaviours, such as high-confidence failures, or failures in trivial cases. More generally, improving AI systems to take into account new data requires extensive testing by expert developers to avoid regression. These issues severely impact their availability for defence systems, which are characterised by the lack of data, for instance when dealing with enemy intelligence, and by the need for trustable results and rapid adaptation, including from data that cannot be shared with system developers for confidentiality reasons or because of poor connectivity. This is especially important when the information to manage is highly variable or unpredictable and high adaptability is needed.

The challenge is to develop new Artificial Intelligence methods that are able to make use of less training data than current state-of-the-art deep learning algorithms while maintaining similar performance, to provide better control over the output space in order to ensure a more consistent behaviour, and to limit the development efforts when adapting systems to new data. These methods must prove their worth on realistic and challenging use cases representative of military operations.

Scope

The aim is to tackle the problem of robustness and frugality in military AI software components to facilitate the development of new systems and their adaptation to the evolution of their environment, including from user supervision, for a reasonable cost, with minimal intervention from expert developers, and without regression. State-of-the-art research on transfer learning, zero- or few-shot learning, active learning, domain adaptation, hybrid AI and other relevant topics should be leveraged to propose new methods to improve AI-based methods, while preserving high performance.

Targeted activities

The proposals must cover the following activities as referred in article 10.3 of the EDF Regulation, not excluding possible downstream activities eligible for research actions if deemed useful to reach the objectives:

- Activities that aim to create, underpin and improve knowledge, products and technologies, including disruptive technologies for defence, which can achieve significant effects in the area of defence.

The proposals must address in particular the following objectives:

- Design of relevant military use cases where trustworthy and frugal AI algorithms are needed (i.e. targeting specific tasks for which data-greedy algorithms are currently outperforming other methods), and for which representative data can be collected and performance can be measured in an objective way.
- Development of new methods for reducing the need for data and supervision to train and adapt AI systems (and simultaneous monitoring of the state of the art, which is important in this quickly evolving domain but should take place as a background activity integrated with system development), for example through:
    - simulation and generative models,
    - transfer, semi-supervised, self-supervised, and active learning,
    - hybridisation with user-defined rules.
- Development of new methods for improving robustness guarantees by design, for example through:
    - new algorithms increasing the robustness of existing neural networks methods that are intrinsically not robust,
    - evaluation and surveillance of both the output space and the environment.
- Implementation of benchmarking experiments on the use cases to demonstrate the advantages and drawbacks of the proposed methods.

Functional requirements

The proposed solutions should fulfil the following requirements:

1) General

- For each use case addressed, several approaches should be explored by different research teams.
- The proposed techniques should be presented in the proposals.
- All systems addressing a given use case should be benchmarked using the same experimental protocol (metric, data, train/test split, etc.) in order to ensure comparability.
- In all experiments, several runs should be performed in order to provide the means and variances of system performance estimates.
- A strong and solid open source strategy has to be defined to ensure sharing of the generic results, functions, software with a license compatible the further development and commercial exploitation of the results (e.g. ePL, L-GPL, etc.).
- For at least one use case, means to reproduce the experiments in a comparable way should be ensured beyond the project, by publishing as open data the use case

description, associated dataset and metrics. The consortium member(s) guaranteeing this sustainable availability should be clearly identified.
- Possibilities and conditions to provide further use-case data and means to reproduce experiments and benchmarks with internal methods, in particular for national authorities and their technical centres, should be described. The consortium member(s) ensuring this should be clearly identified.

2) Use cases

- Use cases should be defined and precisely described, including a description of the data to be collected and used for the experiments and a description of the metrics to assess progress.
- Use cases should revolve around one or several of the following topics:
    - Situation Awareness and intelligence (ATD/ATR, monitoring, change detection, data fusion...), for multiple vectors (robot, UXV, vehicle) and sources (multimodal and/or multilingual)
    - Operational C2 (decision aid, threat assessment, effect prediction, movement coordination, mission planning...)
    - Mission equipment (autonomous vehicle, delocalised decision...)
- Use cases should be representative of modern military conditions, by using sufficient amounts of real or realistic data.
- Use-cases should be challenging, i.e. existing methods from academic and/or industry state-of-the-art should not be close to a saturation point (e.g. a 100% success rate for a simple image recognition use case, without challenges, on a basic set of simulated data, is not relevant)
- The process by which an end user could adapt a system to fit its own data or rules should be investigated, in order to determine whether it is possible to do so without expertise in AI.
- Systems should be resilient to inconsistent inputs and to attacks (adversarial attacks, data poisoning...)

3) Frugal AI

- Frugal AI systems should require smaller amounts of data than traditional state-of-the-art ones to offer similar performances.
- Systems should be benchmarked with respect to the cost of data creation (in particular as a function of the number of labelled and unlabelled examples) and/or system supervision (e.g. minimal amount of supervision needed to provide a correct output)

4) Robust AI

- Robust AI systems should be able to ensure some predefined properties and behaviours. When adapting to new environments, they should ensure non-regression and possibly guide user supervision.
- Systems should be benchmarked with respect to these abilities and offer enhanced performance compared to traditional stat-of-the-art systems (by avoiding failure in trivial cases or inconsistent behaviours while maintaining performance in other cases).

Expected impact

The expected impacts are to:

- Accelerate the introduction of robust AI in military systems;
- Increase trust of experts and end users in AI systems;
- Increase system performance and resilience;
- Enhance technological autonomy.