

Artificial Intelligence, Machine Learning and Big Data for Hybrid Military Operations (AI4HMO)

(STO-MP-IST-190)

Executive Summary

The IST-190 symposium provided a forum for invited and contributed papers that work “towards a common roadmap for future technologies, addressing the identified knowledge gaps, while recognizing the opportunities offered by available techniques related to emerging technologies in the areas of Artificial Intelligence (AI), Machine Learning (ML) and Big Data (BD) for hybrid military operations.” Of necessity, it was a virtual symposium held via Webex, but it was nonetheless a very successful symposium thanks to the efforts of the Co-Chairs, Dr. Michael Wunder and Maj. Gen. Michael Faerber, and others in the organizing committee. Three Keynote addresses were given by highly distinguished speakers, and 34 papers contributed papers were given by subject matter specialists. The papers were split into seven topic-related groups that were presented in parallel sessions over two days. There were two such sessions at any given time, and the attendees could choose between them. The contributed papers are diverse and they report on a wealth of experience. They were all well-written, and the presenters were all excellent. The Best Paper Award and the Early Career Scientist Best Paper Award were announced at the end of the symposium. All 34 papers and presentation slides are available.

The technologies of AI and ML are evolving at a rapid pace, and they are exploiting the availability of Big Data, which has its own specialized set of techniques. There is currently a bewildering variety of existing methods and applications that are enabled by some combination of these technologies, and more are being proposed and explored every day. Some capabilities are extensions of what we know; some are reasonably predictable based on what is known; and some cannot be anticipated and will be surprisingly effective. The IST-190 symposium sought to identify and explore the potential of these emerging technologies for hybrid military operations. The emphasis of the papers was on defense and preparedness.

The papers presented at IST-190 showed that the threat of these combined technologies is real, and that AI/ML practitioners are gaining experience in applying them to military operations. The papers also show, collectively and in diverse ways, that defending against the threat requires the development of new and improved tools to deal with the technical challenges. The need for solutions is growing.

New tools are needed and welcome, of course, but new developments take time. Greatly improving the capabilities of existing tools will address many immediate needs. These include:

- Compensate for the lack of data for “infrequent” events with few available exemplars
 - Generative and adversarial methods can augment available data sets
- Explain AI/ML derived decisions and recommendations
 - Black box directives can mislead and undermine confidence
- Give accurate self-assessment of the reliability of AI/ML recommendations, and of the correctness of aggregated (fused) heterogeneous data sets
 - Make robust decisions in a fog of uncertainty
- Use natural language processing (NLP) for HUMINT

- Often critical in AI/ML systems that exploit hard-soft information fusion
- Methods for real time adaptation to evolving threats
 - Perfect assessments that come too late are of limited value
- Support building trust in the system
 - Data provenance / drill down
 - Built-in sanity checks for the human in the loop

Many innovations will inevitably be developed by the private sector. For success, innovations that are successful in the private sector must be transitioned to meet demanding military operational needs that will severely stress the capabilities of commercial AI/ML methods. Case studies presented in the symposium suggest that tools for hybrid military operations should be jointly developed by military operation specialists and subject matter specialists to ensure that the focus is on the real and evolving need, and to build trust in the system.

Intelligence artificielle, apprentissage automatique et données massives pour les opérations militaires hybrides (AI4HMO)

(STO-MP-IST-190)

Synthèse

Le colloque de l'IST-190 a offert un espace de discussion autour d'articles d'invités et de contributeurs qui travaillent « dans l'optique d'une feuille de route commune pour les futures technologies, traitent les lacunes identifiées et reconnaissent les opportunités offertes par les techniques disponibles liées aux technologies émergentes dans les domaines de l'intelligence artificielle (IA), l'apprentissage automatique (AA) et les données massives (DM) pour les opérations militaires hybrides. » Par nécessité, le colloque s'est tenu virtuellement via Webex, mais il a été néanmoins très réussi, grâce aux efforts des deux co-présidents, le Dr. Michael Wunder et le major général Michael Faerber, et des autres membres du comité d'organisation. Le colloque s'est ouvert sur trois allocutions données par des intervenants très distingués, puis 34 articles ont été présentés par des spécialistes. Les articles étaient divisés en sept groupes thématiques présentés en sessions parallèles en l'espace de deux jours. Il y avait toujours deux sessions en même temps et les participants pouvaient choisir à laquelle assister. Les articles étaient divers et portaient sur une riche expérience. Ils étaient tous bien écrits et les conférenciers étaient tous excellents. Le prix du meilleur article et le prix du meilleur article d'un jeune scientifique ont été annoncés à la fin du colloque. Les 34 articles et les diaporamas sont tous mis à disposition.

Les technologies de l'IA et de l'AA évoluent rapidement et exploitent la disponibilité des données massives, auxquelles correspondent un ensemble de techniques spécialisées. Il existe actuellement une diversité stupéfiante de méthodes et d'applications rendues possibles par la combinaison de ces technologies et d'autres sont proposées et explorées chaque jour. Certaines capacités sont le prolongement de ce que nous connaissons, certaines sont raisonnablement prévisibles en fonction des connaissances et certaines sont impossibles à anticiper et seront étonnamment efficaces. Le colloque de l'IST-190 a cherché à identifier et étudier le potentiel de ces technologies émergentes pour les opérations militaires hybrides. Les articles mettaient l'accent sur la défense et l'état de préparation.

Les articles présentés à l'IST-190 ont montré que la menace de ces technologies combinées était réelle et que les praticiens de l'IA/AA gagnaient de l'expérience en les appliquant aux opérations militaires. Les articles ont montré également, de manière collective et diverse, que la lutte contre cette menace passait par l'élaboration de nouveaux outils, meilleurs, pour relever les défis techniques. Le besoin de solutions va croissant.

De nouveaux outils sont nécessaires et bienvenus, naturellement, mais leur développement prend du temps. L'amélioration considérable des capacités des outils existants répondra à beaucoup de besoins immédiats, parmi lesquels :

- Compenser le manque de données sur les événements « peu fréquents » avec les quelques occurrences disponibles
 - Les méthodes génératives et contradictoires peuvent étoffer les ensembles de données disponibles

- Expliquer les décisions et recommandations déduites de l'IA/AA
 - Les directives de type « boîte noire » peuvent être trompeuses et miner la confiance
- Fournir une auto-évaluation précise de la fiabilité des recommandations d'IA/AA et de la correction des ensembles de données hétérogènes agrégées (fusionnées)
 - Prendre des décisions solides dans un brouillard d'incertitude
- Utiliser le traitement du langage naturel (NLP) pour le renseignement humain (HUMINT)
 - Souvent crucial dans les systèmes d'AI/AA qui exploitent la fusion des informations certaines et incertaines
- Méthodes pour l'adaptation en temps réel aux menaces qui évoluent
 - Les évaluations parfaites qui arrivent trop tard sont d'une valeur limitée
- Soutenir l'établissement de la confiance dans le système
 - Provenance des données / approfondissement
 - Contrôles de cohérence intégrés pour l'humain dans la boucle

Beaucoup d'innovations seront inévitablement développées par le secteur privé. Les innovations réussies du secteur privé doivent être adaptées pour répondre aux besoins opérationnels militaires exigeants, qui constitueront une contrainte importante pour les méthodes d'IA/AA du commerce. Les études de cas présentées lors du colloque suggèrent que les outils destinés aux opérations militaires hybrides devraient être élaborés conjointement par des spécialistes des opérations militaires et des spécialistes du domaine particulier, afin que l'accent soit mis sur le besoin réel et évolutif et pour donner confiance dans le système.