Deep Models and Artificial Intelligence for Military Applications:
AAAI Technical Report FS-17-03

Autonomous Outcomes: Shaping the Future Data Environment to Build Trust in Artificial Intelligence and Machine Learning Applications

Major Scott A. Humr
United States Marine Corps
Marine Corps University
scott.humr@usmc.mil

Abstract

Advances in artificial intelligence (AI) and machine learning (ML) are already demonstrating great utility in a variety of domains that point to great opportunities for adoption in a wide variety of military applications. For this reason, data will become the life-blood of many AI and ML enabled technologies. Yet, developing trusted data sets for the purposes of training and testing AI and ML applications will become a central issue to eliciting predictable behaviors of such technology in order to foster trust in autonomous systems. Therefore, the US Department of Defense (DoD) cannot sit idle while AI and ML developments remain forthcoming. Rather, the US military can begin laying the ground work for constructing training data in domain specific ways that will help convergence with AI and ML in the future.

Introduction

Autonomous systems enabled by AI and ML on the battlefield are projected to proliferate in the very near future (South, 2017). Undeniably, these systems will require vast amounts of trusted data to develop behaviors and to elicit actions predictable to military leaders. However, data sources within the military are disparate, often unstructured, and come in a wide-variety of formats and classifications that pose many challenges to developing trusted training data for AI and ML applications. Developing a framework to facilitate data munging for maturing trusted training data, could become a key enabler to ensuring the military is postured to rapidly gain the most from AI and ML applications. Consequently, this approach can help build a foundation of trust in such technologies.

Developing data set frameworks ahead of AI adoption will not only allow the US military to train and employ AI technologies faster, it will have second and third order salutary effects on day-to-day information and knowledge management throughout. This position paper explores the challenges and opportunities associated with developing such frameworks for improving AI and ML outcomes with an aim to spur discussions on developing trusted training data.

Challenges

Provisioning the requisite data to train domain specific AI and ML applications provides several formidable difficulties. First, few standards exist for data formats or applying consistent meta-data to data and information before it is processed. Haphazard business procedures and archaic paper-based processes often inhibit effective data discovery and efficient retrieval. An absence of consistent standards results in a proliferation of largely amorphous data sets across the military enterprise making it difficult to organize and verify data efficiently. Service specific processes can bear similarities in many regards, yet exist in different formats across the Joint Information Environment (JIE).

Second, data repositories exist in many locations such as regional data centers, government and private clouds, and on premise servers globally distributed. Understanding where the most accurate data resides is often problematic as it is sometimes sneaker-netted across domains, ran in batch cycles, or updated only periodically. Lack of access to complete data sets might lead to locally optimal results. Enterprise data also spans across classification levels and would likely contribute to increasing the classification of AI and ML applications, to which fewer personnel have security clearance to access.

These problems raise questions of what data developers will use to mature military centric AI and ML applications effectively and how access to the most important data can be achieved. Vast differences in opinion on what constitutes accuracy or relevancy in qualitative types of training

Disclaimer: The views expressed by the author do not represent the views of the United States Government, the United States Department of Defense, or the United States Marine Corps.

data could potentially produce distinctive outcomes. Questionable training data might contribute to how people perceive results and further add to the arcane nature of AI and ML technologies. Accordingly, these challenges may produce suboptimal results that directly influence trust operators and leaders have in autonomous systems that leverage AI or ML (Freedberg, 2017). These challenges could become insurmountable if military leadership does nothing to influence the current data environment and work towards laying the ground work for facilitating assimilation of AI and ML technologies.

Opportunities

Influencing the future data environment has never been more important. While aspects of cyber security: confidentiality, integrity, availability, and non-repudiation will remain important for the foreseeable future, properly classifying, tagging, and rating data in standard ways will become equally important for eliciting optimal results downstream to AI and ML applications. Currently, no such framework exists across the DoD that addresses data munging. However, advances in collaboration technologies, expert systems, and enterprise resource management programs can support better data curation, collaboration, and rich feedback from a larger body of individuals. Technologies such as Blockchain can further ensure that the most important data and transactions are protected, which could provide a method for furthering trust in the DoD's most important data.

Adoption of such enterprise-wide systems would also improve current efforts in Big Data analytics, data tuning, and promote conventional knowledge discovery through extant search engine technologies, therefore, providing current and future benefits. Creating such a system also hedges risk if AI and ML adoption proves too contentious or embracing analogous future technologies takes longer than anticipated. Benefits of trusted data would accrue regardless if the DoD adopts AI and ML technologies, yet would also lay the foundation for more rapid technology adoption if a true paradigm shift occurs. Agreeing on particular data taxonomies, ontological frameworks, and knowledge modeling could prove contentious, therefore, the DoD should start now on charting this course.

Discussion

The ability to influence future outcomes in the fields of AI and ML are promising. Engendering trust with the commander potentially faced with making decisions based on recommendations from AI and ML applications will become a central issue. While semi-autonomous systems and manned-unmanned teaming are a current reality in the US military today, it is predicted that they will only increase as these technologies become more adaptable and capable to an increasing number of scenarios (Macak and Jensen, 2017). Yet, such evolutionary steps in capabilities point to a reality that, in some instances, fully autonomous systems could become the choice du jour in future operating scenarios that demand rapid adaptations to environmental variables that are beyond human processing capabilities such as cyber warfare.

In order to fully exploit the speed at which these machines may operate, commanders will need to have a level of confidence built on a foundation of trust in the data used to train these systems. Just as confidence in a military commander's ability to rapidly assess a situation, develop keen insight from often limited information and solutions to complex problems through years of real-world experiences, education and training, a similar assurance in the data and resultant outcomes of AI and ML will need to be engendered through testing and predictable feedback. A proliferation of AI and ML technologies throughout the operating environment may herald an era where future battlefield leadership becomes more akin to a Chief Technology Officer than a traditional foot soldier. Nevertheless, developing AI and ML applications that foster trust in their outcomes facilitates rapid decision making in order to outcycle an enemy's own operational tempo will be beneficial and produce the best outcomes for the US military.

Conclusions

The approaches and questions raised in this position paper are principally exploratory and speculative for the express nature of cultivating interest in this area and to challenge a largely overlooked evolutionary step towards building trust in autonomous systems. For these reasons, the DoD needs to pursue and mature a multi-strategic approach for addressing the complexities of data wrangling across the JIE in support of current and future AI and ML technologies. While current technologies exist to facilitate many of the proposals this paper recommends, still, DoD leadership will need to lead the way in directing the Services to collaborate and lay aside particular cultural parochialism and procedural positions to achieve more optimal collaboration and outcomes envisaged for AI and ML technologies.

References

Freedberg Jr., S.J. "Artificial Stupidity: Learning To Trust Artificial Intelligence (Sometimes)." *Breaking Defense, July 5, 2017,* http://breakingdefense.com/2017/07/artificial-stupidity-learning-to-trust-the-machine.

Macak, A. and Jensen, B. "Your Grandfather's Manned-Unmanned Teaming: Looking Back to Stay Ahead. *War on the Rocks,* April 4, 2017, https://warontherocks.com/2017/04/your-grandfathers-manned-unmanned-teaming-looking-back-to-stay-ahead.

South, T. "Future infantry might not need humans." *Army Times,* July 31, 2017, https://www.armytimes.com/news/your-army/2017/07/30/future-infantry-might-not-need-humans.