Военные применения машинного обучения

Д.Е. Намиот, Е.А. Ильюшин, И.В. Чижов

***Аннотация*—Настоящая статья посвящена прикладным аспектам применения систем машинного обучения. Очевидно, что области практического применения такого рода решений постоянно увеличиваются. Основным двигателем здесь является то, что с практической точки зрения машинное обучение рассматривается как синоним для понятия искусственный интеллект, внедрению которого в развитых странах посвящены специальные программы. Естественно, что среди таких внедрений рассматриваются и военные применения. Причем здесь можно отметить интересную особенность. Если раньше, военные области служили толчком для развития техники, заказывался поиск решений для военной техники и т.д., то в данном случае все, скорее, движется в обратном направлении. Сначала появляются новые решения (разработки), использующие машинное (глубинное) обучение, а затем их начинают использовать, в том числе, и в военных системах. В статье приводится обзор опубликованных военных программ использования искусственного интеллекта в военной сфере, который составлен с целью представить именно технологии и решения в области машинного обучения, которые применяются (используются) для военных систем.**

***Ключевые слова*—машинное обучение, искусственный интеллект, устойчивые системы.**

I. Введение

Машинное обучение становится, на сегодняшний день, одной из наиболее часто используемых технологий во многих прикладных системах. На сегодняшний день машинное обучение является практическим синонимом термина Искусственный Интеллект, программы развития которого являются уже национальными программами во многих странах [1]. При этом использовать возможности машинного обучения в приложениях становится все проще. Многие библиотеки машинного обучения и онлайн-сервисы уже не требуют глубоких знаний в области машинного обучения, использование этой технологии уверенно движется к автоматизации (AutoML) [2].

Для военных применений, как и для всех других критических систем, естественным является повышенной внимание к устойчивости решений, стойкости к возможным атакам на такие системы, возможности объяснения принимаемых решений. То есть тому, что и рассматривается в теме кибербезопасности систем машинного обучения. Собственно говоря, военная область является одним из основных пользователей (потребителей) решений по кибербезопасности. Именно поэтому, статья является продолжением серии публикаций, посвященных устойчивым моделям машинного обучения [3, 4]. Она подготовлена в рамках проекта кафедры Информационной безопасности факультета ВМК МГУ имени М.В. Ломоносова по созданию и развитию магистерской программы "Искусственный интеллект в кибербезопасности" [5].

Традиционно, военные применения были заказчиком (инициатором) множества научно-технических разработок. Технологии во всем мире создавались по военным заказам, а потом, возможно, находили и другое применение. С решениями на базе искусственного интеллекта (машинного обучения, как это понимается сейчас, в большинстве случаев) картина выглядит обратной. Сначала появляются методы (модели, алгоритмы), а далее для них уже находится применение, в том числе, и военное.

В этой статье приводится анализ опубликованных программ использования систем искусственного интеллекта в военной области с точки зрения применяемых технологий (моделей, алгоритмов) машинного обучения. То есть наша цель – представить именно технологии, а не характеристики военных применений. Очевидно, что все детали по такого рода программам явно не публикуются. Соответственно, в этих случаях мы описываем технологии (модели и т.д.), которые могли бы быть, по мнению авторов, задействованы в соответствующих системах.

Наш обзор проектов по устойчивому машинному обучению [3] содержит, в том числе, и проекты, выполняемые для военных. Как было указано выше, устойчивость систем машинного обучения представляет собой определяющую характеристику для критических применений. В данной же статье мы хотели бы затронуть все известные проекты, связанные с машинным обучением.

II. Военный искусственный интеллект в проектах США

Здесь можно упомянуть следующие работы. Во-первых, это проект Maven [6]. В [7] цели этого проекта

Статья получена 3 декабря 2021. Исследование выполнено при поддержке Междисциплинарной научно-образовательной школы Московского университета «Мозг, когнитивные системы, искусственный интеллект»

Д.Е. Намиот – МГУ имени М.В. Ломоносова (email: dnamiot@gmail.com)
Е.А. Ильюшин - МГУ имени М.В. Ломоносова (email: john.ilyushin@gmail.com)
И.В. Чижов - МГУ имени М.В. Ломоносова (email: ichizhov@cs.msu.ru)

описываются как автоматизация обработки видео-данных с помощью алгоритмов компьютерного зрения и машинного обучения. Данные (видео) при этом собирались беспилотниками. Искусственный интеллект предназначался для автоматизации работы специалистов, просматривавших такие видеофайлы. Идея состоит в автоматическом определении враждебной активности и, соответственно, повышении скорости принятия решений. “Ручной” просмотр таких данных, где большую часть времени ничего не происходит, очевидно, чреват пропусками важной информации.

Технически, это можно описать как автоматическую разметку (аннотацию) видео-данных в стиле AutoML решений (никакой ручной настройки быть не должно, видеоданные должны анализироваться как есть). У автоматизации видео-наблюдений применений, очевидно, будет множество. В силу этого, очевидно, должен также быть некоторый API, с помощью которого сторонние приложения смогут запрашивать результаты классификации (разметки) видео-данных. Прикладная область (что будет распознаваться) должна определяться данными, которые использовались для обучения.

В качестве прототипа такой системы можно назвать, например, проект Google AI Video [8] – рис. 1.

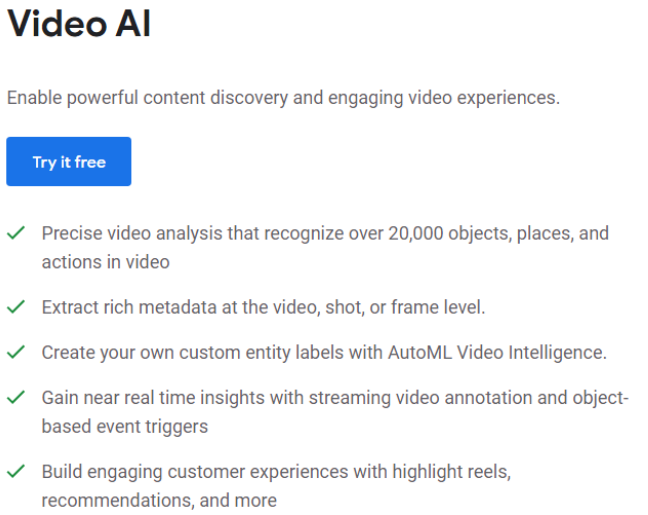

Рис. 1. Google AI Video [8]

Компания Google одно время являлась исполнителем по проекту Maven [9].

Тема разметки видео достаточно широко представлена в литературе. Например, можно указать на обзоры [10, 11]. Kaggle даже проводил спонсируемое Google соревнование по этой тематике [12]. Исследования в этой области касаются таких тем, как обнаружение объектов [17], отслеживание (трекинг) объектов [18], распознавание отдельных элементов (лиц [20], номерных знаков [21]) классификация изображений [24] и маркировка (разметка) сцен [25].

На рисунке 2 представлен один из популярных подходов к распознаванию (обнаружению) объектов – выделение регионов с последующей классификацией [13]. YOLO является одним из наиболее часто используемых Open Source решений для распознавания объектов на видео [19].

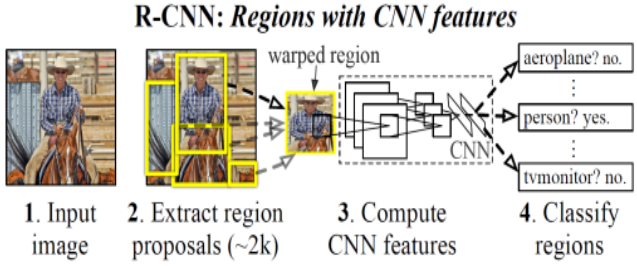

Рис. 2. Распознавание объектов [13]

Разметка сцен в последние десятилетия вызывает большой интерес. Цель состоит в том, чтобы предоставить семантическую метку для каждого пикселя изображения с помощью некоторого предопределенного набора меток. Другими словами, при синтаксическом анализе сцены каждое изображение сегментируется или разбирается на области, связанные с семантическими категориями. Традиционные параметрические подходы к синтаксическому анализу сцены изучают объектную модель для каждой категории объектов. Модели обучения и соответствующие им параметры оцениваются на этапе обучения.

Предположим, что мы хотим добавить новые категории объектов к существующей системе. Для этого нам нужно изучить новую модель для новых категорий объектов, что часто требует много времени. Напротив, в непараметрических подходах, вместо изучения сложных моделей для каждой категории объектов, знания из помеченных обучающих изображений переносятся на немаркированное изображение. Типичные непараметрические подходы к синтаксическому анализу сцены состоят из трех основных этапов. На первом этапе мы получаем небольшое подмножество обучающих изображений, которые визуально похожи на изображение запроса. На втором этапе метки из полученных обучающих изображений переносятся в изображение запроса. До этого момента каждому пикселю могут быть присвоены разные метки. На третьем этапе для агрегирования меток используется структура условного случайного поля (Conditional Random Field - CRF). Таким образом, эти методы сопоставляют изображение запроса с существующим набором аннотированных изображений. Затем метки из аннотированных изображений переносятся в изображение запроса. Наиболее важные преимущества непараметрических подходов заключаются в том, что они не зависят от набора данных и количества категорий объектов. Кроме того, эти подходы не требуют повторного изучения параметров модели для каждого набора данных.

Сжатый обзор перечисленных направлений есть, например, в работе [26], которая сама по себе рассматривает видео-данные в Умном городе. Это еще

одно подтверждение того, что само по себе направление семантической сегментации видео данных является естественным шагов в развитии систем видеонаблюдения. Камеры становятся доступнее экономически, их становится много, и возникает естественная идея автоматизировать процесс просмотра. Экспертов (не только в военной сфере) просто не хватит для просмотра видео. Даже в формате анализа видео, записанного с помощью дронов, есть множество приложений вне военных применений, например, в строительстве (контроль работ) [14] или транспорте (инспекция транспортных сооружений, интеграция BIM и ГИС) [15, 16] и т.д.

Очевидно также, что если мы говорим о военном применении анализа видео, то такого рода системы должны считаться с состязательными атаками. Исторически используемые методы маскировки (камуфляжа) могут быть дополнены специальными средствами для “обмана” алгоритмов машинного обучения [22].

Можно также предположить, что в специальных применениях передача потокового видео с дрона может быть невозможна, и соответствующий анализ должен будет проводиться на борту летательного аппарата или в каких-то комбинированных моделях. Соответственно, речь может идти о каких-либо Edge-моделях [23]. В работе [36] описано как раз такое применение. Можно также предположить, что специальные применения потребуют использования коллаборативных моделей, когда будут анализироваться несколько потоков параллельно, для увеличения точности оценки [27]. Совместное использование дронов рассматривается как классическая задача для военных применений.

Отдельно необходимо отметить важность прикладных API для систем анализа сцен. В частности, с их помощью станет возможным хранить индексную информацию о видеофайлах, что позволит, например, сравнивать новые данные с историческими видео.

В целом, описывая технологии, стоящие за проектом Maven, можно отметить следующее. Это область, которая собирает в себе практически все основные направления (достижения) в машинном обучении. Об этом свидетельствует и огромное количество работ, и необходимые большие усилия, которые нужны даже просто для отслеживания текущих результатов исследований. С одной стороны, наличие открытых решений позволяет достаточно быстро стартовать с некоторым прототипом (стендом), но реализация промышленной системы, работающей с заданными показателями точности и защищенной (в какой-то степени) от состязательных атак является весьма сложной. Собственно говоря, размеры компаний-подрядчиков по этому проекту (Google и др.) свидетельствуют именно об этом.

Организационно, проект Maven относится к созданной в июне 2018 года организацией Joint AI Center [28], которая отвечает за создание военных систем искусственного интеллекта и продвижение исследований к ключевых технологиях проекта Maven. Обзор других организаций США, вовлеченных в создание военных систем искусственного интеллекта есть, например, в работе [29].

Проект DARPA ‘AI Next’ [30] включает 5 основных направлений:

- AI capability,
- robust AI,
- adversarial AI,
- high-performance AI
- next-generation AI.

Согласно анонсу [31] эти направления определяются так:

New Capabilities: технологии искусственного интеллекта регулярно применяются для реализации научно-исследовательских проектов DARPA, в том числе более 60 существующих программ (рис. 3). Этот пункт говорит об использовании технологий искусственного интеллекта во все большем количестве программ, поддерживаемых DARPA.

Robust AI: устойчивость для систем машинного обучения. Мы рассматривали это направление в своих работах [3, 4]. Отмечается, что надежность (устойчивость) является критическим фактором для внедрения технологий искусственного интеллекта в тактическом звене.

Adversarial AI: борьба с атаками на системы машинного обучения. Тесно связано с предыдущим пунктом, на самом деле. Технически, так называемые состязательные атаки (специальная модификация входных данных для предотвращения корректной работы систем искусственного интеллекта или наоборот, достижения желаемой работы) неотличимы от проблем обучением системы – в обоих случаях работа системы на реальных данных не соответствует тому, что было показано на тренировочных данных. Другие типы атак (отравление, бэкдоры) более похожи на “традиционные” проблемы кибербезопасности. DARPA отмечает необходимость масштабирования таких решений.

High Performance AI: рост производительности компьютеров за последнее десятилетие обеспечил успех машинного обучения в сочетании с большими наборами данных и библиотеками программного обеспечения. Повышенная производительность при более низком энергопотреблении важна для развертывания как в центре обработки данных, так и в тактических условиях. DARPA продемонстрировало обработку алгоритмов искусственного интеллекта с 1000-кратным ускорением и 1000-кратным КПД по сравнению с современными цифровыми процессорами. Также рассматривается специализированное обрудование для задач искусственного интеллекта [32, 33]. В фокусе также повышение эффективности машинного обучения и методы, позволяющие резко снизить требования к

размеченным обучающим данным [34].

Next Generation AI: алгоритмы машинного обучения, позволяющие распознавать лица и беспилотные автомобили, были изобретены более 20 лет назад. DARPA играет ведущую роль в новаторских исследованиях по разработке следующего поколения алгоритмов искусственного интеллекта, которые превратят компьютеры из инструментов в партнеров по решению проблем. Исследование DARPA направлено на то, чтобы позволить системам ИИ объяснять свои действия, а также приобретать и рассуждать на основе здравого смысла. DARPA R&D принесло первые успехи в области искусственного интеллекта, включая экспертные системы и поиск, а в последнее время разработало передовые инструменты и оборудование для машинного обучения. DARPA сейчас создает новую волну технологий искусственного интеллекта, которые позволят Соединенным Штатам сохранить свое технологическое превосходство в этой критически важной области. Здесь можно отметить, что объяснение результатов работы важно для устойчивого машинного обучения. Если наша система представляет собой черный ящик, то мы не можем доказывать какие-то ее свойства (просто по определению черного ящика). Соответственно, системы для критических применений, включая военную область, должны быть способны объяснять результаты работы [35]. И новые подходы (модели) также нужны для устойчивости, поскольку в современных архитектурах состязательные атаки неизбежны.

Указанный выше ресурс [31] содержит большой обновляемый список поддерживаемых DARPA программ (рис. 3) и технологий AI (рис. 4).

Рис. 3 Примеры программ DARPA [31]

Ongoing Efforts

- Artificial Intelligence Mitigations of Emergent Execution (AIMEE)
- Automating Scientific Knowledge Extraction (ASKE)
- Artificial Intelligence Research Associate (AIRA)
- Civil Sanctuary
- Context Reasoning for Autonomous Teaming (CREATE)
- Constructive Maching Learning Battles with Adversary Tactics (COMBAT)
- Cooperative Secure Learning (CSL)
- Ditto: Intelligent Auto-Generation and Composition of Surrogate
- ECoSystemic
- Gamebreaker
- Ground Artificial Intelligence Language Acquisition (GAILA)
- Hybrid AI to Protect Integrity of Open Source Code (SocialCyber)
- Hyper-Dimensional Data Enabled Neural Networks (HyDDENN)
- Intelligent Neural Interfaces (INI)

Рис. 4 Примеры технологий DARPA [31]

III. Военный искусственный интеллект в Европе

В этом разделе рассматриваются европейские проекты в области военного искусственного интеллекта.

В статьях отмечается, что финансирование таких работ в Европе отстает от США. В [37] упоминаются следующие направления: адаптивный камуфляж (что можно рассматривать и как физическую атаку на системы распознавания), коллективные роботы для разминирования [38], роботы для сухопутных войск [39], которые также могут действовать совместно. Рой роботов (рис. 5) – это активно исследуемая тема [40].

Рис.5.Коллективное использование дронов [41]

В [42] (исследовательская работа, выполненная по заказу вооруженных сил Швеции) рассматривается целый ряд технологий.

Морское наблюдение, которое осуществляется с помощью стационарных радиолокационных станций, патрульных самолетов, кораблей, средств электронного слежения – машинное обучение используется для выявления движений судов, которые могут быть незаконными, небезопасными, угрожающими и аномальными. Поиск таких аномалий осуществляется на основе Fuzzy ARTMAP - архитектуры нейронной сети представленной для инкрементального обучения с учителем распознаванию категорий и многомерных карт по входам в виде произвольных последовательностей аналоговых или двоичных входных векторов, которые могут представлять нечеткие или четкие функции [43]. Другой подход - ассоциативное обучение шаблонам движения для прогнозирования движения судна на основе его текущего местоположения и направления движения [44]. Другие модели используют обучение без учителя для неконтролируемая кластеризация на основе моделей гауссовой смеси (GMM) [45] и ядерной оценки плотности (KDE) [46]. Модели позволяют обнаруживать суда, которые меняют направление, пересекают морские пути, движутся в обратном направлении или с высокой скоростью. Также для определения аномального движения используются байесовские сети [47].

Другой рассматриваемый класс задач – это обнаружение подводных мин по результатам обследования дна подводными дронами с помощью глубинного обучения [48], а также использование синтетических данных для этого процесса [49].

Описывается также использование GAN (генеративных состязательных сетей) для

- Реконструкции - заполнении промежутков в частично закрытых изображениях или объектах [50].
- Увеличения разрешения: преобразование изображений из низкого разрешения в высокое [51].
- Преобразования изображения в изображение: преобразование изображений из зимы в лето, из ночного видения в изображения в дневном свете и т.д. [52].

Благодарности

Мы благодарны сотрудникам кафедры Информационной безопасности факультета Вычислительной математики и кибернетики МГУ имени М.В. Ломоносова за ценные обсуждения данной работы.

References

[1] Fatima, Samar, Kevin C. Desouza, and Gregory S. Dawson. "National strategic artificial intelligence plans: A multi-dimensional analysis." Economic Analysis and Policy 67 (2020): 178-194.

[2] He, Xin, Kaiyong Zhao, and Xiaowen Chu. "AutoML: A Survey of the State-of-the-Art." Knowledge-Based Systems 212 (2021): 106622.

[3] Namiot D., Ilyushin E., Chizhov I. Ongoing academic and industrial projects dedicated to robust machine learning //International Journal of Open Information Technologies. – 2021. – Т. 9. – №. 10. – С. 35-46.

[4] Namiot D., Ilyushin E., Chizhov I. The rationale for working on robust machine learning //International Journal of Open Information Technologies. – 2021. – Т. 9. – №. 11. – С. 68-74.

[5] Artificial Intelligence in Cybersecurity. http://master.cmc.msu.ru/?q=ru/node/3496 (in Russian) Retrieved: Sep, 2021.

[6] Neubert, Mitchell J., and George D. Montañez. "Virtue as a framework for the design and use of artificial intelligence." Business Horizons 63.2 (2020): 195-204.

[7] Daniel Hoadley and Nathan Lucas. 2018. Artificial Intelligence and National Security. https://www.a51.nl/sites/default/files/pdf/R45178.pdf Retrieved Nov, 2020

[8] Google AI Video https://cloud.google.com/video-intelligence Retrieved Nov, 2020

[9] Shane, Scott, and Daisuke Wakabayashi. "'The business of war': Google employees protest work for the Pentagon." The New York Times 4 (2018): 2018.

[10] Garcia-Garcia, Alberto, et al. "A survey on deep learning techniques for image and video semantic segmentation." Applied Soft Computing 70 (2018): 41-65.

[11] Wang, Wenguan, et al. "A survey on deep learning technique for video segmentation." arXiv preprint arXiv:2107.01153 (2021).

[12] Google Cloud & YouTube-8M Video Understanding Challenge https://www.kaggle.com/c/youtube8m Retrieved Nov, 2020

[13] R. B. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 580–587.

[14] Chen, Binghuang, and Xiren Miao. "Distribution line pole detection and counting based on YOLO using UAV inspection line video." Journal of Electrical Engineering & Technology 15.1 (2020): 441-448.

[15] Куприяновский В. П. и др. Цифровая трансформация экономики, железных дорог и умных городов. Планы и опыт Великобритании //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 10. – С. 22-31.

[16] Куприяновский В. П. и др. Экономические выгоды применения комбинированных моделей BIM-ГИС в строительной отрасли. Обзор состояния в мире //International Journal of Open Information Technologies. – 2016. – Т. 4. – №. 5. – С. 14-25.

[17] Joshi, Kinjal A., and Darshak G. Thakore. "A survey on moving object detection and tracking in video surveillance system." International Journal of Soft Computing and Engineering 2.3 (2012): 44-48.

[18] Ciaparrone, Gioele, et al. "Deep learning in video multi-object tracking: A survey." Neurocomputing 381 (2020): 61-88.

[19] Du, Juan. "Understanding of object detection based on CNN family and YOLO." Journal of Physics: Conference Series. Vol. 1004. No. 1. IOP Publishing, 2018.

[20] Masi, Iacopo, et al. "Deep face recognition: A survey." 2018 31st SIBGRAPI conference on graphics, patterns and images (SIBGRAPI). IEEE, 2018.

[21] Arsenovic, Marko, et al. "Deep learning driven plates recognition system." Proc. 17th Int. Sci. Conf. Ind. Syst.(IS). 2017.

[22] Li, Shasha, et al. "Stealthy Adversarial Perturbations Against Real-Time Video Classification Systems." NDSS. 2019.

[23] Murshed, MG Sarwar, et al. "Machine learning at the network edge: A survey." ACM Computing Surveys (CSUR) 54.8 (2021): 1-37.

[24] Li, Ying, et al. "Deep learning for remote sensing image classification: A survey." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 8.6 (2018): e1264.

[25] Lateef, Fahad, and Yassine Ruichek. "Survey on semantic segmentation using deep learning techniques." Neurocomputing 338 (2019): 321-348.

[26] Wang, Li, and Dennis Sng. "Deep learning algorithms with applications to video analytics for a smart city: A survey." arXiv preprint arXiv:1512.03131 (2015).

[27] Ahmed, Imran, et al. "Towards collaborative robotics in top view surveillance: A framework for multiple object tracking by detection using deep learning." IEEE/CAA J. Autom. Sinica (2020).

[28] J. Harper and S. Magnuson, ''The three waves of AI,'' Nat. Defense, vol. 102, no. 774, p. 6, 2018

[29] Wang, Wei, et al. "Investigation on Works and Military Applications of Artificial Intelligence." IEEE Access 8 (2020): 131614-131625.

[30] Y. Tadjdeh, ''DARPA's 'AI next' program bearing fruit,'' Nat. Defense, vol. 104, no. 788, p. 8, 2019.

[31] AI Next Campaign https://www.darpa.mil/work-with-us/ai-next-campaign Retrieved: Dec, 2021

[32] Reuther, Albert, et al. "Survey and benchmarking of machine learning accelerators." 2019 IEEE high performance extreme computing conference (HPEC). IEEE, 2019.

[33] Schneider, Ethan. "Hardware Architectures for Accelerating Machine Learning & a Deeper Dive into CUDA and Tensor Cores."

[34] Jin, Charles, and Martin Rinard. "Towards Context-Agnostic Learning Using Synthetic Data." Advances in Neural Information Processing Systems 34 (2021).

[35] Došilović, Filip Karlo, Mario Brčić, and Nikica Hlupić. "Explainable artificial intelligence: A survey." 2018 41st International convention on information and communication technology, electronics and microelectronics (MIPRO). IEEE, 2018.

[36] AI-Enabled Drone Shows US Army It Can Localize Targets https://www.thedefensepost.com/2021/01/26/ssci-ai-enabled-drone/ Retrieved: Dec, 2021

[37] Europe hopes new R&D fund will boost meager defense capabilities and create opportunities for science https://www.science.org/content/article/europe-hopes-new-rd-fund-will-boost-meager-defense-capabilities-and-create Retrieved: Dec, 2021

[38] AIDED https://ec.europa.eu/commission/presscorner/detail/en/fs_20_1094 Retrieved: Dec, 2021

[39] ARTUS https://ec.europa.eu/commission/presscorner/detail/en/fs_20_1095 Retrieved: Dec, 2021

[40] Hüttenrauch, Maximilian, Sosic Adrian, and Gerhard Neumann. "Deep reinforcement learning for swarm systems." Journal of Machine Learning Research 20.54 (2019): 1-31.

[41] Drone Swarm performance and applications https://www.embention.com/news/drone-swarm-performance-and-applications/ Retrieved: Dec, 2021

[42] Svenmarck, Peter, et al. "Possibilities and challenges for artificial intelligence in military applications." Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting. Neuilly-sur-Seine France, 2018.

[43] Bradley J Rhodes, Neil A Bomberger, Michael Seibert, and Allen M Waxman. Maritime situation monitoring and awareness using learning mechanisms. In Military Communications Conference, MILCOM, pages 646–652. IEEE, 2005

[44] Bradley J Rhodes, Neil A Bomberger, and Majid Zandipour. Probabilistic associative learning of vessel motion patterns at multiple spatial scales for maritime situation awareness. In Information Fusion, 2007 10th International Conference on, pages 1–8. IEEE, 2007

[45] Rikard Laxhammar. Anomaly detection for sea surveillance. In Information Fusion, 2008 11th International Conference on, pages 1–8. IEEE, 2008.

[46] Rikard Laxhammar, Goran Falkman, and Egils Sviestins. Anomaly detection in sea traffic-a comparison of the gaussian mixture model and the kernel density estimator. In Information Fusion, 2009. FUSION'09. 12th International Conference on, pages 756–763. IEEE, 2009.

[47] Steven Mascaro, Ann E Nicholso, and Kevin B Korb. Anomaly detection in vessel tracks using bayesian networks. International Journal of Approximate Reasoning, 55(1):84–98, 2014.

[48] David P Williams. Underwater target classification in synthetic aperture sonar imagery using deep convolutional neural networks. In Pattern Recognition (ICPR), 2016 23rd International Conference on, pages 2497–2502. IEEE, 2016.

[49] Killian Denos, Mathieu Ravaut, Antoine Fagette, and Hock-Siong Lim. Deep learning applied to underwater mine warfare. In OCEANS 2017-Aberdeen, pages 1–7. IEEE, 2017.

[50] Bo Yang, Hongkai Wen, Sen Wang, Ronald Clark, Andrew Markham, and Niki Trigoni. 3d object reconstruction from a single depth view with adversarial learning. In International Conference on Computer Vision Workshops(ICCVW), 2017.

[51] Christian Ledig, Lucas Theis, Ferenc Huszar, Jose Caballero, Andrew Cunningham, Alejandro Acosta, Andrew P. Aitken, Alykhan Tejani, Johannes Totz, Zehan Wang, and Wenzhe Shi. Photo-realistic single image super-resolution using a generative adversarial network. In 2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017, pages 105–114, 2017.

[52] Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A Efros. Unpaired image-to-image translation using cycle-consistent adversarial networks. arXiv preprint arXiv:1703.10593, 2017.

Military applications of machine learning

Dmitry Namiot, Eugene Ilyushin, Ivan Chizhov

Abstract— **This article is devoted to the applied aspects of the application of machine learning systems. It is obvious that the areas of practical applications of this kind of solution are constantly increasing. The main driver here is that, from a practical point of view, machine learning is seen as a synonym for the concept of artificial intelligence, the introduction of which in developed countries is dedicated to special programs. Naturally, military applications are also considered among such implementations. And here an interesting feature can be noted. If earlier, the military areas served as an impetus for the development of technology, the search for solutions for military equipment was ordered, etc., then in this case everything is rather moving in the opposite direction. First, new solutions (developments) that use a machine (deep) learning appear, and then they begin to be used, including in military systems. The article provides an overview of published military programs for the use of artificial intelligence in the military sphere, which is compiled with the aim of presenting precisely the technologies and solutions in the fields of machine learning that are applied (are used) for military systems.**

Keywords—machine learning, explainability, interpretability, inference

REFERENCES

[1] Fatima, Samar, Kevin C. Desouza, and Gregory S. Dawson. "National strategic artificial intelligence plans: A multi-dimensional analysis." Economic Analysis and Policy 67 (2020): 178-194.
[2] He, Xin, Kaiyong Zhao, and Xiaowen Chu. "AutoML: A Survey of the State-of-the-Art." Knowledge-Based Systems 212 (2021): 106622.
[3] Namiot D., Ilyushin E., Chizhov I. Ongoing academic and industrial projects dedicated to robust machine learning //International Journal of Open Information Technologies. – 2021. – T. 9. – #. 10. – S. 35-46.
[4] Namiot D., Ilyushin E., Chizhov I. The rationale for working on robust machine learning //International Journal of Open Information Technologies. – 2021. – T. 9. – #. 11. – S. 68-74.
[5] Artificial Intelligence in Cybersecurity. http://master.cmc.msu.ru/?q=ru/node/3496 (in Russian) Retrieved: Sep, 2021.
[6] Neubert, Mitchell J., and George D. Montañez. "Virtue as a framework for the design and use of artificial intelligence." Business Horizons 63.2 (2020): 195-204.
[7] Daniel Hoadley and Nathan Lucas. 2018. Artificial Intelligence and National Security. https://www.a51.nl/ sites/default/files/pdf/R45178.pdf Retrieved Nov, 2020
[8] Google AI Video https://cloud.google.com/video-intelligence Retrieved Nov, 2020
[9] Shane, Scott, and Daisuke Wakabayashi. "'The business of war': Google employees protest work for the Pentagon." The New York Times 4 (2018): 2018.
[10] Garcia-Garcia, Alberto, et al. "A survey on deep learning techniques for image and video semantic segmentation." Applied Soft Computing 70 (2018): 41-65.
[11] Wang, Wenguan, et al. "A survey on deep learning technique for video segmentation." arXiv preprint arXiv:2107.01153 (2021).
[12] Google Cloud & YouTube-8M Video Understanding Challenge https://www.kaggle.com/c/youtube8m Retrieved Nov, 2020
[13] R. B. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in IEEE Conference on Computer Vision and Pattern Recognition, 2014, pp. 580–587.
[14] Chen, Binghuang, and Xiren Miao. "Distribution line pole detection and counting based on YOLO using UAV inspection line video." Journal of Electrical Engineering & Technology 15.1 (2020): 441-448.
[15] Kuprijanovskij V. P. i dr. Cifrovaja transformacija jekonomiki, zheleznyh dorog i umnyh gorodov. Plany i opyt Velikobritanii //International Journal of Open Information Technologies. – 2016. – T. 4. – #. 10. – S. 22-31.
[16] Kuprijanovskij V. P. i dr. Jekonomicheskie vygody primenenija kombinirovannyh modelej BIM-GIS v stroitel'noj otrasli. Obzor sostojanija v mire //International Journal of Open Information Technologies. – 2016. – T. 4. – #. 5. – S. 14-25.
[17] Joshi, Kinjal A., and Darshak G. Thakore. "A survey on moving object detection and tracking in video surveillance system." International Journal of Soft Computing and Engineering 2.3 (2012): 44-48.
[18] Ciaparrone, Gioele, et al. "Deep learning in video multi-object tracking: A survey." Neurocomputing 381 (2020): 61-88.
[19] Du, Juan. "Understanding of object detection based on CNN family and YOLO." Journal of Physics: Conference Series. Vol. 1004. No. 1. IOP Publishing, 2018.
[20] Masi, Iacopo, et al. "Deep face recognition: A survey." 2018 31st SIBGRAPI conference on graphics, patterns and images (SIBGRAPI). IEEE, 2018.
[21] Arsenovic, Marko, et al. "Deep learning driven plates recognition system." Proc. 17th Int. Sci. Conf. Ind. Syst.(IS). 2017.
[22] Li, Shasha, et al. "Stealthy Adversarial Perturbations Against Real-Time Video Classification Systems." NDSS. 2019.
[23] Murshed, MG Sarwar, et al. "Machine learning at the network edge: A survey." ACM Computing Surveys (CSUR) 54.8 (2021): 1-37.
[24] Li, Ying, et al. "Deep learning for remote sensing image classification: A survey." Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery 8.6 (2018): e1264.
[25] Lateef, Fahad, and Yassine Ruichek. "Survey on semantic segmentation using deep learning techniques." Neurocomputing 338 (2019): 321-348.
[26] Wang, Li, and Dennis Sng. "Deep learning algorithms with applications to video analytics for a smart city: A survey." arXiv preprint arXiv:1512.03131 (2015).
[27] Ahmed, Imran, et al. "Towards collaborative robotics in top view surveillance: A framework for multiple object tracking by detection using deep learning." IEEE/CAA J. Autom. Sinica (2020).
[28] J. Harper and S. Magnuson, ''The three waves of AI,'' Nat. Defense, vol. 102, no. 774, p. 6, 2018
[29] Wang, Wei, et al. "Investigation on Works and Military Applications of Artificial Intelligence." IEEE Access 8 (2020): 131614-131625.
[30] Y. Tadjdeh, ''DARPA's 'AI next' program bearing fruit,'' Nat. Defense, vol. 104, no. 788, p. 8, 2019.
[31] AI Next Campaign https://www.darpa.mil/work-with-us/ai-next-campaign Retrieved: Dec, 2021
[32] Reuther, Albert, et al. "Survey and benchmarking of machine learning accelerators." 2019 IEEE high performance extreme computing conference (HPEC). IEEE, 2019.
[33] Schneider, Ethan. "Hardware Architectures for Accelerating Machine Learning & a Deeper Dive into CUDA and Tensor Cores."
[34] Jin, Charles, and Martin Rinard. "Towards Context-Agnostic Learning Using Synthetic Data." Advances in Neural Information Processing Systems 34 (2021).
[35] Došilović, Filip Karlo, Mario Brčić, and Nikica Hlupić. "Explainable artificial intelligence: A survey." 2018 41st International convention on information and communication technology, electronics and microelectronics (MIPRO). IEEE, 2018.
[36] AI-Enabled Drone Shows US Army It Can Localize Targets https://www.thedefensepost.com/2021/01/26/ssci-ai-enabled-drone/ Retrieved: Dec, 2021
[37] Europe hopes new R&D fund will boost meager defense capabilities and create opportunities for science https://www.science.org/content/article/europe-hopes-new-rd-fund-will-boost-meager-defense-capabilities-and-create Retrieved: Dec, 2021
[38] AIDED https://ec.europa.eu/commission/presscorner/detail/en/fs_20_1094 Retrieved: Dec, 2021
[39] ARTUS https://ec.europa.eu/commission/presscorner/detail/en/fs_20_1095 Retrieved: Dec, 2021

[40] Hüttenrauch, Maximilian, Sosic Adrian, and Gerhard Neumann. "Deep reinforcement learning for swarm systems." Journal of Machine Learning Research 20.54 (2019): 1-31.
[41] Drone Swarm performance and applications https://www.embention.com/news/drone-swarm-performance-and-applications/ Retrieved: Dec, 2021
[42] Svenmarck, Peter, et al. "Possibilities and challenges for artificial intelligence in military applications." Proceedings of the NATO Big Data and Artificial Intelligence for Military Decision Making Specialists' Meeting. Neuilly-sur-Seine France, 2018.
[43] Bradley J Rhodes, Neil A Bomberger, Michael Seibert, and Allen M Waxman. Maritime situation monitoring and awareness using learning mechanisms. In Military Communications Conference, MILCOM, pages 646–652. IEEE, 2005
[44] Bradley J Rhodes, Neil A Bomberger, and Majid Zandipour. Probabilistic associative learning of vessel motion patterns at multiple spatial scales for maritime situation awareness. In Information Fusion, 2007 10th International Conference on, pages 1–8. IEEE, 2007
[45] Rikard Laxhammar. Anomaly detection for sea surveillance. In Information Fusion, 2008 11th International Conference on, pages 1–8. IEEE, 2008.
[46] Rikard Laxhammar, Goran Falkman, and Egils Sviestins. Anomaly detection in sea traffic-a comparison of the gaussian mixture model and the kernel density estimator. In Information Fusion, 2009. FUSION'09. 12th International Conference on, pages 756–763. IEEE, 2009.
[47] Steven Mascaro, Ann E Nicholso, and Kevin B Korb. Anomaly detection in vessel tracks using bayesian networks. International Journal of Approximate Reasoning, 55(1):84–98, 2014.
[48] David P Williams. Underwater target classification in synthetic aperture sonar imagery using deep convolutional neural networks. In Pattern Recognition (ICPR), 2016 23rd International Conference on, pages 2497–2502. IEEE, 2016.
[49] Killian Denos, Mathieu Ravaut, Antoine Fagette, and Hock-Siong Lim. Deep learning applied to underwater mine warfare. In OCEANS 2017-Aberdeen, pages 1–7. IEEE, 2017.
[50] Bo Yang, Hongkai Wen, Sen Wang, Ronald Clark, Andrew Markham, and Niki Trigoni. 3d object reconstruction from a single depth view with adversarial learning. In International Conference on Computer Vision Workshops(ICCVW), 2017.
[51] Christian Ledig, Lucas Theis, Ferenc Huszar, Jose Caballero, Andrew Cunningham, Alejandro Acosta, Andrew P. Aitken, Alykhan Tejani, Johannes Totz, Zehan Wang, and Wenzhe Shi. Photo-realistic single image super-resolution using a generative adversarial network. In 2017 IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, Honolulu, HI, USA, July 21-26, 2017, pages 105–114, 2017.
[52] Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A Efros. Unpaired image-to-image translation using cycle-consistent adversarial networks. arXiv preprint arXiv:1703.10593, 2017.

.