В настоящее время США, Китай, Великобритания, Франция, Израиль, Индия и ряд других стран реализуют национальные военные программы, предусматривающие применение искусственного интеллекта (ИИ) как в системах управления войсками и оружием, так и в отдельных образцах вооружения и военной техники (ВВТ). В общем случае под этим термином можно понимать способность какого-либо искусственно созданного объекта, например, цифровой вычислительной системы обучаться для решения определенного класса задач. Обычно они рассматриваются как творческие или аналитические, так и трудно формализуемые в виде ограниченного набора решающих правил, ранее их решение традиционно считалось прерогативой человека. В исследовании "Искусственный интеллект и национальная безопасность", выполненном для конгресса США в 2019 году (Artifi cial Intelligence and National Security - Congressional Research Service Report R45178 от 21.11.2019 года - AINS), утверждается, что главной причиной создания различных систем военного назначения, обладающих ИИ, является необходимость оперативной обработки структурированных и неструктурированных данных огромных объемов (так называемых больших данных), обусловленная постоянным расширением числа, номенклатуры и технических возможностей современных средств добывания информации. Причем эти сведения могут представляться в разнообразной форме, включая фото-, видео- и радиолокационные изображения, а также аудио- и текстовые сообщения на разных языках, данные, полученные из киберпространства, и т. д. Там же отмечается, что ИИ в ближайшем будущем распространится во всех видах боевой и обеспечивающей деятельности вооруженных сил (ВС). Согласно прогнозу американской компании "Маркетс энд маркетс рисёрч", ежегодный рост до 2025 года мирового рынка систем и средств ИИ составит порядка 14,75% Основную роль в этом будут играть США, а ключевыми производителями оборудования и программного обеспечения станут американские компании "Локхид-Мартин", "Рейтеон", "Нортроп-Грумман", "АйБиЭМ" (IBM), "Дженерал дайнэмикс", "Нвидиа", английская компания "БАэ системз" и французская "Талес". В то же время согласно "Плану развития систем искусственного интеллекта в Китае" (принят в 2017 году), к 2030-му КНР должна стать мировым лидером в технологии ИИ, в том числе, применяемой в ВВТ.

Основным способом реализации технологий, широко применяемых сегодня в том числе при создании систем искусственного интеллекта военного назначения, является искусственная нейронная сеть (ИНС), представляющая собой набор отдельных цифровых вычислительных элементов - нейронов, обычно расположенных на нескольких последовательных слоях сети. При этом она не программируется в привычном смысле этого слова, а обучается. Эта особенность - главное преимущество ИНС перед традиционными алгоритмами вычислений. В процессе обучения нейронная сеть способна выявлять сложные зависимости между входными данными и выходными, а также выполнять обобщение. Она с высокой вероятностью сможет получить корректный результат на основании данных, которые отсутствовали в обучающей выборке, неполных и/или "зашумленных", а также частично искаженных. В зарубежных публикациях перечисляется широкий круг задач, для эффективного решения которых в ВС целесообразно использовать системы с ИИ. Так, указывается, что подобные системы будут наиболее полезны в разведке, а также при идентификации объектов в процессе обработки видео- и фотоматериалов, получаемых со средств видовой разведки. Кроме того, в ходе обучения на нейронную сеть подается большой массив специально подготовленных изображений, требуемых объектов разведки (например, летательных аппаратов, кораблей, различных видов оружия, физических лиц и т. д.), сделанных под различными углами, освещением и в различном окружении. Нейросеть анализирует характерные признаки изображения (линии, их соединения, формы, цвет, размер и т. п.) и строит модель распознавания, обеспечивающую идентификацию объектов с минимально допустимым уровнем ошибок первого и второго рода. В развитых странах уже сейчас существуют образцы вооружений, реализующие описанные возможности ИИ. Так, в начале 2020 года компания "Рейтеон" объявила о развертывании системы разведки, наблюдения и целеуказания "Истар" (ISTAR - Intelligence Surveillance Target Acquisition and Reconnaissance) на самолетах ВВС Великобритании "Сентинел".

Данная система обладает ИИ и обеспечивает:

- обнаружение интересующих наземных и морских объектов и наблюдение за их перемещением;
- формирование карты местности контролируемых районов;
- оценку оперативной ситуации путем контроля активности перемещения различных объектов.

Подобными возможностями обладают системы разведки, наблюдения и целеуказания на базе беспилотного летательного аппарата (БПЛА) MQ-4C "Тритон", стоящего на вооружении ВМС США.

Другими задачами, возлагаемыми на системы с искусственным интеллектом, являются определение типа обнаруженного радиосигнала и излучающего его радиопередающего средства при ведении радиоэлектронной разведки, распознавание и перевод многоязычной речи в неблагоприятных условиях акустической обстановки, формирование геопространственных сведений из разрозненных неструктурированных геоданных, оценка назначения и характеристик различных объектов по результатам их наблюдения, обработка двухмерных изображений объектов для получения трехмерных. По программе "Блэйд" (BLADE - Behavioral Learning for Adaptive Electronic Warfare System), выполняемой для агентства перспективных исследований Пентагона ДАРПА (DARPA), компанией "Локхид-Мартин" разрабатывается система радиоэлектронной борьбы, предназначенная для автоматического подавления средств радиосвязи противника с непрерывной оценкой ее эффективности с целью преодоления возможных мер противодействия. Утверждается, что ИИ играет ключевую роль в обеспечении эффективности создаваемой системы. Следующей важной прикладной областью применения ИНС в военном деле является киберпространство. В AINS указывается, что ИИ является ключевым элементом, обеспечивающим выполнение самых сложных киберопераций. Его алгоритмы, реализованные в искусственной нейронной сети, могут автоматически определять наличие угроз, оценивать их опасность, модифицировать с целью защиты от них собственное программное обеспечение. По оценке специалистов ДАРПА, выполнение всех этих операций измеряется секундами, а не месяцами, что характерно при задействовании большого штата экспертов в соответствующих областях компьютерных знаний. Потенциально киберсистемы с ИИ способны одновременно решать задачи киберзащиты и кибернападения. Известно об успешных экспериментах, проводимых китайской корпорацией "Тенцент" с целью несанкционированного доступа к ИНС, распознающих различные объекты. Целью такого доступа является сокрытие или подмена объекта распознавания. Специально для защиты от подобного вредоносного воздействия на нейронную сеть, вызывающего ошибки в ее поведении, в ДАРПА существуют специальные программы "Гард" (GARD - Guaranteeing AI Robustness against Deception) по разработке аппаратно-программных средств, обеспечивающих гарантированную устойчивость систем с ИИ от попыток их взлома. Экспертами по кибербезопасности предлагается использовать методы шифрования кодов исполняемых в ИНС программ для защиты от кибернападения.

Еще одним направлением использования систем с искусственным интеллектом являются информационные операции. Уже сейчас они умеют формировать поддельные фото-, аудио-, видеоматериалы, причем встраивая в них реальные элементы обстановки и реальных действующих лиц, создают в Интернете ложные профили вымышленных или настоящих людей с поддержкой ретроспективы их семейных отношений, образования, карьеры, связей, кредитной истории и т. д. Данные технологии могут использоваться для создания ложных, так называемых фейковых новостей в средствах массовой информации, разработки легенд оперативным сотрудникам, дискредитации определенных лиц или их шантажа. Известен проект "Медифор" (MediFor - Media Forensics) агентства ДАРПА по противодействию подобным системам, направленный на вскрытие и документирование фактов их применения. Однако известно, что интеллектуальные средства создания ложной информации также могут обладать способностью обучения методам противодействия способам их обнаружения. Существует еще одно важное направление развития военных систем, обладающих искусственным интеллектом, - централизованное планирование и координация проведения военных операций различного масштаба в воздушном, космическом, кибер, морском и наземном пространстве. В зарубежной литературе подобные действия получили название "многосферное управление и контроль" (Multi-Domain Command and Control - MDC). Путем сбора и обработки всей доступной информации, полученной от различных источников, предлагается создавать интегрированный источник информации, так называемую глобальную оперативную картину, на основе которой командирам различного уровня будут автоматически предлагаться наиболее эффективные варианты действий для достижения целей операции. Известно о разработке подобных систем в интересах ВВС США компаниями "Локхид-Мартин" и "Харрис". Кроме того, следует отметить, что различные автоматизированные системы поддержки принятия решений и компьютерного моделирования оперативной обстановки в ВС развитых стран широко применялись с 70-х годов прошлого столетия, но эти системы не обладали возможностью обучения и, соответственно, искусственным интеллектом. Одними из первых используемых на практике военных средств с ИИ стали имитационные тренажеры, применяемые для обучения операторов различных военных машин. Целью имитации являлось воссоздание реальных условий боевой обстановки, например, путем формирования соответствующего видео- и звукового контента для загрузки на устройства отображения информации в процессе подготовки оператора и изменение этих условий в ответ на его действия. В настоящее время наиболее широко ИИ используется в военной логистике ВС США. Такие системы уже сейчас применяются для оценки потенциальных потребностей в запчастях, определения наиболее рациональных по времени выполнения и стоимости способов их доставки. Принцип их работы заключается в автоматическом анализе технических параметров, получаемых от различных датчиков, размещенных в средствах вооружения, с целью определения необходимости и объема проведения операций обслуживания или ремонта военной техники. Американскими военными специалистами отмечается, что логистические военные системы с ИИ обеспечивают более эффективную организацию операций по критериям количество удовлетворенных заявок/стоимость логистических операций/продолжительность их проведения.