Концепция IoBT (Интернет вещей на поле битвы) все еще находится на начальной стадии, и предпринимаются значительные усилия в области исследований и разработок (R&D) для практической реализации IoBT по всему миру.

Недавно в Национальном университете оборонных технологий (Чанша, Китай) было проведено исследование (Фэн и др., 2020), целью которого было изучение устойчивости IoBT в направленной сети. Были сделаны несколько важных выводов:

* Способность поддерживать сетевое подключение при атаке противника является критически важным свойством IoBT-сетей.
* С использованием модели сети был проведен анализ устойчивости IoBT-сети при оптимальной атакующей стратегии, что дало представление о разработке эффективных стратегий для обеспечения безопасности и санитарной обработки IoBT-сети несмотря на вмешательство противника.
* Гетерогенность устройств и гетерогенные многослойные сети увеличивают сложность IoBT.

Аналогично, Исследовательская лаборатория армии США, находящаяся в подчинении Командования будущего армии (Army Futures Command), учредила Союз для совместных исследований (CRA) для разработки нишевых технологий, включая IoBT, искусственный интеллект, кибербезопасность, робототехнику и т. д. CRA IoBT (DEVCOM) ориентирован на усиление коммерческих исследований IoT с междисциплинарными науками для решения армейских задач, особенно в условиях операций в высоко динамичных, ограниченных ресурсах и враждебных средах.

**Манифестация IoBT в Вооруженных Силах Индии**

Учитывая угрозу национальной безопасности как с Запада, так и с Севера, необходимо оперативное обновление военных возможностей Индии. В условиях огромных требований к модернизации оборудования и других оперативных и логистических проблем, использование нишевых технологий, таких как робототехника, искусственный интеллект (ИИ) и IoBT, еще не получило широкого распространения. Тем не менее, ограниченное использование таких технологий уже началось в некоторых критически важных формированиях с использованием коммерчески доступного оборудования.

В контексте Индии исследования и разработки (R&D) в области IoBT все еще находятся на начальной стадии. Это требует неотложного внимания, особенно с учетом размера экономики страны и того факта, что Индия уже занимает значительное место на мировой арене, и многие страны, особенно из Глобального Юга, рассматривают Индию как своего лидера.

Технология 5G является основой для внедрения IoBT, и ее повсеместное распространение будет иметь решающее значение для быстрого обмена информацией в сети IoBT. Исследовательская площадка индийских исследований 5G в IIT Мадрасе (TOI, 2022) разработала полные решения "от конца до конца", которые могут быть настроены и включают безопасный чип NB-IoT. Необходимо внедрять отечественные решения 5G, которые смогут работать в различных типах местности, при этом используя существующие радиосвязь, оптоволоконные и спутниковые каналы связи.

**Проект Сети для Спектра (NFS)**

В 2012 году в рамках проекта "Сеть для спектра" (NFS) Министерство обороны (MoD) и Департамент телекоммуникаций (DoT) Индии разработали концепцию сети для соединения критически важных оборонных объектов. Проект включает создание сети на основе оптоволоконных кабелей (OFC), предназначенной исключительно для оборонной связи. Оптоволоконные кабели были проложены по всей стране, включая участки с разнообразными рельефами, с использованием технологий защиты от вторжений, мониторинга сети и ГИС-картографирования, что делает эту сеть одной из самых передовых и защищенных для вооруженных сил. Эту инфраструктуру можно будет использовать для создания IoBT-сети, предназначенной исключительно для нужд вооруженных сил.

В рамках лозунга «Атманирбхар Бхарат» (Самодостаточная Индия) Министерство оборонного производства (MoD) реализует несколько новых проектов. Согласно отчетам за июль 2022 года, разрабатываются несколько проектов, интегрированных с искусственным интеллектом (ИИ). Некоторые из них приведены ниже:

* **iSentinel** — Интеллектуальная автоматизированная система отслеживания и идентификации угроз. Разработанная как система наблюдения для борьбы с террористическими угрозами в пограничной и контртеррористической (CI/CT) среде, iSentinel представляет собой систему обнаружения и отслеживания угроз на основе глубокого обучения. Она может быть эффективно интегрирована с Системами Анти-Инфильтрации (AIOS) с целью противодействия трансграничному терроризму.
* **Умные шлемы**. Для обеспечения реального ситуационного осведомления в боевых условиях разработан «Умный шлем», который в реальном времени может захватывать 3D-данные о неизвестной местности и помогать в принятии различных решений. «Умный шлем» включает оптический сенсор, установленный на шлеме солдата, и может быть эффективно использован в специальных операциях на линии соприкосновения (LC) и в управлении границами на северных рубежах. Это устройство помогает отслеживать потенциальные угрозы, а также местоположение собственных войск в неизвестной местности, обеспечивая полное situational awareness для принятия решений.
* **Механизм разрешенной блокчейн-технологии**. Это решение предназначено для создания доверенной платформы связи с использованием блокчейн-технологии. Идея заключается в создании защищенной сети для передачи данных между различными субъектами. Эта технология будет неотъемлемой частью IoBT-сети, обеспечивая прозрачность, безопасность и возможность аудита данных среди участников сети.

Эти инициативы являются важными шагами в направлении создания высокотехнологичной и защищенной инфраструктуры для вооруженных сил Индии, а также для развития сетей IoBT в будущем.

**Реализация IoBT в Индийской армии**

С учетом текущего прогресса в рамках инициативы **«Атманирбхар Бхарат»** и **«Года технической абсорбции»** Индийской армии, существует настоятельная необходимость интегрировать выводы из различных передовых технологий, таких как искусственный интеллект (ИИ), робототехника, дроны, глубокое обучение, блокчейн и Интернет вещей (IoT). Эти технологии должны быть использованы для разработки индивидуальных решений для конкретных оперативных задач, таких как контртеррористические и контрповстанческие операции (CI/CT) или борьба с китайской угрозой в высокогорных районах (HAA) вдоль северных границ Индии.

**Будущие изменения в ведении войны для Индийской армии**

Интеграция нишевых технологий в военные действия существенно изменит способы, которыми Индийская армия будет действовать в ближайшем будущем. Вооруженные силы должны сосредоточиться на **«подходе снизу-вверх»**, позволяя даже самым маленьким подразделениям работать с интеллектуальными системами. Однако реализация **IoBT**, где солдаты и машины взаимодействуют для формирования специализированных единиц или команд для выполнения конкретных задач, сопряжена с рядом проблем. Эти проблемы потребуют изменений в подходе, обучении и организации, некоторые из которых приведены ниже:

1. **Подход к ведению войны**
   * Необходимость принять более **целостный подход к ведению войны**, который включает изменения в тактике и методах из-за появления новых технологий. Руководители, младшие командиры и солдаты на местах должны ознакомиться с управлением и использованием этих технологий в условиях быстрого темпа и уязвимой среды.
   * В настоящее время Индийские вооруженные силы действуют через конкретные роды войск и службы. Однако существует растущая потребность в **разрушении изолированных подходов** и большей **совместимости** в операциях, используя возможности **сильно связанную IoBT-сеть**.
2. **Информационная война**
   * В современных условиях **информация** стала одним из самых мощных оружий. Чтобы соответствовать этим изменениям, вооруженные силы должны развивать **культуру, ориентированную на информацию**, акцентируя внимание на процедурах **сбора, обработки и распространения данных** с помощью IoBT-сети. Такой подход обеспечит использование информации как решающего элемента в операциях.
3. **Человек против машины**
   * Внедрение **автономных систем**, таких как роботы, роя дронов и БПЛА, представляет собой значительную проблему, особенно в области **сотрудничества человека и машины**. Основная проблема заключается в риске исключения людей из процесса принятия решений. Хотя автономные системы могут обеспечивать огромные возможности, **человеческая логика и суждения** не могут быть полностью заменены машинным интеллектом в военных действиях.
   * Поэтому важно, чтобы **право на принятие решений** оставалось за командующими в рамках **цикла OODA (Наблюдать, Ориентироваться, Решать, Действовать)**, даже если IoBT-сети будут оснащены **искусственно интеллектуальными датчиками** и **умным оружием**, способными обеспечивать быстрый и мощный огонь.

Эти вызовы подчеркивают необходимость сбалансированного подхода, который обеспечит, чтобы IoBT усиливал возможности Индийской армии, но при этом человеческое руководство и принятие решений оставались центральными для эффективных операций. Интеграция IoBT существенно изменит способы, которыми армия будет действовать, обеспечивая лучшее оснащение для противостояния современным угрозам в реальном времени и в условиях высокого риска.

**Независимое облако для вооруженных сил**

Индийская армия запустила высоко зашифрованное «Облако армии» как часть своей инициативы по поглощению технологий, следуя примеру облачного сервиса **«Мегх Радж»** Национального центра информатики. «Облако армии», вместе с проектом **Сеть для спектра** (NFS), произведет революцию в стратегическом принятии решений на самом высоком уровне, как только умные датчики будут интегрированы, чтобы предоставить всестороннюю картину поля боя в реальном времени.

**Фокус на специализацию**

Исследования и разработки в области новых технологий требуют, чтобы офицеры специализировались в данной области. Инновации, будучи важным аспектом, требуют от специалистов значительного времени для завершения проекта. Недавно армия внедрила кадровую политику (Датта, 2024), согласно которой офицеры, специализирующиеся в нишевых технологиях, могут продолжать работать в своей области при повышении до полковника, а не быть переведенными на командные должности. Такие политики стимулируют исследования и разработки нишевых технологий и способствуют быстрому превращению армии в технологически превосходную силу. Подобные усилия могут быть предприняты на уровне трех видов вооруженных сил.

**Аспекты подготовки**

Помимо исследований и разработок, также важно обучать тактических командиров, младших лидеров и солдат на местах эффективно использовать нишевые технологии во время активных операций. Ручные военные игры использовались долгое время. Однако с развитием новых технологий требуется новый подход к обучению. Можно ввести компьютерные военные игры, которые будут моделировать различные возможные сценарии, такие как кибератаки, подавление связи, война с дронами, усиленные операции с использованием сети IoBT и другие.

**Кибербезопасность**

Поскольку будущие бои будут вестись с использованием машин, соединенных через различные сети, кибербезопасность приобретает особое значение. Мы уже живем в эпоху, когда войны ведутся не только на поле боя, но и за его пределами, как это можно было наблюдать в контексте войны России с Украиной, конфликтов на Ближнем Востоке или даже пандемии COVID-19.

**Заключение**

IoBT как технология непременно окажет всестороннее влияние на будущее поле боя. Будучи быстро развивающейся нацией и одной из самых сильных военных держав мира, Индия несет ответственность за разработку и внедрение этой технологии на своём преимуществе как можно скорее. Сочетание IoBT с другими нишевыми технологиями будет действовать как мультипликатор силы и позволит нашим вооруженным силам вести будущие сражения в реальном времени.