

DOI 10.35775/PSI.2025.116.4.034

УДК 32.327

Н.А. НИКИТИН

аспирант Дипломатической академии МИД России;

Главный специалист Управления международного сотрудничества

Российской академии наук, Россия, г. Москва

E-mail: nikitanikitin@internet.ru

РАЗВИТИЕ ВОЗМОЖНОСТЕЙ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО- КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ НАТО В ВОЕННО-ПОЛИТИЧЕСКИХ ЦЕЛЯХ В КОНТЕКСТЕ МЕЖДУНАРОДНОЙ БЕЗОПАСНОСТИ

В статье исследуется развитие возможностей использования информационно-коммуникационных технологий НАТО в военно-политических целях в контексте международной безопасности. Основное внимание уделяется двум взаимосвязанным аспектам: интеграции искусственного интеллекта (ИИ) и больших данных в военную стратегию Североатлантического альянса, а также эволюции концепции гибридных войн. Автор рассматривается влияние технологического прогресса на традиционные подходы к военному планированию и ведению операций. В статье подчеркивается, что НАТО активно внедряет ИИ в разведывательные системы, процессы принятия решений и систему кибербезопасности, что позволяет военно-политическому блоку сохранять технологическое превосходство. Однако подобная деятельность также порождает новые вызовы, включая этические и правовые вопросы, связанные с автономными системами военного назначения. Параллельно исследуется феномен гибридных войн, сочетающих военные и невоенные методы воздействия, такие как информационно-психологические операции, кибератаки и экономическое давление. Особое внимание уделяется стратегическим коммуникациям НАТО и их роли в современном информационном противоборстве. Автор анализирует, как Североатлантический альянс адаптируется к новым угрозам, вновь активизируя антироссийскую направленность своей политики. В заключении статьи отмечается, что отсутствие четких международно-правовых норм, регулирующих применение новых технологий в военных конфликтах, создает серьезные риски для глобальной стабильности. Автор приходит к выводу, что дальнейшее изучение рассматриваемых вопросов требует комплексного подхода, включая анализ конкретных кейсов, оценку эффективности мер противодействия и разработку механизмов международного регулирования.

Ключевые слова: киберпространство, кибербезопасность, ИКТ, информационная безопасность, киберзащита, кибератака, киберагрессия.

Введение. Сегодня, в условиях бурного развития информационно-коммуникационных технологий и стремительно трансформирующейся системы международных отношений, которая рассматривается многими исследователями в парадигме усиления турбулентности, нестабильности и гетерогенности, киберпространство становится принципиально новой ареной как для межгосударственного взаимодействия, так и противостояния. Более того, практическая имплементация широкого инструментария прокси-войн в киберпространстве существенно нивелирует риск для государства или военного блока быть обвиненным в агрессии [4].

Повсеместная имплементация высоких технологий приводит к значительным изменениям в мировосприятии и модифицирует привычную картину реальности, затрагивая различные сферы социальной и политической деятельности. Цифровизация, развитие искусственного интеллекта, виртуальной и дополненной реальности способствуют формированию новых эпистемологических парадигм, в рамках которых границы между физическим и цифровым пространством постепенно стираются. Так, по мнению российского политолога И.С. Семененко, «революция в информационных технологиях придала новые качества социокультурной динамике современного мира, отличительная черта которого – это углубляющиеся разрывы социальной ткани современных обществ в условиях уплотнения информационных потоков и поистине драматического роста их воздействия на сознание и поведение людей» [8].

Ключевые информационно-коммуникационные технологии составляют основу «четвертой промышленной революции», которая в наиболее развитых странах уже началась. Дополнительными объективными стимулами к внедрению данных технологий будут и старение населения, существенно обостряющее рост потребности к роботизации, и изменение климата, требующее обработки все увеличивающихся массивов о состоянии планеты, и осознание важности цифровых технологий в условиях различного рода пандемий.

Современные информационно-коммуникационные технологии (ИКТ) играют ключевую роль в трансформации военно-политической стратегии и практики международных организаций, включая Североатлантический альянс. В условиях глобальной цифровизации и усиления киберугроз ИКТ становятся не только инструментом повышения оперативной эффективности, но и важным элементом стратегического сдерживания и обеспечения международной безопасности. Использование НАТО информационно-коммуникационных технологий в военно-политических целях отражает стремление Североатлантического альянса адаптироваться к вызовам современности, включая кибертерроризм, гибридные угрозы и дестабилизацию информационного пространства.

Информационно-коммуникационные технологии в военно-политической стратегии НАТО: вызовы и перспективы. На сегодняшний день вопросы обеспечения кибербезопасности выходят на глобальный уровень, на уровень создания единой системы кибербезопасности как государственных акторов, так и международных организаций, включая Североатлантический альянс.

Необходимо констатировать, что после долгого периода либерализации режимов передачи различных высоких технологий и ноу-хау, являвшегося одним из главных двигателей глобализации, начался обратный процесс – замедления темпов передачи технологий – в первую очередь, вследствие сознательных усилий, предпринимаемых национальными государствами для защиты своего технологического суверенитета от различных посягательств со стороны конкурентов. Особенно активно этот процесс идет в сфере информационно-коммуникационных технологий. По различным оценкам специалистов, сокращение темпов диффузии технологий будет иметь существенные экономические последствия – в первую очередь, для развивающихся стран и приведет к существенному снижению производительности труда, а также повышению стоимости производства и цен на многие товары. Весьма заметными потери от фрагментации будут и в тех отраслях, где особенно нужно функционирование единых платформ – например при осуществлении трансграничных финансовых транзакций.

Говоря о ключевых геополитических последствиях сокращения темпов диффузии технологий, данный феномен может усугублять проблему «цифрового разрыва» и становиться еще одним фактором углубления социального неравенства в странах Глобального юга, вести к снижению темпов экономического роста и таким образом становиться еще одним потенциальным фактором общественного недовольства, грозящего нестабильностью и конфликтами. Представляется возможным констатировать, что сокращение темпов диффузии технологий может помочь национальным государствам обеспечивать технологический суверенитет, а также побудить конкурентов к получению технологических секретов незаконными способами – в том числе посредством кибершпионажа [6].

Еще одной крайне примечательной тенденцией научно-технологического развития в течение последнего десятилетия стало заметное несоответствие между темпами развития технологий и темпами адаптации к ним структур управления на национальном и глобальном уровне с точки зрения разработки соответствующих стандартов, правил и норм. Среди областей, в которых это проявляется наиболее заметно – искусственный интеллект, геновая инженерия, космические технологии. Вероятность возникновения глобальных стандартов в данных сферах в ближайшие годы представляется довольно низкой в условиях роста геополитического противоборства. Достаточно посмотреть, например, на постоянное увеличение числа государств, требующих локализации основных объемов данных на своей территории.

Анализ роли ИКТ в контексте эволюции военно-политической доктрины Североатлантического альянса, а также его влияния на баланс сил в современной системе международных отношений позволяет выявить последствия для глобальной и региональной безопасности. Внедрение передовых технологий, таких как искусственный интеллект, большие данные и квантовые вычисления, открывает новые возможности для укрепления обороноспособности.

Развитие возможностей использования информационно-коммуникационных технологий в рамках НАТО является важным элементом стратегии

Североатлантического альянса в условиях современной геополитической реальности. Основные точки развития данных возможностей можно выделить следующим образом:

- 1) использование искусственного интеллекта (ИИ) и больших данных;
- 2) интеграция информационно-коммуникационных технологий (ИКТ)

в гибридные войны.

Использование искусственного интеллекта (ИИ) и больших данных. Использование искусственного интеллекта (ИИ) и больших данных в военно-политических целях становится важным элементом стратегии Североатлантического альянса в условиях цифровой трансформации. Данные технологии открывают новые возможности для анализа данных, прогнозирования угроз и оптимизации военных операций. В контексте международной безопасности применение ИИ и больших данных требует тщательного анализа, так как оно может как способствовать стабильности, так и создавать новые риски.

Говоря о растущей роли искусственного интеллекта (далее – ИИ) в современной системе международных отношений, первоначально необходимо отметить качественный прогресс в его развитии за последнее десятилетие. В силу самого характера данной технологии дальнейшее развитие ИИ с высокой вероятностью ознаменует и будет существенно способствовать качественному прорыву на всех направлениях научного познания и технологий, который не будет иметь аналогий в истории человечества и который чреват в том числе серьезными геополитическими последствиями [4]. Являясь частью процесса цифровизации международных отношений, ИИ влияет на восприятие меняющейся системы самими акторами.

Отметим, что на современном этапе гонка в области искусственного интеллекта обусловлена:

- радикальным ростом мощностей суперЭВМ, использующих микропроцессорные решения на графической архитектуре, и обеспечением их доступности для исследований в области ИИ;
- развитием соответствующих разделов прикладной математики;
- развитием методов программирования для компьютеров (особенно для суперЭВМ);
- некоторым продвижением в области когнитивных исследований [6].

Говоря об использовании Североатлантическим альянсом ИИ в военно-политических целях в контексте международной безопасности, целесообразно отметить некоторые ключевые вехи.

В 2019 году экспертами Оборонного колледжа НАТО был подготовлен доклад, содержащий обоснование необходимости активизации разработок в сфере искусственного интеллекта. Согласно представленным в документе выводам, совершенствование технологий, базирующихся на ИИ, машинном обучении и анализе больших данных, могло бы способствовать значительному повышению уровня военного превосходства стран-участниц Североатлантического альянса.

В докладе подчеркивалось, что «доработка и совершенствование существующего технологического и промышленного потенциала позволит НАТО сохранить и нарастить военное превосходство, тем самым на долгие годы, обеспечив его вклад в поддержание глобальной безопасности» [2].

В этом же году на полях промышленного форума НАТО бывший генеральный секретарь альянса Йенс Столтенберг объявил о планах военно-политического блока ускорить интеграцию технологий искусственного интеллекта в различные военные системы. В частности, он отметил, что в течение 15 лет предполагается заменить парк самолетов радиолокационного обнаружения и управления AWACS на системы, функционирующие на основе искусственного интеллекта [3].

В 2021 году Североатлантическим альянсом была одобрена Стратегия по искусственному интеллекту, направленная на обеспечение ответственного и этичного использования ИИ в военных целях [12]. Данный документ подчеркивал важность разработки стандартов и принципов, которые бы минимизировали риски, связанные с автономными системами.

Стратегия Североатлантического альянса в области искусственного интеллекта включает три ключевые сферы: анализа данных, изображений и киберзащиту. В документе подчеркивается, что киберпространство стало ключевой сферой для современных вызовов безопасности, а кибератаки могут иметь серьезные последствия для политической, экономической и военной стабильности стран-членов альянса. В документе отмечается, что НАТО рассматривает киберпространство как область операций, наравне с сушей, морем, воздухом и космосом. Североатлантический альянс подтверждает свою приверженность укреплению киберзащиты, включая развитие потенциала для предотвращения, обнаружения, реагирования и восстановления после кибератак. Особое внимание уделяется коллективной обороне, которая является одной из основополагающих задач НАТО в соответствии со Статьей 5 Вашингтонского договора. В документе подчеркивается, что масштабная кибератака может быть приравнена к вооруженному нападению, что может привести к активации механизмов коллективной обороны. Кроме того, акцентируется внимание на важности международного сотрудничества в области кибербезопасности. НАТО призывает к соблюдению норм международного права в киберпространстве, включая принципы уважения суверенитета, неприменения силы и мирного урегулирования споров. Военно-политический блок также поддерживает диалог с партнерами, включая частный сектор, академические круги и гражданское общество, для укрепления киберустойчивости [14].

В стратегии обозначены 4 ключевые цели:

1) обеспечение основы для того, чтобы НАТО и союзники могли подавать пример и поощрять разработку и использование ИИ ответственным образом в целях обороны и безопасности;

2) ускорение внедрения ИИ в разработку и предоставление новых возможностей, повышение функциональной совместимости в рамках альянса, в том числе за счет предложений по сценариям использования ИИ, структур и программ;

3) защита и мониторинг технологий искусственного интеллекта в НАТО и обеспечение внедрение новшеств, учитывая соображения политики безопасности;

4) выявление и защита от угроз злонамеренного использования ИИ государственными и негосударственными субъектами [14].

Анализ интеграции искусственного интеллекта (ИИ) и больших данных в стратегию Североатлантического альянса демонстрирует, что данные технологии становятся ключевым инструментом обеспечения военно-технического превосходства, оптимизации операций и противодействия киберугрозам. Принятие Стратегии по искусственному интеллекту в 2021 году подчеркивает стремление НАТО к ответственному использованию автономных систем, однако отсутствие глобального регулирования создает риски гонки вооружений и непреднамеренной эскалации. Несмотря на преимущества в анализе данных и кибербезопасности, дальнейшее развитие военного ИИ требует международных норм для минимизации угроз стратегической стабильности, сохраняя баланс между инновациями и безопасностью.

Интеграция информационно-коммуникационных технологий (ИКТ) в гибридные войны. Современные гибридные войны характеризуются сочетанием традиционных военных методов с невоенными средствами, такими как информационно-психологические операции, кибератаки и использование социальных сетей для дестабилизации противника. Информационно-коммуникационные технологии (ИКТ) играют ключевую роль в конфликтах, обеспечивая быстрое распространение информации, координацию действий и проведение киберопераций. НАТО, как ведущий военно-политический блок, активно интегрирует ИКТ в свои стратегии гибридной войны, что требует детального анализа.

Гибридные войны предполагают использование широкого спектра инструментов, включая пропаганду, дезинформацию и кибератаки, для достижения стратегических целей. ИКТ позволяют осуществлять эти действия с высокой эффективностью. Ключевыми задачами гибридной войны являются достижение полного или фрагментарного распада государственности, радикальная трансформация внутренней или внешней политики, смена правящей элиты на подконтрольные политические режимы, установление внешнего доминирования в идеологической и финансово-экономической сферах, а также дестабилизация общества с последующим подчинением его диктату иностранных государств или транснациональных корпораций [1]. Отечественные исследователи подчеркивают, что современные конфликты все чаще включают информационные операции, направленные на подрыв доверия к государственным институтам и создание социальной напряженности. В этом контексте НАТО активно развивает свои возможности в области кибербезопасности и информационных операций [11].

Технология гибридных войн настолько стала широко распространенной, что на встрече Совета министров иностранных дел НАТО, состоявшейся в декабре 2015 г., была принята «Стратегия гибридных войн». Согласно позиции

государств-членов Североатлантического альянса, гибридная война представляет собой комплекс мер, исключающих прямое применение конвенциональных средств, но предусматривающих использование информационно-пропагандистских кампаний, инструментов экономического давления, а также скрытое задействование подразделений специального назначения [5].

По словам бывшего генерального секретаря НАТО Йенса Столтенберга, суть стратегии базируется на «трех китах: подготовке, сдерживании и обороне». Помимо ответов на гибридные угрозы, интенсификации работы разведывательных служб и обмене развединформацией, в документе также предполагалась возможность применения специальных сил быстрого реагирования [5].

Представляется возможным констатировать, что на современном этапе один из ключевых треков для ведения гибридных войн государствами Североатлантического альянса является российское направление, что обусловлено комплексом геополитических, экономических и военно-стратегических факторов. В данном контексте особую значимость приобретает использование инструментов информационно-психологического воздействия, направленного на дестабилизацию внутривнутриполитической ситуации в Российской Федерации, подрыв доверия к государственным институтам и формирование негативного образа страны в международном пространстве. Помимо этого, наблюдается активное применение экономических санкций, поддержка оппозиционных движений и использование киберпространства для проведения скоординированных атак на критическую инфраструктуру. Подобные действия осуществляются в рамках стратегии «ограниченной конфронтации», позволяющей достигать стратегических целей без прямого военного столкновения, что соответствует современным тенденциям трансформации методов ведения войны в условиях глобализации и цифровизации.

По мнению российского политолога И.Н. Панарина, «стратегия ведения гибридной войны НАТО предполагает доминирование инструментов «мягкой силы» и нацелена на дезинтеграцию евразийского пространства, создание хаоса и нестабильности в соседних с Россией государствах с использованием технологий цветных революций, информационной войны, терроризма и экстремизма, финансово-экономического давления, военно-силового принуждения» [7].

Исследование сущности гибридной войны, проводимой руководством Североатлантического альянса в отношении Российской Федерации, предполагает всесторонний анализ методов ее реализации во внешнеполитической и внутривнутриполитической сферах. На международной арене страны коллективного Запада последовательно осуществляют меры, нацеленные на ослабление геополитических позиций России и ее маргинализацию в системе международных отношений и мировой политики [10]. Данная форма противостояния оказывает деструктивное воздействие на международный имидж России, подрывает доверие к национальному политическому руководству и создает прямые угрозы безопасности государства. В институциональном аспекте это проявляется в блокировании российских инициатив в Совете Безопасности ООН, где оппоненты

последовательно препятствуют реализации предлагаемых Россией решений, включая гуманитарные проекты, руководствуясь собственными геополитическими интересами. Через механизмы международных политических форумов, трансформированных в площадки гибридного противодействия, западные акторы осуществляют системную кампанию по снижению влияния России, используя медиа-инструменты для дискредитации государственного управления и общественно-политического устройства страны.

В рамках «Стратегии гибридных войн» ключевое значение в информационном противоборстве с Российской Федерацией принадлежит Центру стратегических коммуникаций НАТО, учрежденному в 2015 году в Риге (Латвия). Данная структура реализует инновационную концепцию стратегических коммуникаций Североатлантического альянса, интегрирующую широкий арсенал инструментов – от методов публичной дипломатии и PR-технологий до психологических операций и силового воздействия [9].

«Стратегия гибридных войн» представляет собой эволюционное развитие более ранней концепции гибридных угроз, сформулированной в 2010 году. В командовании стратегических исследований НАТО уже тогда отмечалась ограниченность традиционных подходов в реализации задач сдерживания, особенно в условиях расширения географических рамок потенциальных конфликтов за пределы Североатлантического региона. Эксперты НАТО аргументировали необходимость разработки инновационных методов и технологий противодействия. Однако целесообразно отметить, что в 2010 году основной акцент делался на противодействие террористическим угрозам, тогда как потенциальные риски, связанные с Китаем и Россией, лишь косвенно прослеживались в аналитических материалах, не получая явного формулирования [13].

Современные гибридные войны, сочетающие военные и невоенные методы (информационно-психологические операции, кибератаки, экономическое давление), стали ключевым инструментом стратегического противоборства, с активным использованием ИКТ для дестабилизации противника. Североатлантический альянс, разработав «Стратегию гибридных войн» в 2015 году, выступает за имплементацию комплексного подхода, включающего элементы кибербезопасности, пропаганды и спецопераций, при этом особое внимание уделяется противодействию России через инструменты «мягкой силы» и информационного воздействия, что подтверждается деятельностью Центра стратегических коммуникаций НАТО. Однако подобная тактика, направленная на подрыв государственности и международного влияния оппонентов, сталкивается с необходимостью правового регулирования и баланса между сдерживанием угроз и эскалацией конфликтов, что требует дальнейшего анализа последствий цифровизации современных войн.

Заключение. Проведенное исследование позволяет констатировать, что в современных условиях цифровой трансформации происходит принципиальная эволюция военно-политических стратегий, выражающаяся в двух взаимосвязанных процессах. С одной стороны, наблюдается активная интеграция

передовых технологий искусственного интеллекта и больших данных в военное планирование и оперативную деятельность, что кардинально меняет традиционные представления о ведении боевых действий. С другой стороны, происходит качественная трансформация самой природы конфликтов, где на первый план выходят гибридные методы противоборства, сочетающие военные и невоенные средства воздействия. Анализ стратегических документов и практической деятельности Североатлантического альянса демонстрирует, что НАТО последовательно реализует курс на технологическое доминирование, активно внедряя системы искусственного интеллекта в разведывательную деятельность, процессы принятия решений и кибербезопасность. Особое внимание уделяется развитию автономных систем военного назначения, что, с одной стороны, повышает оперативную эффективность, а с другой порождает серьезные этические и правовые дилеммы, связанные с вопросами контроля и ответственности за принимаемые решения. Параллельно с технологической модернизацией происходит концептуальное переосмысление природы современных конфликтов. Гибридные войны, сочетающие информационно-психологические операции, кибератаки, экономическое давление и другие невоенные методы воздействия, становятся доминирующей формой стратегического противоборства. Создание Центра стратегических коммуникаций НАТО и разработка соответствующей концептуальной базы свидетельствуют о системном подходе Североатлантического альянса к ведению информационного противоборства, где особый акцент делается на антироссийской направленности. При этом исследование выявило существенные пробелы в международно-правовом регулировании новых форм конфликтов. Отсутствие четких норм, регламентирующих применение искусственного интеллекта в военных целях, неопределенность правового статуса кибератак, недостаточная проработанность вопросов, связанных с информационными операциями – все это создает серьезные вызовы международной безопасности. Перспективы дальнейшего исследования обозначенной проблематики видятся в углубленном анализе конкретных случаев применения новых технологий в военных конфликтах, оценке эффективности различных моделей противодействия гибридным угрозам, а также в разработке комплексных подходов к международно-правовому регулированию возникающих вызовов. Особого внимания заслуживает изучение баланса между технологическим прогрессом в военной сфере и необходимостью сохранения глобальной стабильности. Таким образом, современные военно-политические стратегии переживают период глубокой трансформации, обусловленной цифровой революцией. Эти изменения требуют не только постоянного научного осмысления, но и выработки новых механизмов международного сотрудничества, способных обеспечить устойчивое развитие в условиях технологической неопределенности и возрастающих вызовов гибридного противоборства.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. **Баранов Н.А., Попов П.В.** Стратегии гибридных войн стран НАТО как вызов российской Федерации // Евразийская интеграция: экономика, право, политика. 2019. № 2 (28).
2. В НАТО выступили за активное развитие программ искусственного интеллекта // RT. 2019 // <https://russian.rt.com/world/news/610689-nato-razvitie-programm-intellekt>.
3. Искусственный интеллект в НАТО: динамичное внедрение, ответственное использование // НАТО. 2020 // <https://www.nato.int/docu/review/ru/articles/2020/11/24/iskusstvennyj-intellekt-v-nato-dinamichnoe-vnedrenie-otvetstvennoe-ispol-zovanie/index.html>.
4. Картина нарождающегося мира: базовые черты и тенденции. Москва: Дипломатическая академия МИД России, 2024.
5. НАТО приняла стратегию против гибридных войн // Newsland. 2015 // <https://newsland.com/post/4854888-nato-priniala-strategiiu-protiv-quotgibridnykh-voinquot>.
6. О мегатрендах мирового развития на период до 2035 года и их геополитическое значение. Москва: Институт перспективных стратегических исследований Национального исследовательского университета «Высшая школа экономики», 2023.
7. **Панарин И.Н.** Гладиаторы гибридной войны // Экономические стратегии. 2016. № 2.
8. **Семененко И.С.** Политические изменения в современном мире: новые контуры исследовательского поля // Политическая наука перед вызовами глобального и регионального развития / под ред. О.В. Гаман-Голутвиной. М.: Аспект Пресс, 2016.
9. About Strategic Communications. NATO STRATCOM. Centres of Excellence // Newsland. 2015 // <https://www.stratcomcoe.org/aboutstrategic-communications>.
10. **Fridman O.** The Danger of Russian Hybrid Warfare. London: H C Hurst & Co, 2017 // King's Centre For Strategic Communications Department of War Studies King's College London. 2017 // http://www.cicerofoundation.org/lectures/Ofer_Fridman_The_Danger_of_Russian_Hybrid_Warfare.pdf.
11. **Galeotti M.** Hybrid War or Gibridnaya Voina? Small Wars Journal // Amazon. 2016 // <https://www.amazon.com/Gibridnaya-Getting-non-linear-military-challenge/dp/1365549801>.
12. NATO. NATO's Artificial Intelligence Strategy // NATO. 2021 // <https://www.nato.int>.
13. NATO's Response to Hybrid Threats // NATO. 2018 // https://www.nato.int/cps/en/natohq/topics_156338.%20htm?selectedLocale=ru.
14. Summary of the NATO Artificial Intelligence Strategy // NATO. 2021 // https://www.nato.int/cps/em/natohq/official_texts_187617.htm.

N.A. NIKITIN

Postgraduate Student, Diplomatic Academy
of the Ministry of Foreign Affairs of Russia; Chief Specialist,
Department for International Cooperation of the Russian Academy
of Sciences, Moscow, Russia

DEVELOPING NATO INFORMATION AND COMMUNICATION TECHNOLOGIES CAPABILITIES USING FOR MILITARY- POLITICAL PURPOSES IN THE CONTEXT OF INTERNATIONAL SECURITY

The article examines the development of NATO's capabilities to use information and communication technologies for military-political purposes in the context of international security. The main focus is on two interrelated aspects: the integration of artificial intelligence (AI) and big data into the military strategy of the North Atlantic Alliance, and the evolution of the concept of hybrid wars. The author examines the impact of technological progress, especially in the field of AI, on traditional approaches to military planning and operations. The article emphasizes that NATO is actively introducing AI into intelligence systems, decision-making processes and cybersecurity, which allows the military-political bloc to maintain technological superiority. However, such activities also give rise to new challenges, including ethical and legal issues related to autonomous military systems. In parallel, the phenomenon of hybrid wars is examined, combining military and non-military methods of influence, such as information and psychological operations, cyber attacks and economic pressure. Particular attention is paid to NATO strategic communications and their role in modern information warfare. The author analyzes how the North Atlantic Alliance is adapting to new threats, once again activating the anti-Russian focus of its policy. In conclusion, the article notes that the lack of clear international legal norms governing the use of new technologies in military conflicts creates serious risks for global stability. The author comes to the conclusion that further study of the issues under consideration requires a comprehensive approach, including analysis of specific cases, assessment of the effectiveness of countermeasures, and development of international regulation mechanisms.

Key words: NATO, cybersphere, cybersecurity, ICT, information security, cyberdefense, cyberattack, cyberaggression.