DOI 10.35775/PSI.2025.69.4.021
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

ТРАНСФОРМАЦИЯ СОВРЕМЕННОЙ ПОЛИТИКИ НАТО В КИБЕРПРОСТРАНСТВЕ

Сегодня, в условиях стремительного развития технологий, которые всецело затрагивают все аспекты человеческой жизнедеятельности, все большую важность приобретает понятие «киберпространство». Являясь одним из ключевых компонентов системы международных отношений и мировой политики, киберпространство становится принципиально новой ареной для межгосударственного взаимодействия и регулирования, а также ожесточенного противостояния. В статье анализируется трансформация политики НАТО в киберпространстве, рассматриваемая в контексте усиления глобальной турбулентности и технологических вызовов. Исследование выявляет три ключевых этапа эволюции стратегии альянса, отражающих переход от фрагментарных мер к системной милитаризации киберпространства. На первом этапе (конец 1990-х – 2006 гг.) происходило институциональное оформление кибербезопасности в рамках НАТО. Пражский (2002) и Рижский (2006) саммиты закрепили киберугрозы в повестке альянса, а создание системы реагирования на киберинциденты (NCIRC) обозначило переход от национальных мер к наднациональной координации. Второй этап (2007-2014 гг.) характеризовался кризисным реагированием на масштабные атаки (Эстония, 2007; Грузия, 2008; Украина, 2014), что ускорило разработку стратегических документов, включая Концепцию 2010 года. Создание Киберцентра в Таллине (2008) подтвердило растущую роль киберпространства в гибридных конфликтах. Третий этап (2014 – н.в.) ознаменовался признанием киберпространства «пятой областью операций» (Варшавский саммит, 2016) и развитием наступательных возможностей. Интеграция киберсил в командную структуру НАТО и внедрение концепции многодоменных операций (MDO) отражают милитаризацию цифровой среды. Исследование демонстрирует, что эволюция подходов НАТО определяется технологическими и геополитическими факторами. Однако сохраняются проблемы атрибуции атак, правового регулирования и баланса между обороной и наступательными операциями. В перспективе развитие киберстратегии альянса потребует уточнения критериев применения статьи 5 Североатлантического договора и гармонизации национальных и наднациональных механизмов безопасности.

Ключевые слова: *НАТО, киберсфера, кибербезопасность, ИКТ, информационная безопасность, киберзащита, кибератака, кибератрессия.*

Введение. Современная система международных отношений рассматривается многими исследователями в парадигме усиления турбулентности, нестабильности и гетерогенности. Технологический прорыв позволяет говорить о повсеместном применении интернет-технологий во всех без исключения сферах международных отношений, включая международную безопасность.

На современном этапе киберпространство стало ключевой сферой геополитической конкуренции, что подтверждает необходимость адаптации стратегий международных организаций к новым вызовам и угрозам. НАТО является частью системы европейской и глобальной безопасности и одним из наиболее значимых международных институтов во всем мире. Будучи ведущим военно-политическим блоком, Североатлантический альянс активно трансформирует свою политику в киберпространстве, стремясь обеспечить коллективную кибербезопасность и противодействовать угрозам гибридного характера. В условиях роста кибератак на критическую инфраструктуру и использования информационно-коммуникационных технологий в качестве инструмента политического и военного давления, Североатлантический альянс пересматривает доктринальные подходы, усиливает координацию между странами-членами и развивает собственный наступательный потенциал с использованием кибертехнологий. В данной статье анализируются основные направления трансформации политики НАТО в киберпространстве, включая нормативно-правовые инициативы, оперативные механизмы реагирования, а также стратегические приоритеты в контексте меняющегося характера угроз. Особое внимание уделяется роли альянса в формировании международных стандартов кибербезопасности и его взаимодействию с гражданским и частным секторами.

Трансформация политики НАТО в киберпространстве отражает эволюцию подходов альянса к новым вызовам и угрозам, связанных с цифровизацией и ростом зависимости от информационных технологий. Стратегия Североатлантического альянса в киберпространстве прошла несколько ключевых этапов, каждый из которых был обусловлен изменениями в технологической и геополитической среде.

Становление киберполитики: от осознания угроз к первым институциональным решениям. Говоря о понятиях киберпространство, информационная безопасность, ИКТ следует учитывать, что начало их практического применения в мировой политике датируется концом XX, началом XXI веков. Истоки появления вышеперечисленных понятий прослеживаются вплоть до возникновения интернета в его современном понимании и являются неразрывно связанными с научно-технологическим прогрессом. По мере развития современных технологий, киберпространство существенно расширялось, включая в себя принципиально новые элементы, такие как социальные сети, виртуальные сообщества и онлайн платформы. Постепенное внедрение широкого инструментария практического применения кибервозможностей в сферу международных отношений и международной безопасности следует рассматривать в качестве комплексного и постоянно эволюционирующего явления. По мере планомерного роста

зависимости акторов международных отношений от цифровой инфраструктуры, киберпространство перешло в парадигму источника потенциальных, в том числе витальных угроз и уязвимостей.

Организация Североатлантического договора признает растущую важность киберпространства в сфере безопасности и активно занимается противодействием киберугрозам. Подход НАТО к киберпространству основан на понимании того, что оно является областью операций наряду с сушей, морем, воздухом и космическим пространством. Важно понимать, что краеугольная 5 статья Североатлантического договора предусматривает коллективный ответ в том числе при кибератаке на одно из государств-членов альянса. Так, по словам бывшего генерального секретаря НАТО Йенса Столтенберга, «Серьезная кибератака может привести к срабатыванию статьи 5, согласно которой нападение на одного союзника рассматривается как нападение на всех» [12]. При этом главной опасностью практического применения такого подхода является несовершенство алгоритма идентификации источника злонамеренного акта кибер-воздействия.

Первые упоминания о киберугрозах в документах НАТО появились в конце 1990-х годов, когда альянс начал осознавать потенциальные риски, связанные с развитием информационных технологий. В этот период киберпространство рассматривалось преимущественно как сфера гражданской инфраструктуры, а не как область военных операций. Однако уже в 1999 году, во время операции «Союзная сила», альянс столкнулся с кибератаками на свои системы, что стало первым сигналом о необходимости уделять больше внимания кибербезопасности [6]. Американские политологи Джон Аркилла и Дэвид Ронфельдт, отмечали, что уже в этот период началось формирование концепции «кибервойны» как новой формы конфликта, где информационные технологии играют ключевую роль [6]. Однако на данном этапе Североатлантический альянс еще не имел четкой стратегии в киберпространстве, а меры по защите носили фрагментарный характер.

Рассматривая процесс эволюции подходов европейских государств-членов НАТО, необходимо констатировать об изменении объектно-субъектных отношений понятия кибербезопасности (от традиционных интерпретаций киберпространства к экосистемным терминам и концепциям) [5]. Более того, при изучении темы особенностей региональной кибербезопасности НАТО на европейском континенте необходимо учитывать принципиальное различие американского и европейского подходов. Европейские государства-члены альянса сталкивались с теми же проблемами и вызовами в киберпространстве, что и их американские партнеры, однако в данной парадигме наблюдается фундаментальное различие институциональных структур США и европейских стран. В то время как в случае с США имели место единая внешняя политика, централизированные вооруженные силы и единый бюджет, европейским государствам-членам Североатлантического альянса приходилось затрачивать усилия на разработку и внедрение собственных программ по имплементации политики в сфере кибербезопасности на национальных уровнях, при этом осуществляя координацию

в рамках наднациональной структуры в лице Европейского Союза и военно-политического блока в лице НАТО [10].

Хотя стратегия Североатлантического альянса всегда в той или иной мере затрагивала проблемы обеспечения собственных систем связи и обмена информацией, защита от кибернетических угроз в качестве доктринально оформленного компонента стратегии впервые была включена в политическую повестку организации в ходе саммита НАТО в Праге в 2002 году [8], а в последствии вновь актуализирована по итогам саммита в Риге в 2006 году [13]. Так, согласно итоговому коммюнике Пражского саммита, государства-члены альянса договорились «укреплять свои возможности по защите от кибератак» [8].

Говоря о важнейшей вехе формирования современной стратегии кибербезопасности НАТО как на глобальном, так и региональном уровнях (на Европейском континенте) следует обратиться к итогам Пражского саммита 2002 года. Одним из наиболее важных последствий данного саммита стало заложение фундамента к созданию программы киберзащиты «NCIRC» (NATO Computer Incident Response Capability) (Возможность реагирования на компьютерные инциденты НАТО) в 2002 году.

Программа изначально задумывалась как централизованный механизм для:

1) мониторинга компьютерных инцидентов;

2) координации реагирования на кибератаки;

3) разработки стандартов защиты информационной инфраструктуры;

4) обеспечения оперативного обмена информацией между странами-членами.

Особое значение имело то, что NCIRC стала первым наднациональным механизмом киберзащиты в военно-политической организации такого масштаба. Ее создание ознаменовало переход от разрозненных национальных мер к системному подходу в обеспечении коллективной кибербезопасности [11].

Значение NCIRC для развития киберполитики Североатлантического альянса трудно переоценить. Программа не только обеспечила практический инструментарий защиты, но и:

1) заложила основы для последующего признания киберпространства областью операций;

2) способствовала выработке общих стандартов и процедур;

3) создала прецедент наднационального управления кибербезопасностью.

Таким образом, создание NCIRC стало поворотным моментом в трансформации подходов НАТО к вопросам кибербезопасности, ознаменовав переход от концептуальных дискуссий к практической реализации принципов коллективной кибероборонь.

Представляется возможным констатировать, что в период 1990-2006 гг. киберпространство превратилось в ключевую сферу обеспечения международной безопасности, требующую комплексного и адаптивного регулирования. Изначально воспринимаемое как второстепенная область гражданской инфраструктуры, киберпространство постепенно трансформировалось

в полноценный театр военных и стратегических операций, что потребовало от Североатлантического альянса разработки специализированных механизмов противодействия угрозам.

Особое значение в этом процессе сыграли Пражский и Рижский саммиты НАТО, на которых были заложены основы современной киберполитики альянса, включая создание системы реагирования на киберинциденты (NCIRC).

Период кризисного реагирования: кибератаки как катализатор трансформации стратегии альянса. В качестве второго этапа трансформации политики Североатлантического альянса в киберпространстве возможно выделить период 2007-2014 годов, характеризуемого прежде всего началом формирования основ киберполитики военно-политического блока.

По мнению западных исследователей в области кибербезопасности, «тремя наиболее яркими примерами киберагрессии между национальными государствами являются события в Эстонии (2007 г.), Грузии (2008 г.) и Украине (2014, 2015 гг.), совершенные Россией и ее прокси» [10]. Так, по мнению западных исследователей, «в 2007 году с российской стороны имели место непрерывные DDoS атаки, направленные на нарушение стабильной работы веб-сервисов эстонского правительства. В 2008 году, за три недели до начала операцию по принуждению к миру Грузии, российской стороной вновь была применена стратегия использования DDoS-атак с целью блокировки веб-ресурсов (что позже стало частью российской общей стратегии ведения боевых действий). В 2014 году в ходе воссоединения Крыма с Россией также имели место многочисленные кибератаки, направленные на государственные и частные медиа сервисы украинской стороны» [10].

Одним из запоминающихся событий в области формирования современной стратегии Североатлантического альянса в сфере кибербезопасности в Европе стало открытие Киберцентра НАТО в г. Таллине (Эстония) в 2008 году. Ключевой предпосылкой к данному событию стала серия массированных кибератак сайтов газет, основных банков и правительственных учреждений Эстонии [2]. Примечательным является тот факт, что ответственность за упомянутые действия была возложена на Россию при отсутствии каких-либо исчерпывающих доказательств. Тем самым уже в конце 2010-х годов стал явно прослеживаться более чем однозначный вектор антироссийской риторики в политике как отдельных государств Североатлантического альянса, так и самого военно-политического блока.

Рассматривая итоговое коммюнике саммита НАТО в Лиссабоне (2010 г.), следует отметить существенный рост внимания государств-членов альянса к киберпространству. Согласно Стратегической концепции 2010 года «Активное участие, современная оборона», принятой на встрече в верхах в Лиссабоне в ноябре 2010 года, государства-члены альянса согласились, что произошел качественный скачок в интенсификации кибератак, а также усилился их негативный эффект, напрямую воздействующий на государственные органы, коммерческие предприятия, транспортные системы и логистику, тем самым комплексно подрывая

национальные экономики. Исходя из вышесказанного, было принято принципиальное решение «совершенствовать способность НАТО по предотвращению и обнаружению кибератак, защите и нивелированию причиненного ими ущерба, в частности, используя процесс планирования с целью укрепления и координации национальных средств киберзащиты, путем связывания всех органов альянса централизированной сетью киберзащиты и интеграции механизмов НАТО и государств-членов по осведомлению, предупреждению и реагированию на киберугрозы» [1].

Анализ трансформации политики НАТО в киберпространстве в период 2007–2014 годов позволяет сделать вывод о качественном изменении подхода альянса к кибербезопасности. Данный этап характеризовался переходом от фрагментарных мер к формированию системной стратегии, что было обусловлено серией масштабных кибератак в Эстонии (2007), Грузии (2008) и Украине (2014) приписываемых России. Эти инциденты продемонстрировали, что киберпространство стало неотъемлемой частью современных конфликтов, а его использование в гибридных войнах потребовало от НАТО разработки новых механизмов коллективной обороны. Важным шагом в этом направлении стало создание Киберцентра НАТО в Таллине (2008), что подчеркнуло растущую роль кибербезопасности в стратегии альянса. Примечательно, что обвинения в адрес России носили преимущественно политизированный характер, что отражало усиление антироссийской риторики в политике НАТО. Дальнейшее институциональное развитие киберполитики альянса было закреплено в Стратегической концепции НАТО 2010 года, где киберугрозы были официально признаны вызовом коллективной безопасности, требующим скоординированных мер защиты. Таким образом, рассматриваемый период стал ключевым этапом в трансформации подходов НАТО к киберпространству, когда Североатлантический альянс перешел от реагирования на отдельные инциденты к формированию комплексной системы кибероборонь.

Милитаризация киберпространства: признание областью операций. В качестве третьего этапа трансформации политики Североатлантического альянса в киберпространстве представляется возможными выделить период с 2014 года по настоящее время, характеризуемого, прежде всего, признанием киберпространства областью операций.

События 2014 года стали катализатором кардинального пересмотра Североатлантическим альянсом подходов к обеспечению коллективной безопасности, в том числе в киберпространстве. Воссоединение Крыма с Россией оказало значительное воздействие на систему международной безопасности, в частности на стратегическое планирование НАТО. Североатлантический альянса, был вынужден вернуться к традиционной задаче сдерживания Москвы.

Целесообразно упомянуть прошедший в 2016 г. саммит НАТО в Варшаве, где киберпространство было официально признано сферой операций военно-политического блока. Саммит в Варшаве проходил в ключевой для альянса момент, связанный с кардинальными изменениями в Европейском регионе и на мировой

арене в целом. С точки зрения Коллективного Запада с Соединенными Штатами в главной роли, НАТО столкнулось с существенными угрозами безопасности евроатлантического региона. Так, согласно 70 статье итогового коммюнике Варшавского саммита, «кибернетические нападения представляют явную угрозу безопасности Североатлантического союза и могут оказать столь же вредное воздействие на современные общества, что и обычные нападения. В Уэльсе мы пришли к соглашению о том, что киберзащита является частью основной задачи НАТО по обеспечению коллективной обороны. Теперь, в Варшаве мы вновь подтверждаем оборонительный мандат НАТО и признаем кибернетическое пространство как сферу операций, где НАТО должен так же эффективно обороняться, как и в воздухе, на суше и на море» [3]. По мнению профессора А.В. Крутских, именно Варшавский саммит НАТО стал поворотным моментом в плане милитаризации киберпространства. С 2018 года Североатлантический альянс приступил к интеграции киберсил государств-участников НАТО в командную структуру военно-политического блока. В планах было создание в 2023 году объединенного киберпотенциала альянса, который в случае необходимости был бы задействован Союзным командованием операций, в том числе при проведении наступательных кибероперациий [4].

Говоря о современной политике НАТО в киберпространстве нельзя не упомянуть трансформацию подхода к так называемым «многодоменным операциям» (Multi-Domain Operations, MDO). Концепцию MDO, впервые имплементированную в 2016 году в результате осознания рисков недостаточной защиты компьютерных систем, можно охарактеризовать в качестве некоего результата осмысления киберпространства в качестве витального компонента активного противоборства акторов международных отношений и неотъемлемого компонента глобальной и региональной системы безопасности. Таким образом, уже в 2016 году киберпространство рассматривали в качестве не только связующего звена и платформы для взаимодействия систем ведения боевых действий, но и как обособленную оружейную платформу [9]. Развитие вооруженными силами США концепта MDO шло параллельно с эволюцией подхода Североатлантического альянса к кибероперациям. В то время как вышеупомянутый Киберцентр НАТО в г. Таллине (Эстония) продолжал свою работу, руководством альянса было объявлено открытие Интегрированного центра НАТО по киберзащите (NICC) и заявлено продолжение разработки доктрины для кибероперациий [7].

Проведенный анализ третьего этапа трансформации политики НАТО в киберпространстве позволяет констатировать качественно новый уровень милитаризации киберпространства в стратегии альянса. Варшавский саммит 2016 года стал поворотным моментом, официально закрепившим статус киберпространства как полноценной области военных операций наравне с традиционными сферами – сушей, морем и воздухом. Это решение отражало растущее понимание того, что кибератаки могут наносить сопоставимый ущерб национальной безопасности, что и обычные военные нападения.

Важнейшими характеристиками данного периода стали:

1) институционализация киберпотенциала через интеграцию национальных киберсил в структуру альянса;

2) разработка концепции многодоменных операций (MDO), рассматривающей киберпространство как самостоятельную платформу ведения боевых действий;

3) создание новых структурных элементов для координации оборонительных и наступательных возможностей.

Эволюция подходов НАТО демонстрирует переход от оборонительной парадигмы к комплексному восприятию киберпространства как:

1) среды для ведения гибридных конфликтов;

2) самостоятельного театра военных действий;

3) критически важного элемента системы коллективной безопасности.

Однако подобная милитаризация киберпространства вызывает ряд вопросов, касающихся: критериев применения статьи 5 Вашингтонского договора; правовых рамок наступательных кибероперациий; баланса между национальными и наднациональными элементами кибербезопасности.

Таким образом, рассматриваемый период заложил основы для дальнейшего развития киберстратегии НАТО, определив киберпространство как ключевой элемент современной системы международной безопасности, требующий постоянной адаптации подходов альянса к новым вызовам и угрозам.

Заключение. Таким образом, резюмируя вышесказанное, следует отметить, что на современном этапе стал очевиден экспоненциальный рост значимости киберпространства в деятельности Североатлантического альянса. С течением времени международное сообщество свидетельствовало эволюцию доктринального оформления подходов альянса к проблемам обеспечения кибербезопасности, а также стратегии деятельности в киберпространстве. Киберпространство имеет огромное значение для организации и ее членов, поскольку современные военные операции и общая безопасность все более зависят от цифровых технологий. В то же время следует выделить роль ключевого для Североатлантического альянса европейского региона, государства Европейского союза остаются уникальными и важнейшими партнерами НАТО. В контексте современных геополитических реалий именно Европа является ареной для обкатки нововведений альянса в киберпространстве. Начав свое зарождение в начале 2000-х годов, политика государств-членов НАТО в киберпространстве эволюционировала, планомерно отвечая на новые вызовы и угрозы.

Проведенное исследование трансформации политики НАТО в киберпространстве с конца XX века по настоящее время позволяет выделить три ключевых этапа трансформации подходов альянса, каждый из которых характеризовался качественным изменением восприятия киберугроз и методов противодействия им.

На первом этапе (конец 1990-х – 2006 гг.) происходило осознание потенциальных рисков киберпространства, что нашло отражение в первых концептуальных

документах и создании базовых структур защиты (NCIRC). Пражский (2002) и Рижский (2006) саммиты Североатлантического альянса заложили институциональные основы киберполитики НАТО, хотя меры носили преимущественно оборонительный и фрагментарный характер.

Второй этап (2007-2014 гг.) был ознаменован реакцией на серию масштабных кибератак, что привело к созданию Киберцентра НАТО в Таллине (2008) и принятию Стратегической концепции НАТО 2010 года. В этот период происходит переход от технического восприятия киберугроз к их осмыслению как элемента гибридных войн и инструмента геополитического противостояния.

Третий этап (2014 – н.в.) характеризовался окончательной милитаризацией киберпространства, официально признанного на Варшавском саммите (2016) полноценной областью операций. Разработка концепции многодоменных операций (MDO) и создание Интегрированного центра по киберзащите свидетельствовали о переходе к комплексному восприятию киберпространства как: самостоятельного театра военных действий; критического элемента системы коллективной безопасности; платформы для наступательных операций.

Анализ эволюции подходов НАТО позволяет сделать следующие выводы:

1) произошла трансформация от технико-оборонительных мер к комплексной военно-политической стратегии;

2) киберпространство стало неотъемлемым элементом концепции коллективной обороны;

3) сформировался институциональный каркас кибербезопасности альянса;

4) сохраняются проблемы атрибуции атак и правового регулирования наступательных операций.

Перспективы дальнейшего развития киберполитики НАТО связаны с необходимостью:

1) совершенствования механизмов коллективного реагирования;

2) разработки четких критериев применения 5 статьи Североатлантического договора;

3) балансирования между наступательными и оборонительными возможностями;

4) гармонизации национальных и наднациональных подходов.

Таким образом, трансформация стратегии Североатлантического альянса в киберпространстве отражает общую тенденцию милитаризации цифровой среды, что требует постоянной адаптации международно-правовых норм и механизмов поддержания стратегической стабильности в условиях новых технологических вызовов.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК:

1. Активное участие, современная оборона «Стратегическая Концепция Обороны и Обеспечения Безопасности Членов Организации Североатлантического Договора» Утверждена Главами Государств и Правительств в Лиссабоне // НАТО. 2010 // https://www.nato.int/cps/en/natohq/official_texts_68580.htm?selectedLocale=ru.
2. В Таллине начал работу центр киберзащиты НАТО // SecurityLab.ru. 2008 // https://www.securitylab.ru/news/353773.php.
3. Заявление по итогам встречи на высшем уровне в Варшаве обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Варшаве 8-9 июля 2016 // НАТО. 2016 // https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=ru.
4. **Крутских А.В.** Угрозы безопасности в цифровой среде и международное сотрудничество в области цифровой безопасности // Международные отношения: грани настоящего и будущего / [под ред. И.С. Иванова, И.Н. Тимофеева, Е.О. Карпинской, Е.А. Солодухиной, С.М. Гавриловой]; Российский совет по международным делам (РСМД). М.: НП РСМД, 2023.
5. **Романова Т.А., Малова А.Н.** Проблема применения категории «стрессоустойчивость» в политике кибербезопасности Евросоюза // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2019. № 1.
6. **Arquilla J. & Ronfeldt D.** Networks and Netwars: The Future of Terror, Crime, and Militancy. RAND Corporation // Internet Archive. 2001 // https://archive.org/details/networksnetwars00john/page/n1/mode/2up.
7. Black and Lynch, «Cyber Threats to NATO from a Multi-Domain Perspective» // NATO CCDCOE // https://ccdcoe.org/uploads/2023/11/Cyber_Threats_to_NATO_2023.pdf.
8. Cyber defence // NATO. 2024 // https://www.nato.int/cps/fr/natohq/topics_78170.htm?selectedLocale=en#defence.
9. Gady and Stronell «Cyber Capabilities and Multi-Domain Operations in Future High-Intensity Warfare in 2030» // IISS // https://www.iiss.org/publications/.
10. **Ilves L.K., Evans T.J., Cilluffo F.J. & Nadeau A.A.** European Union and NATO Global Cybersecurity Challenges: A Way Forward. PRISM. 2016. № 6 (2) // JSTOR // https://www.jstor.org/stable/26470452?seq=1.
11. NATO Cyber Defence // NATO. 2024 // https://www.nato.int/cps/en/natohq/topics_78170.htm.
12. NATO will defend itself // NATO. 2019 // https://www.nato.int/cps/en/natohq/news_168435.htm.
13. Riga Summit Declaration // NATO. 2006 // https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en.

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

TRANSFORMATION OF MODERN NATO CYBERSPACE POLICY

Today, in the context of the rapid development of technologies that fully affect all aspects of human life, the concept of «cyberspace» is becoming increasingly important. Being one of the key components of the system of international relations and world politics, cyberspace is becoming a fundamentally new arena for interstate interaction and regulation, as well as fierce confrontation. The article analyzes the transformation of NATO's policy in cyberspace, viewed in the context of increasing global turbulence and technological challenges. The study identifies three key stages in the evolution of the alliance's strategy, reflecting the transition from fragmented measures to the systemic militarization of cyberspace. At the first stage (late 1990s – 2006), cybersecurity was institutionalized within the framework of NATO. The Prague (2002) and Riga (2006) summits consolidated cyber threats on the alliance's agenda, and the creation of the Cyber Incident Response System (NCIRC) marked the transition from national measures to supranational coordination. The second stage (2007-2014) was characterized by a crisis response to large-scale attacks (Estonia, 2007; Georgia, 2008; Ukraine, 2014), which accelerated the development of strategic documents, including the 2010 Concept. The establishment of the Cyber Center in Tallinn (2008) confirmed the growing role of cyberspace in hybrid conflicts. The third stage (2014 – present) was marked by the recognition of cyberspace as the «fifth area of operations» (Warsaw Summit, 2016) and the development of offensive capabilities. The integration of cyber forces into the NATO command structure and the introduction of the concept of multi-domain operations (MDO) reflect the militarization of the digital environment. The study demonstrates that the evolution of NATO's approaches is determined by technological and geopolitical factors. However, problems remain with attribution of attacks, legal regulation, and the balance between defense and offensive operations. In the future, the development of the alliance's cyber strategy will require clarifying the criteria for applying Article 5 of the North Atlantic Treaty and harmonizing national and supranational security mechanisms.

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