Апрель 2025

МЕЖДУНАРОДНАЯ ЖИЗНЬ

Проблемы внешней политики, дипломатии, национальной безопасности

Американский взгляд на мир

В номере:

Москва. Издается с марта 1922 г.

Вадим Козюлин

Главный научный сотрудник ИАМП Дипломатической академии МИД России, кандидат политических наук

v.kozyulin@dipacademy.ru

Ключевые слова: *информационная война, когнитивная война, пропаганда, информационная экосистема, психологические операции, ноополитика.*

СОСТОЯНИЕ И ПЕРСПЕКТИВЫ МЕЖДУНАРОДНО-ПРАВОВОГО ОГРАНИЧЕНИЯ ИНФОРМАЦИОННОЙ ВОЙНЫ ЗАПАДА ПРОТИВ РОССИИ

В условиях глобального информационного доминирования Пентагон увеличивает подразделения по проведению информационных операций против России и усиливает прокси-подразделения в ВСУ. В опубликованной в июле 2023 года «Стратегии по операциям в информационной среде на 2023 год» говорится о необходимости создания специальных «информационных сил», чтобы «получать и поддерживать информационные преимущества… для успешной работы в информационном пространстве». Информационная война приобретает новые изощренные формы, нацеленные, в частности, на когнитивное восприятие как отдельных лиц, так и целых наций.

Сохранение национальной информационной экосистемы России становится одной из приоритетных задач государства. Нашей стране необходимо научиться противодействовать иностранным деструктивным информационным операциям и подготовить гражданских и военных экспертов, обладающих навыками противодействия иностранному информационному влиянию.

Понятие «информационная война»

Понятийный аппарат в сфере информационного противодействия еще формируется, и можно обнаружить разнообразие понятий и даже терминологическую путаницу: информационная, когнитивная, психологическая, гибридная, меметическая, кибервойна и война влияния.

В 2011 году МИД России предложил концепцию Конвенции об обеспечении международной информационной безопасности. Она не получила поддержки государств - участников ООН, однако в концепции имеется определение: «информационная война» - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны[1].

В доктрине информационной безопасности РФ 2016 года одной из потенциальных угроз безопасности России называется «наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях», а также усиление деятельности организаций, «осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса»[2].

В статье 2 Соглашения между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности в качестве самой первой угрозы международной информационной безопасности выделяется разработка и применение информационного оружия, подготовка и ведение информационной войны[3].

В западном понимании понятие «информационная война» связано с военными действиями. Информационная война направлена на военное и разведывательное сообщества противника. В меморандуме №30 от 1993 года заместителей министра обороны и председателя Комитета начальников штабов Вооруженных сил США информационная война определена как «действия, предпринимаемые для достижения информационного превосходства в поддержке национальной военной стратегии посредством воздействия на информацию и информационные системы противника»[4].

Американский теоретик информационных войн Мартин Либицкий выделил семь видов информационных войн в рамках вооруженного конфликта: командно-управленческая война; разведывательная война; электронная (включает криптографию и нарушение электронных коммуникаций врага: радаров, радиосвязи, компьютерных сетей); психологическая война (пропаганда, направленная на массовое сознание); хакерская война (диверсионные действия в компьютерных сетях, направленные против гражданских объектов, а также защита от таких действий); экономическая война (перекрытие каналов электронной коммерции); кибервойна[5].

Представляется, что сегодня ближе к российскому пониманию информационной войны стоит термин «когнитивная война», под которым понимаются действия государства или влиятельных групп для манипулирования механизмами познания противника и его населения, чтобы ослабить, влиять на него или даже подчинить себе. Этот термин начал использоваться в таком значении в Соединенных Штатах с 2017 года.

Считается, что информационная война носит сиюминутный, недолговременный характер, где в качестве инструментария используют инструментарий из ложных новостей.

Когнитивная война сочетает связанные с информационной войной новейшие кибертехнологии и человеческую составляющую «мягкой силы», а также манипулятивные аспекты психологических операций (т. н. PSYOPS). То есть она находится на пересечении двух операционных областей, которые ранее управлялись по отдельности: психологические операции и операции влияния («мягкая сила»), с одной стороны, и кибероперации, предназначенные

для нанесения ущерба или уничтожения физических информационных активов, - с другой. Обычно они включают в себя искаженное, как правило компьютерными средствами, описание реальности, отвечающее интересам «атакующей» стороны. При этом используются все элементы информационной войны, включая операционные аспекты психологии и нейронаук. Современные информационные технологии служат эффективным средством доставки соответствующего контента целевой аудитории.

Когнитивная война напрямую связана с информационной, поскольку ее целью является изменение восприятия и измерение этого изменения восприятия. То есть она направлена не только на контроль потока информации, но и на оценку воздействия информации, а также оценку того, как воздействие можно усилить. Когнитивные операции основаны на глубоких знаниях ученых и стратегического сообщества в области когнитивных наук (от нейробиологии до когнитивной психологии и интерфейсов «мозг-компьютер»).

В условиях возрастающей конфронтации России и Запада информационная и когнитивная войны будут приобретать все большие масштабы и новые формы.

История информационной войны США против СССР и России

18 августа 1948 года Совет национальной безопасности США принял директиву 20/1 «Цели США в войне против России»[6]. Эта дата считается началом информационной войны США против СССР. Директива объявила войну качественно нового типа, где оружием служит информация, а борьба ведется за целенаправленное изменение общественного сознания. Задача заключалась во внедрении в советское общественное сознание таких ложных представлений об окружающем мире, которые позволили бы в дальнейшем манипулировать как населением страны, так и ее правящей элитой.

В январе 1981 года директор ЦРУ Уильям Колби представил доклад Президенту США Рональду Рейгану, в котором предложил новую наступательную стратегию по демонтажу «советской империи». Цели и средства этого наступления были обозначены в серии секретных докладов по национальной безопасности (National Security Decision Directives - NSDD). Качественно новым этапом в подрывной деятельности против СССР стало то, что руководство ею, которое раньше осуществлялось спецслужбами, теперь официально возглавили вашингтонские чиновники высшего государственного уровня. В подписанной Рейганом директиве NSDD-75 предписывалось прямое вмешательство во внутренние дела соцстран с целью подрыва их режимов[7].

Главную ставку делали на создание и консолидацию «внутренних оппозиционных сил», которые при поддержке извне должны были добиться захвата власти и политической переориентации своих стран на Запад. В директиве говорилось о том, что в основу конкретных действий должна быть положена «Программа демократии и публичной дипломатии». Эта программа, в частности, предусматривала подготовку будущих руководящих кадров и создание прозападных политических партий и профсоюзов в соцстранах, а также в странах третьего мира, придерживающихся социалистической ориентации. Были выделены средства на издание и распространение литературы, опровергающей «марксистскую диалектическую философию». В начале 1990-х годов США в результате информационно-психологической войны достигли своих целей. Пришедшее к власти правительство Клинтона стояло перед стратегическим выбором. Выбор был сделан в пользу информационной войны за тотальное мировое господство.

В 2004 году американский политолог Збигнев Бжезинский в своей книге констатировал, что Россия проиграла информационно-психологическую войну[8].

Результаты влияния цифровых технологий и западной идеологии

Анализ динамики времени пребывания молодежи в цифровой среде говорит о радикальном погружении молодежи в цифровое информационное пространство.

Аналитики российского провайдера услуг связи «Мегафон» выяснили, что в 2023 году дети стали тратить больше мобильного трафика на мессенджеры, чем на соцсети и музыку, вместе взятые. А лидером по росту стал «Телеграм», прибавивший 86% по сравнению с предыдущим годом. Любимыми приложениями у детей остаются видеосервисы: юные абоненты тратят на просмотр роликов 32% трафика. «Телеграм» и «WhatsApp» догоняют «YouTube» и «TikTok»: в этом году доля мессенджеров выросла более чем в полтора раза и достигла 30%[9].

Виртуальная реальность выступает в качестве пространства для конструирования социального смысла. Уход молодёжи от социума (эскапизм) проникает во все сферы жизни индивида, влияет на мировоззрение, формирует ценности и стиль жизни человека. Возможности Интернета позволяют создавать субкультуры, существование которых в реальном мире невозможно. Цифровая среда выступает как канал формирования стереотипов через определенные интернет-жанры: демотиваторы, мемы, интернет-комиксы и другие креолизованные тексты.

Угрозы традиционным духовно-нравственным ценностям

Информационные войны могут оказывать незримое влияние на духовно-нравственную сферу российского общества. Современные информационные технологии открывают для этого почти неограниченные возможности. RAND Corporation предлагает воспользоваться ими, переосмыслить стратегию США и сформулировать «ноополитику» как основу нового способа продвижения американских интересов в век информации[10].

Сущность ноополитики заключается в том, что решающим фактором в будущих идейных (ментальных) войнах станет вопрос - «чей нарратив победит». Переход к ноополитике предполагает среди прочего создание международных «специальных сил для СМИ», которые будут продвигать демократию за границей, создавать механизмы «для защиты демократических ценностей», разоблачать «темную сторону «мягкой силы», источниками которой называют Китай, Иран, Россию, а также такие негосударственные сети, как «Аль-Каида», «Исламское государство» и «WikiLeaks». RAND предлагает проводить периодические обзоры национальной «информационной позиции» по отношению к союзникам и противникам, которая «теперь так же важна, как и военная позиция». Такие меры призваны «отполировать имидж Соединенных Штатов и их союзников в мире; уменьшить остроту и жестокость конфликтов; оживить дипломатию, особенно публичную; и направить мир на курс к устойчивому миру и процветанию».

Разрабатываемые сегодня для военных нужд программы для анализа и влияния на поведение противника (такие, как программа COMPASS[11]) будут широко востребованы в гражданских сферах: например, для навязывания дебатов, продвижения нарративов, тестирования лояльности населения и пр.

Эффективному решению подобного рода задач будут способствовать стремительно развивающиеся сегодня «большие языковые модели» (Large Language Models). Такие программы способны не только создавать необходимый контент, но также делать тонкий профайлинг общественных групп с тем, чтобы создавать для них адресные нарративы. Они уже становятся сильным подспорьем для операторов информационных войн.

Российские традиционные духовно-нравственные ценности представляют собой одну из главных мишеней информационных операций. Результатом информационной войны может стать:

- размывание российских традиционных ценностей и ослабление единства народа Российской Федерации через внешнюю культурную и информационную экспансию, пропаганду насилия, нетерпимости и вседозволенности, а также уменьшение интеллектуального и культурного уровня, особенно среди молодежи;
- деформация исторической памяти, распространение ложных представлений об исторической отсталости России;
- принижение роли русского языка как инструмента сохранения и продвижения русской и многонациональной российской культуры, что может вести к противопоставлению русского языка другим языкам и разрывам общественных связей;
- блокирование передачи традиционных ценностей и знаний новым поколениям, размывание этнической, провинциальной и сельской культуры, замещение их мультикультурой на основе западной попкультуры;
- обесценивание семьи и семейных отношений, разрыв социальных связей и рост индивидуализма.

Ввиду того, что информационное противодействие становится частью противостояния с Западом, Россия нуждается в профессионально подготовленных кадрах и хорошо оснащенных институтах для ведения такого рода работы.

Механика информационной войны

Информационная война состоит из последовательности информационных операций, объединенных единым замыслом и согласованных по целям, задачам, формам и методам информационного воздействия. Элементами информационной войны также могут быть пропагандистские, неизбирательные, нацеленные на большие массы людей кампании и информационные идеологические диверсии (локальные действия с целью нанесения противнику конкретного ущерба).

Исторически известны применяемые в информационной войне *методы*:

- Метод большой лжи (использовался Геббельсом).
- Использование ограниченности человеческого восприятия для перегрузки людской памяти регулярно повторяющимися простыми формулировками через повторяющиеся кампании. Последовательность кампаний не должна оставлять времени для размышлений и оценок.
- Эксплуатация «стадного чувства» толпы, стремления принадлежать к определенной общественной группе. С помощью его возможно стимулировать моду, синхронизацию поступков, стремление к определенному «образу жизни», подчинение лидерам.
- Канонизация и дьяволизация отдельных личностей и исторических периодов.
- Переписывание истории.

Существуют распространенные *тактики* информационных и когнитивных войн:

- *Дезинформация:* распространение ложной или вводящей в заблуждение информации с намерением обмануть и манипулировать восприятием.
- *Пропаганда:* систематическое распространение информации, идей или слухов с целью формирования общественного мнения или влияния на поведение.
- *Психологические операции:* использование психологических методов для воздействия на эмоции, отношения и поведение целевых лиц или групп.
- *Манипуляции в социальных сетях:* целенаправленная организованная активность в сетях под видом естественных социальных информационных обменов. Обычно используются

такие методы, как астротурфинг (создание фейковых массовых движений), марионеточные аккаунты (создание нескольких фейковых аккаунтов для усиления повествования) и использование ботов или автоматизированных систем для манипулирования дискуссиями.

- *Кибератаки:* нацелены на критическую инфраструктуру, системы связи или информационные сети для нарушения информационных потоков или манипулирование ими, создание путаницы или подрыв доверия к цифровым платформам.
- *Меметическая война:* вирусное распространение мемов, культурных символов или крылатых фраз для влияния на общественное мнение и формирования нарративов, которые находят отклик у конкретных целевых групп.
- *Управление восприятием:* формирование и контроль того, как информация воспринимается отдельными людьми или группами. Достигается с помощью методов фреймирования, выборочного раскрытия информации или использования когнитивных предубеждений для влияния на принятие решений.
- *Операции влияния:* формирование мнений, отношений и поведения отдельных лиц или групп посредством целенаправленного обмена сообщениями, манипулирования социальными сетями или выращивания «лидеров мнения», которые могут распространять желаемые идеи.
- *Когнитивная эксплуатация:* использование уязвимостей человеческого познания, таких как когнитивные предубеждения или эвристика, для манипулирования процессами принятия решений. Это может включать в себя использование сообщений, основанных на страхе, или использование предвзятости для укрепления существующих убеждений.
- *Дипфейки и синтетические медиа:* высокореалистичные обработанные видео или аудио могут распространять ложную информацию, обманывать людей и подрывать доверие к визуальным или аудиодоказательствам[12].

Среди *приемов* манипулирования, используемых в ходе информационной войны, встречаются:

- наклеивание ярлыков;
- фальсификация информации;
- внушение с помощью авторитетной личности;
- распространение слухов;
- развенчание идеалов;
- насаждение новых идеалов;
- подмена проблем современности историческим прошлым;
- проецирование современных проблем в прошлое (когда исходя из интересов сегодняшнего дня выискиваются нужные исторические аргументы);
- «историческая» война (развенчание героев и выдающихся людей);
- размывание понятий (в такие слова, как «реформы», «демократия», «ценности», можно вкладывать очень разные смыслы);
- организация обстановки неустойчивости, тревожности за будущее.

В долгосрочном периоде информационная война с использованием подобных приемов может вести к отречению от традиционной веры, коренному изменению мировоззрения, основ общественного сознания, то есть приводить к когнитивным переменам.

Механизмы информационной войны

С августа 2011 года в Вооруженных силах США существует Командование операций военной информационной поддержки (Military Information Support Operations Command, MISOC). В 2017 году командование насчитывало около 2500 военнослужащих. MISOC проводит

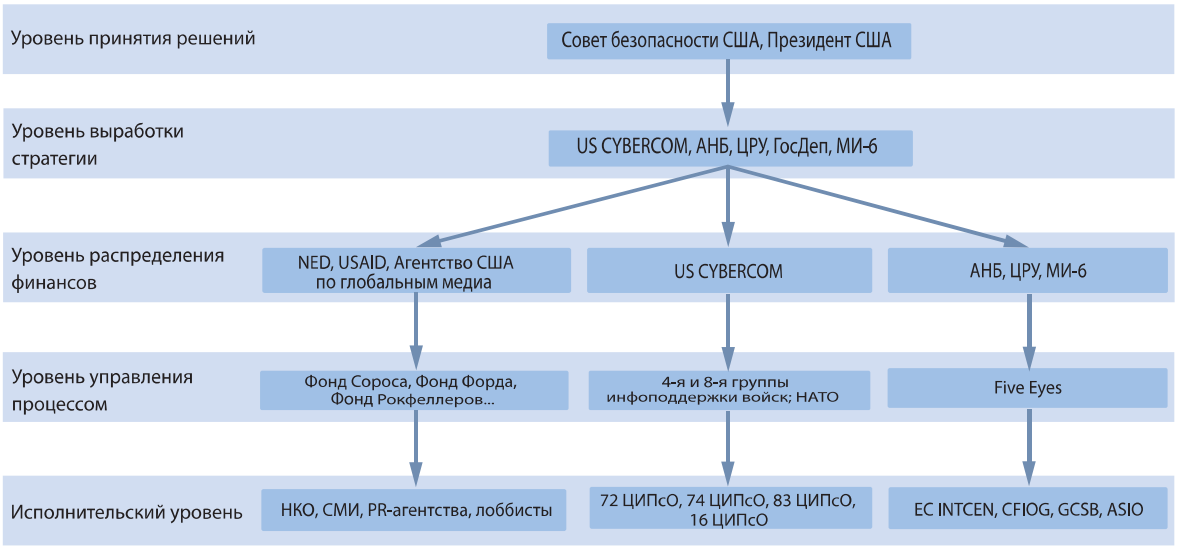
операции по информационному влиянию на иностранную аудиторию с целью воздействия на эмоции, мотивы, объективные рассуждения и в конечном счете изменению поведения иностранных правительств, организаций, групп и отдельных лиц способом, благоприятствующим целям Вашингтона.

У иностранной аудитории MISOC формирует представление о великой военной, политической и экономической мощи и решимости США. В случае конфликта MISOC стремится снизить боевую мощь противника, уменьшить вмешательство гражданского населения, свести к минимуму сопутствующий ущерб и максимально увеличить поддержку собственных операций местным населением. В буклете MISOC говорится, что специальные подразделения командования действуют «убеждая, а не принуждая физически, они полагаются на логику, страх, желание или другие психические факторы для стимулирования определенных эмоций, установок или поведения»[13].

Оценивая эффективность MISOC, подполковник Дэниел Дэвис сказал: «Высокопоставленные военные руководители США настолько исказили правду при общении с Конгрессом США и американским народом относительно условий на местах в Афганистане, что правда стала неузнаваемой»[14].

Летом 2023 года Пентагон опубликовал «Стратегию по операциям в информационной среде на 2023 год». В документе подчеркивается необходимость создания специальных «информационных сил» для «защиты от попыток влияния на общественное мнение». Согласно Стратегии Министерство обороны США должно разработать процедуру быстрого развертывания подразделений информационных сил. Документ предусматривает привлечение военных и гражданских специалистов, совершенствование набора и обучения, перспективы карьерного роста[15].

В настоящее время американскую систему по ведению информационной войны можно представить следующим образом[16]:



Практическое осуществление информационных операций Пентагона можно изучить на примере использования фальшивых аккаунтов «Twitter» для влияния на общественное мнение в Йемене, Сирии, Ираке, Кувейте и других странах[17].

В рамках НАТО также имеются подразделения, занимающиеся информационными операциями. За политику психологических операций НАТО отвечает Военный комитет. Он сформировал рабочую группу Combined Jointed Phycological Operations Task Force, которая служит

центром, где страны-участницы блока могут сверять и координировать свои информационные стратегии.

В документе НАТО «Allied Joint Doctrine for Psychological Operations» говорится: «Понимание и сочувствие являются ключом к PSYOPS; анализ целевой аудитории является инструментом, с помощью которого это достигается. Эффективный анализ должен обеспечить глубокое контекстуальное понимание культурного, исторического и социального состава целевой аудитории, а также глубокое понимание эмоциональных и заслуживающих доверия тем и символов, которые могут быть использованы для воздействия на краткосрочное поведенческое и долгосрочное поведение и изменение отношения. Развитие знаний (включая разведку из всех источников (ASINT) имеет важное значение для эффективного понимания. Психологи должны с пониманием относиться к существующему поведению и отношению целевой аудитории, чтобы понять, как возможно их изменить или усилить»[18].

На базе этого доктринального документа НАТО в Вооруженных силах Украины разработана «Доктрина психологических операций Сил специальных операций Вооруженных сил Украины»[19].

Среди задач психологических операций в доктрине, в частности, названы:

- снижение уровня доверия личного состава войск противника к своему военно-политическому руководству, военному командованию;
- подрыв у военно-политического руководства, военного командования и личного состава войск противника психологической стойкости и готовности к выполнению задач по предназначению;
- формирование и содействие обострению существующих противоречий среди населения общественно-политического, экономического, культурного, этнического, религиозного характеров.

В документе говорится: «Каналами воздействия могут являться: сеть Интернет, сети мобильной связи, другие информационно-телекоммуникационные системы; печатные и электронные средства массовой информации, другие информационные ресурсы сети Интернет; носители внешней рекламы; агентурная сеть и движение сопротивления, ключевые лица, лидеры общественного мнения и ключевые коммуникаторы, другие связанные с целевыми аудиториями лица и группы лиц».

Задачами информационно-психологических операций названы:

- деморализации противника;
- дискредитации (демонизации) противника;
- введение противника в заблуждение;
- снижение поддержки противника со стороны гражданских лиц;
- привлечение гражданских лиц к сотрудничеству;
- обеспечение невмешательства гражданских лиц;
- делегитимизации противника и почвы конфликта.

Среди вариантов применения спецподразделений приводятся:

- распространение слухов о присвоении руководством военных трофеев и другого захваченного имущества;
- распространение слухов о массовом отказе от активных действий со стороны определенных подразделений противника;
- информирование собственного населения и международного сообщества о нарушении противником предварительных соглашений, договоренностей и норм международного гуманитарного права («демонизация» противника);

- рассылка на мобильные телефоны, электронные адреса, мессенджеры руководства и личного состава материалов, которые вызывают стресс, панику, страх;
- распространение среди членов семей материалов с призывом способствовать отказу от участия в боевых действиях военнослужащих, дезертирства;
- размещение видеообращений военнопленных к своим сослуживцам, фото-, видео- и информационных материалов о значительных потерях в живой силе и технике противника;
- побуждение населения к проведению антивоенных мероприятий;
- побуждение населения к предоставлению сведений о перемещении противника, иных действиях войск;
- проведение информационных диверсий (подрывная информационная деятельность).

Способы борьбы с информационными атаками

Существуют некоторые аналитические способы, позволяющие противодействовать инструментам информационной войны:

- *Определение тактики информационной войны:* изучать и идентифицировать различные тактики, используемые в когнитивной войне, такие как кампании по дезинформации, распространение пропаганды, психологические операции и манипуляции в социальных сетях.
- *Мониторинг источников информации:* анализ содержания, происхождения и способов распространения информации помогут выявить потенциальные кампании информационной войны и отследить их источники.
- *Обнаружение и анализ дезинформации:* анализ содержания поможет раскрыть мотивы таких кампаний.
- *Разработка контрмер:* контрмеры могут включать в себя разработку стратегий по разоблачению ложной информации, информирование общественности.
- *Повышение кибербезопасности:* защита от хакерских атак, утечки данных и других форм кибератак, которые могут способствовать ведению когнитивной войны.
- *Разработка рекомендаций для принятия решений:* аналитические доклады помогут принимающим решение лицам в понимании природы и методов информационной войны.

Возможности для международно-правового регулирования

В мае 2023 года Россия вместе с четырьмя странами-единомышленницами внесла на рассмотрение ООН обновленную концепцию Конвенции по международной информационной безопасности[20].

Концепция стала логичным продолжением принятой по инициативе России и еще 26 государств-единомышленников Генеральной Ассамблеей ООН в декабре 2022 года резолюции под названием «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности». В этом решении впервые содержалось положение о необходимости выработки международно-правового механизма по обеспечению информационной безопасности.

Однако в отличие от предыдущих российских инициатив проект конвенции мая 2023 года поддержали только пять государств: Беларусь, Венесуэла, КНДР, Никарагуа и Сирия. Среди поддержавших нет многих традиционных сторонников российского подхода к теме МИБ, прежде всего Китая.

Вероятно, России следует продолжить консультации по данному документу с другими странами, а также продвигать свои подходы через региональные и международные объе-

динения, прежде всего ШОС и БРИКС, особенно в части международного сотрудничества в области информационной безопасности.

Концепция конвенции справедливо не содержит упоминания термина «информационная война». Наверное, этот термин следует рассматривать как журналистский либо, в крайнем случае, пригодный для использования в академических кругах.

Понятие агрессии определено в резолюции Генеральной Ассамблеи ООН: «Агрессией является применение вооруженной силы государством против суверенитета, территориальной неприкосновенности или политической независимости другого государства или каким-либо другим образом, несовместимым с Уставом ООН, как это установлено в настоящем определении»[21].

Проблема применения международного права к информационному противоборству связана со сложностью урегулирования ряда вопросов:

- терминологическая путаница: понятие «информационная война» применяется не только к конфликтам, но и к пропаганде, работе СМИ;
- преобладающий нелетальный характер информационной войны;
- идентификация сторон конфликта (в какой момент человек становится комбатантом);
- возрастающая взаимосвязь между военными и гражданскими информационными ресурсами (использование социальных сетей для военных целей);
- определение «информационная атака», как правило, не имеет связи с материальным миром, тогда как право вооруженных конфликтов сосредоточено на прямом физическом уничтожении.

Обсуждению применимости МГП и его ключевых принципов к «информационным операциям» препятствует двусмысленность информационной войны, поскольку общепринятая концепция нападения связана с порогами, которые должны быть преодолены, чтобы информационная операция квалифицировалась как нападение. При отсутствии причинно-следственной связи, ведущей к причинению физического вреда, действия военных в ходе информационной войны, вероятно, не подпадают под действие традиционного права вооруженного конфликта.

Однако с информационными операциями могут быть связаны понятия МГП «распространение террора» и «сильные страдания». В соответствии с Дополнительным протоколом I любые акты насилия или поведения, направленные на сеяние страха среди гражданского населения, запрещаются. Поэтому психические страдания и действия с первоначальной целью причинения психического вреда находятся в диапазоне, охватываемом нормами МГП. Для применения правил и норм МГП необходимо принять измеримые критерии оценки степени психических и душевных страданий, причиняемых наступательными информационными операциями и военным обманом.

МГП запрещает любое действие или угрозу, основной целью которых является распространение террора среди гражданского населения[22]. Запрет на распространение террора может быть рассмотрен применительно к эффекту, который современные информационные операции оказывают на гражданское население. Несмотря на ненасильственные последствия, информационная война требует более детального регулирования в соответствии с вызовами современного мира, где последствием искажения медиаэкосистемы может стать утрата общественного доверия к государственным СМИ и государственным структурам, политическая нестабильность и морально-психологическое подавление пострадавшего государства со стороны государства-противника.

Кодификацию термина могло бы упростить выделение двух состояний информационной войны: вооруженные столкновения, направленные на уничтожение критической информа-

ционной инфраструктуры, и применение информационного оружия в киберпространстве, нацеленного на искажение массового сознания и управление им.

В качестве самостоятельной категории в международном праве можно определить «информационное оружие», к которой следует отнести информационные системы, способные причинить прямой вред. При этом следует отталкиваться от принципиальных отечественных установок на международных площадках - непризнание ИКТ в качестве оружия, их использование исключительно в мирных целях.

Открытым остается вопрос, можно ли квалифицировать ложную информацию как информационное оружие. Вероятно, не любая ложная информация может считаться информационным оружием. Возможно, более приемлемым будет ввести в оборот понятие «дезинформация».

Среди перспективных направлений развития международного права применительно к информационной войне можно выделить следующие темы:

- Определение понятий «военные действия», «акт насилия», «нападения» применительно к информационным операциям.
- Принятие правил, регулирующих информационные операции.
- Определение и закрепление в международных договорах границ суверенитета в цифровом пространстве, в том числе в области управления адресным пространством глобального киберпространства и его национального сегмента.
- Определение порога вооруженного конфликта (применительно к информационному пространству).
- Уточнение принципов присвоения (атрибуции) ответственности за информационные атаки.
- Определение статуса комбатанта для лиц, осуществляющих акты враждебного использования информационных технологий и дезинформации.
- Принцип невмешательства во внутренние дела применительно к информационному пространству.

---

[1]Конвенция об обеспечении международной информационной безопасности (концепция). 22 сентября 2011 г. // http://polit-discourse.ru/articles/295

[2]Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ №646 от 05.12.2016 г. // Собр. законодательства Рос. Федерации. 2016. №50. Ст. 7074.

[3]Соглашение между правительствами государств - членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности: международное соглашение, принятое государственными органами и/или другими субъектами права ШОС // Бюллетень международных договоров. №1. 2012 г.

[4]*Алексеев Г.В.* Информационная война как социально-правовая категория // Научно-технический вестник Санкт-Петербургского государственного университета информационных технологий, механики и оптики. 2004. №12. С. 163-168.

[5]*Libicki Martin C.* What Is Information Warfare // https://www.goodreads.com/book/show/2232467.What_Is_In formation_Warfare

[6]Thomas H. Etzold and John Lewis Gaddis, eds. Containment: Documents on American Policy and Strategy, 1945-1950. NSC 20/1 (pages 173-203) // https://archive.org/details/NSC201-USObjectivesWithRespectToRussia/NSC_20_1_book/

[7]US Relations with the USSR. National Security Decision Directive 75. 17 Jan. 1983 // https://irp.fas.org/offdocs/nsdd/nsdd-75.pdf