# ИНФОРМАЦИОННЫЕ ВОЙНЫ КАК «ЦИФРОВОЙ» АСПЕКТ ГЛОБАЛИЗАЦИИ

**Мехтиева Н. Р.**[*]

*Статья посвящена рассмотрению информационного аспекта процесса глобализации с акцентом на информационное противостояние между различными субъектами в киберпространстве. Проанализированы институциональные и функциональные проявления феномена информационной глобализации, а также информационный аспект понятия «мягкая сила». Автор предлагает классификацию феномена информационных войн на основе критерия открытости и иллюстрирует ее конкретными примерами. Основной тезис, проводимый в статье, состоит в том, что феномен информационных войн выходит за рамки сугубо милитаристской сферы и в современную цифровую эпоху получает гражданское измерение, проявляясь, в частности, в феномене медиавойн.*

***Ключевые слова:*** *информационная война, кибератаки, Интернет, глобализация, глобальные информационные корпорации.*

*The article is devoted to the information aspect of globalization process, with an emphasis on the informational opposition between various subjects within cyberspace. The author also analyses the institutional and functional manifestations of the phenomenon of information globalization, and also of the informational aspect of the 'soft power' notion. She offers a classification of 'information wars' based on the transparency criterion and illustrates it by particular examples. The main idea of the article is that in the current digital era the 'information wars' phenomenon surpasses the purely militaristic sphere and also obtains a civil dimension which shows up in the media-wars phenomenon.*

***Keywords:*** *information war, cyber-attacks, Internet, globalization, global media corporations.*

При описании нынешнего миропорядка стало уже общим местом использование термина «глобализация», понимаемого как формирование и функционирование экономических, политических и информационных взаимосвязей и взаимодействий в глобальном (то есть планетарном) масштабе. Глобализация в этом смысле носит универсальный и всеохватывающий характер и затрагивает весь сложный комплекс общественных отношений. Речь идет, в зависимости от сферы исследования, о той или иной «глобализации с прилагательным», причем на первый план чаще всего выдвигаются экономические и политические аспекты, информационные же грани глобализации остаются на периферии анализа в качестве производных [см.: Глобализация… 2002; Global… 2014].

[*] Мехтиева Нигяр Рустам кызы – аспирант кафедры «Зарубежное регионоведение и внешняя политика» Российского государственного гуманитарного университета. E-mail: nika_mex@hotmail.com.

Что же представляет собой «информационная глобализация»? Без ответа на этот общий вопрос невозможно перейти к рассмотрению более частных, в том числе к проблеме информационных войн, безусловно, имеющих глобальное измерение. Представляется, что «информационную глобализацию» можно рассматривать в двух аспектах: **институциональном** и **функциональном**. В первом случае она выступает как объективный процесс организации (и самоорганизации) глобальной информационной инфраструктуры, то есть сети информационных институтов, обеспечивающих создание и трансляцию информации. Институциональный аспект охватывает очень широкий спектр процессов: от распространения персональных компьютеров до создания транснациональных медиакорпораций. В функциональном же плане «информационная глобализация» выступает как процесс динамичного действия этих институтов, как течения и флуктуации глобальных информационных потоков, как их пересечение, взаимопроникновение и столкновение, нередко принимающее конфликтный и агрессивный характер. Именно на стыке этих информационных потоков «рождаются» информационные войны, к рассмотрению феномена которых мы перейдем ниже.

В политологической литературе современную эпоху нередко обозначают как информационную, и у подобного определения есть немало оснований. Стремительное, даже экспоненциальное, развитие цифровых технологий привело к тому, что информатизация затронула практически все сферы жизни общества – от «низового», сугубо бытового (уровня обыденных социальных отношений) до таких «высоких» сфер, как военное дело и геополитика.

Сейчас уже невозможно представить, чтобы какое-либо государство при выработке национальной военной доктрины обошло стороной такую важнейшую составляющую, как информационная безопасность. Нельзя забывать и о том, что сама глобальная сеть Интернет появилась на свет во многом как результат развития именно военных технологий и изначально предназначалась для сугубо милитаристских целей. Только спустя десятилетия этот глобальный информационно-сетевой инструмент стал неотъемлемым атрибутом повседневной жизни, но истоки его коренятся в военной сфере. Напомним, что «ключевую роль в появлении новых технологий играло новаторское исследовательское агентство Министерства обороны США DARPA, которое положило начало Интернету. С начала 60-х гг. существовала сеть ARPANET (Advanced Research Project Agency Network), предназначенная для управления перспективным планированием научно-исследовательских работ Министерства обороны США. В 80-х гг. было принято решение о подключении к ARPANET частных и коммерческих структур, вследствие чего и появился Интернет» [Удовик 2002: 221].

Отсюда видно, что информационные и военные технологии изначально шли «рука об руку», и к настоящему времени эта связь, хоть и закамуфлированная «бытовым» пользовательским Интернетом, только усилилась, хотя это не столь очевидно обыденному сознанию. С начала XXI в. применение информационных технологий превратилось в мощный фактор мировой политики, и нередко именно информационная и медиа- составляющие оказывают сильное воздействие на выстраивание международных отношений. Тех целей, которые рискованно достигать военным путем, в условиях доминирования информационных технологий подчас можно достичь «мирными» информационными методами. Именно на стыке этих двух подходов возник термин «информационная война».

Проанализировать феномен информационных войн невозможно в отрыве от понятия «мягкой силы», которое в последнее время приобрело устойчивую медийную и даже научную популярность, стало, если можно так выразиться, политологически модным. Редкая статья о международных отношениях обходится без использования термина «мягкая сила». Здесь рассмотрение этого понятия оказывается не просто данью моде, но и научно оправданным, поскольку информационные войны выступают, с нашей точки зрения, наиболее органичными проявлениями «мягкой силы».

Концепция «мягкой силы», впервые выдвинутая американским политологом Джозефом Наем, изначально имела сугубо электоральное назначение: она была призвана доказать, что когда прямые приемы предвыборной конкуренции оказываются неэффективными, целесообразно задействовать скрытые и незаметные методы политической борьбы. Термин быстро вошел в политический обиход, стал широко применяться политиками, особенно американскими, а затем вышел за рамки предвыборной тематики, получив геополитическое наполнение. Сам Дж. Най доработал свою концепцию применительно к международным отношениям в широко известной монографии «Мягкая сила: средства успеха в мировой политике» [Nye 2004]. Суть концепции мягкой силы состоит в следующем: там и тогда, где и когда достичь цели жестким силовым путем становится объективно невозможным, применимы методы несилового, «мирного» воздействия, обеспечивающие желаемые результаты. Российский политолог Е. Харитонова отмечает: «Дж. Най определяет “мягкую силу” как способность государства достичь желаемого не путем принуждения, а с помощью убеждения, основанного на привлекательности внешней политики, культуры и национальных ценностей» [Харитонова 2015: 48]. Она же заключает: «Противопоставленная “жесткой силе” и основанная на привлекательности или привлекательном имидже государства, “мягкая сила” представляется альтернативным инструментом решения внешнеполитических задач, часто более предпочтительным, чем военные или экономические методы» [Там же].

Любопытно, что параллельно с американскими аналогичные теоретические разработки велись китайскими политологами. Восточный аналог концепции «мягкой силы» носит название «трансграничной орбитальной войны», которая остается малоизвестной русскоязычному читателю. Китайские военные теоретики справедливо полагали, что «победить Соединенные Штаты Китаю невозможно, если сталкиваться на уровне военных сил, но если обсуждать весь набор “орбиталей”, а именно финансовую войну, пропагандистскую войну, различные сетевые формы, то действие на всех возможных “орбиталях” может дать совершенно иной результат» [Громыко 2016].

Примечательно, что две схожие по сути концепции развивались независимо друг от друга на разных «полюсах» современного мира; это свидетельствует, что ими объективно отражен определенный макрополитический тренд: «мягкая сила» действительно оказывается мощным фактором в современной мировой политике.

Важнейшим элементом проведения стратегии «мягкой силы» является информационная война как процесс применения информационной силы. Понятие информационной силы в контексте рассмотрения «мягкой силы» уже применяется в отечественной политологии. Так, к интересным выводам приходит Ю. Давыдов, проанализировавший ряд силовых компонент этого общего понятия: эконо-

мическую, политическую, научно-техническую, идеологическую и информационную силу. Он констатирует: «Среди исследователей идут дискуссии относительно использования информационной силы на международной арене. Это вполне закономерно, ибо человечество вступило в век информации и информационных систем. …Контроль над международными коммуникациями создает новые формы зависимости между государствами. На рубеже веков развернулась “четвертая информационная революция”, во многом характеризующаяся максимальным внедрением мультимедийных, цифровых технологий…» [Давыдов 2004: 76].

В трактовках термина «информационная война» есть и тенденция ставить акцент на втором слове, то есть выделять милитаристский аспект как определяющий. Так, Г. Б. Корсаков, определяя данное понятие применительно к военной стратегии США, отмечает: «Под этим термином понимается комплексное информационное воздействие на систему государственного и военного управления противника, которое уже в мирное время приводило бы к принятию благоприятных для США решений, а в ходе конфликта полностью парализовало бы функционирование структуры управления противника» [Корсаков 2012: 49].

Представляется, что абсолютизация сугубо милитаристского аспекта непомерно сужает спектр проявлений информационных войн. С нашей точки зрения, данный феномен имеет достаточно ярко выраженное «гражданское» измерение, проявляющееся в подчас агрессивном информационном воздействии на общественное сознание и социально-психологическое состояние гражданского населения средствами глобальных СМИ и посредством их «информационного эха» в социальных сетях.

В научной и особенно публицистической литературе имеет место некоторая терминологическая путаница относительно разных видов «войн»: такие предикаты войны, как «медиа», «информационная», «кибер», «цифровая», «сетевая» и т. п., нередко используют как синонимы. Подобную ситуацию можно объяснить тем, что сам феномен информационного противостояния является инновационным элементом мировой политики и пока в недостаточной мере подвергнут теоретическому осмыслению и политологической рефлексии. Рискнем предложить авторскую классификацию различных типов информационных войн и в определенном смысле логически упорядочить обозначенные выше термины.

Наиболее общим, объединяющим родовым понятием выступает термин «информационная война». Руководствуясь критерием степени транспарентности, можно выделить два типа подобного рода войн: *открытые* и *латентные*. К открытым относятся медиавойны, в которых ведущими субъектами информационного противостояния оказываются национальные, региональные или глобальные массмедиа, новостные корпорации. К закрытым или латентным относятся кибервойны, которые могут разворачиваться в форме хакерских атак как между государствами, так и между автономными по отношению к ним интернет-сообществами. Промежуточным (или гибридным) вариантом информационных войн являются, на наш взгляд, сетевые войны. Рассмотрим эти разновидности более детально.

Особенность медиавойн состоит в том, что медиакорпорации как информационные платформы, охватывающие крупные аудитории, создают определенные,

подчас противоречащие друг другу «картины мира». Столкновение в общественном сознании подобного рода противоположных мировоззренческих схем нередко дает эффект информационной войны. Наиболее мощная «новостная» составляющая имеет место, безусловно, в информационной внешней политике США. Исторические корни такого статуса информационно-новостных каналов восходят к завершающему этапу холодной войны между США и СССР. В 1986 г. администрацией Р. Рейгана была принята директива «Об американской международной информационной политике», где, в частности, декларировалось, что «международная информация – неотъемлемая и жизненно важная часть американской стратегии и политики национальной безопасности в общем смысле. В комплексе с инструментами общественной дипломатии международная информационная политика является ключевым стратегическим инструментом формирования фундаментальных политических и идеологических тенденций в мире в долгосрочной перспективе» [Шариков 2015: 28]. Следуя этой установке, в 1989 г. Пентагон создал специальную группу – Командование сил специальных операций, в компетенцию которого входило проведение различного рода психологических операций. Анализируя современную американскую доктрину информационной политики, российский политолог П. А. Шариков приходит к выводу, что «в доктринальных документах по американской стратегии последних лет термин “информационная война” не употребляется. Американцы отказались от использования этого термина в качестве определения способа ведения конфликта исключительно информационными средствами. Вместе с тем в открытых доктринальных документах употребляются такие понятия, как информационные операции военной поддержки (military information support operation), сетецентрические способы ведения боя (net-centric warfare)» [Там же]. С нашей точки зрения, это явно демонстрирует стремление терминологически «закамуфлировать» реализуемую де-факто стратегию информационной войны, проводниками которой выступают как государственные, так и частные информационные агентства США и их политических союзников.

Попытаемся проследить основные векторы подобного рода новостного, а по сути мировоззренческого противостояния, а также стратегии противодействия, которую применяют другие государства для минимизации влияния транснациональных информационных корпораций.

Центром столкновения информационных потоков в последние годы, безусловно, стала Украина. В 2014 г. конгресс США с целью проведения в международном масштабе своей новостной политики принял закон «Об американском иновещании на территории Украины и соседних регионов». Основным институтом, призванным реализовывать данный законодательный акт, стал созданный еще в 1994 г. Совет директоров телерадиовещателей, в состав которого входят ведущие информационные агентства международного профиля с вещанием на 28 языках мира («Голос Америки», «Свободная Европа», «Радио Свобода», CNN и другие). Именно с целью противодействия их активности и, в свою очередь, международной трансляции многополярной картины мира в ноябре 2014 г. было создано агентство «Sputnik», а также активизирована и расширена деятельность медиахолдинга «Russia Today», функционирующего с 2005 г.

Другим стратегическим вектором ведения информационных медиавойн современности выступает геополитическая оппозиция «глобального Севера» и «глобального Юга», причем лидером первого выступают США, а второго – Китай, хотя существует целый ряд локальных «фронтов» этого противостояния. Е. А. Виноградова справедливо отмечает: «В связи с ростом международной напряженности в XXI в. особую актуальность приобретает изучение глобальных технологий, используемых в информационном противоборстве между индустриальными странами Востока и экономически развитыми странами Запада» [Виноградова 2012: 137].

В начале XXI в. «глобальный Юг», особенно в лице Китая, арабского мира, Ирана и стран Латинской Америки, заметно активизировал свою информационную политику, создавая либо существенно расширяя агентства, альтернативные мировым информационным корпорациям. Особенно обращает на себя внимание стратегия КНР по наращиванию информационной мощи на международной арене. Анализируя китайскую политику в глобальном информационном пространстве, секретарь российского МИД Евгений Евдокимов отмечает: «В январе 2009 г. Пекин объявил о планах выделить до 45 млрд юаней (порядка 6,6 млрд долларов) на расширение китайских иноязычных СМИ. Планы включали увеличение количества зарубежных корпунктов государственного информационного агентства “Синьхуа” до 186, а также расширение сферы его деятельности на спутниковое и интернет-вещание. В 2009 г. были запущены каналы на китайском и английском языках, планируется начало вещания на арабском, французском и русском. Центральное телевидение Китая CCTV в дополнение к уже действующим каналам на английском, французском и испанском языках в 2009 г. запустило канал на русском языке, а в 2010 г. – на арабском и португальском» [Евдокимов 2011: 74]. Таким образом, Китай явно оспаривает у США мировое информационное лидерство и в скором времени может вырасти в серьезного игрока на арене глобального медийного противостояния.

Другим регионом «глобального Юга», где активно ведутся медиавойны, является Ближний Восток. Здесь целью подобных операций со стороны США и их союзников выступает переформатирование общественного мнения в сторону толерантности и лояльности по отношению к их внешней и военной политике. Так, перед началом военных операций в Ираке и Афганистане США при техническом содействии своих крупных информационных агентств создали своего рода «филиалы» американских СМИ, в результате чего на свет появился телевизионный канал «Al Hurra» и радиостанция «Sawa», вещающие на арабском языке [Torres 2011: 9]. Симметричным ответом арабского мира на такого рода информационную агрессию стало создание в 2003 г. англоязычной версии влиятельного в регионе новостного канала «Аль-Джазира».

Похожую ситуацию можно наблюдать в Латинской Америке, где против правительств левой политической ориентации развернулась мощная информационная война со стороны американских и западноевропейских транснациональных медийных корпораций, которым вторят местные частные СМИ, находящиеся в непримиримой оппозиции к левым и левоцентристским правительствам. В Аргентине и Бразилии медиакорпорации долгое время выступали своего рода «супер-

партией», сыгравшей важнейшую роль в консолидации правых сил и смене власти в 2015–2016 гг. В настоящее время медиавойна в полном объеме ведется против Венесуэлы и других стран «левой группы». Флагманами массированной информационной атаки выступают испанский медиахолдинг PRISA, владеющий влиятельной газетой «El Pais», а также испаноязычные версии североамериканской компании CNN, британской BBC и др. Эти СМИ проводят четкий редакционный курс на дискредитацию левых президентов и всей их политики, в первую очередь социально-экономической, и безапелляционную поддержку правой оппозиции с целью обеспечить переход власти в ее руки. С целью противодействия информационной агрессии в 2005 г. по инициативе Венесуэлы был создан альтернативный новостной канал «TeleSur» с филиалами в двенадцати государствах Латинской Америки.

Перейдем к рассмотрению другого типа информационных войн. Закрытый, или латентный, тип информационных войн предполагает более широкий «веер» разновидностей, поскольку сама природа информационных «военных» действий предполагает максимальное сохранение анонимности субъекта осуществления операций. Эффективность информационно-диверсионной операции во многом определяется тем, насколько обеспечены и сохранены анонимность и обезличенность проводящего ее субъекта. Это обстоятельство и определяет «популярность» латентных информационных войн в современном арсенале интернет-противостояний.

К латентному типу можно отнести в первую очередь кибервойны. В них решаются военные или околовоенные цели и задачи, но намеренно без использования собственно милитаристского арсенала, а исключительно посредством компьютерных технологий. Например, выведение из строя той или иной инфраструктуры «противника» путем внедрения в электронную систему вируса (как это произошло в 2009 г. в отношении Ирана, когда программа StuxNet, разработанная американскими программистами, нарушила функционирование компьютерной сети и поставила под угрозу проведение иранской ядерной программы). Субъектами противостояния в кибервойне оказываются как отдельные государства, целенаправленно стремящиеся избежать военного столкновения путем перевода противоборства в информационную плоскость, так и анонимные или квазианонимные интернет-сообщества, проводящие хакерские атаки против национальных государств, их политических, экономических или информационных институтов.

Характерно, что ряд государств уже и юридически включили ведение кибервойн в свои военные доктрины. В частности, так поступил Пентагон. В 2010 г. на страницах влиятельного журнала «Foreign Affairs» бывший министр обороны США Уильям Линн в статье под названием «Защищая новые владения. Киберстратегия Пентагона» констатировал: «В вопросах военной доктрины Пентагон уже формально признал киберпространство как новое поле ведения войны. Фактически оно превратилось в критический фактор военных операций как на земле, так и на море и в воздухе» [Lynn III 2010]. По оценке американского эксперта по информационной безопасности Джеймса Льюиса, в настоящее время двенадцать из пятнадцати ведущих военных держав мира ведут прикладные исследования по разработке программ кибервойны, включая тактику и стратегию

[Año... 2013]. В число таких стран входят США, Франция, Германия, Китай, Россия, Япония, Великобритания, Израиль и др. В мировой прессе уже введен в оборот термин «холодная кибервойна» по аналогии с холодной войной между США и СССР в XX в. Эксперты полагают, что в настоящее время мир стоит на пороге полномасштабного информационного киберконфликта, предпосылки которого уже созданы опытом различных стран в первые десятилетия XXI в.

Рассмотрим вкратце историю современных кибервойн. Одной из первых крупных кибероперацией стала акция, осуществленная сербскими военными в период противостояния агрессии НАТО в 1999 г. Национальный герой Сербии капитан Драган создал мобильную военную группировку из 450 человек, в состав которой входили также специалисты в области информационной безопасности. В течение недели им удалось блокировать работу сайта Белого дома, а также внедриться в информационные системы Пентагона и затруднить их функционирование [Fuentes 1999].

С 1998 по 2000 г. была зафиксирована слежка за компьютерами NASA, Пентагона, Министерства энергетики США и ряда научно-исследовательских центров, а также за американскими университетами. В прессе эта операция получила обозначение «Лунный лабиринт» (Moonlight Maze). По неподтвержденной информации, эта двухлетняя операция проводилась российскими хакерами, хотя никаких доказательств причастности России к ней так и не было установлено.

В 2005 г. газета *The Washington Post* опубликовала материал, в котором говорилось о кибератаке со стороны Китая, получившей название «Операция Титан». На этот раз информационной атаке подверглись Государственный департамент, министерства обороны и энергетики [Graham 2005]. Операции «Лунный лабиринт» и «Титан» побудили Конгресс США провести исследование и опубликовать доклад под названием «Информационные операции, электронная война и кибервойна: возможности и связь с вопросами политики». В докладе красной нитью проходил тезис: кибервойны имеют непосредственную связь с мировой политикой; основными потенциальными противниками США в киберпространстве становятся Китай, Россия, Куба, Иран, Ирак, Ливия и КНДР, а также многочисленные негосударственные террористические группы, способные атаковать гражданские и военные американские сети (Congressional Research Service).

В 2010 г. *The Washington Post* опубликовала объемный материал о кибершпионаже Китая в отношении ведущих тридцати четырех американских компаний. Эксперты зафиксировали новый качественный прорыв в уровне защищенности от информационных атак, использовании новых кодов и т. п. Главной целью атак были названы промышленный шпионаж и контрразведка. В прессе данная операция получила наименование «Аврора» [Google… 2010].

Следующим значительным эпизодом мировой кибервойны стал уже упоминавшийся вирус StuxNet, который по оценке экспертов компании «Symantec», специализирующейся на информационной безопасности, стал «первым в истории информационным вирусом, способным наносить ущерб в физическом мире» [The New York Times 2011].

Главная цель вируса StuxNet состояла в том, чтобы разрушить иранские ядерные центрифуги, связанные с процессом обогащения урана, и тем самым предот-

вратить, как утверждалось, создание Ираном атомного оружия. Атака была довольно успешной: удалось вывести из строя около тысячи центрифуг (шестую часть от общего количества, которым располагало тогда правительство Тегерана). По оценкам, внедрение этого информационного червя задержало развитие ядерной программы Ирана на два года. Тем самым после операций «Лунный лабиринт», «Титан» и «Аврора», совершенных в отношении институтов США, активное контрнаступление в мировом киберпространстве начали проамериканские хакеры. С полной уверенностью утверждать, что авторство StuxNet принадлежит Пентагону, нельзя, поскольку нет прямых доказательств его причастности к разработке этого червя; но если следовать логике «кому это нужно», то США оказываются главными бенефициарами результатов информационной атаки на Иран (в то время активно шли переговоры об иранской ядерной программе, и Вашингтон занимал самую жесткую позицию, отказывая Тегерану в праве развивать свою атомную энергетику).

Однако Иран был отнюдь не единственной мишенью вируса. Его запуск ознаменовал, пожалуй, первую в истории скрытую информационную войну всемирного масштаба, поскольку червем StuxNet были заражены компьютеры многих стран. По данным корпорации *Symantec*, из ста тысяч пораженных компьютеров на долю Ирана приходилось более половины (60 тысяч), остальными жертвами этой массовой кибератаки стали компьютеры Индонезии, Индии, Азербайджана, Пакистана, Малайзии, Узбекистана, России и даже Великобритании [Symantec]. Своеобразным «преемником» StuxNet стал вирус Duqu, подвергавший деформации главным образом документацию и текстовые документы Word. Запуск этого вируса также был направлен главным образом против Ирана, но в определенной степени затронул и другие государства: Судан, Францию, Швецию, Индию, Украину.

В 2012–2013 гг. доминанта информационного глобального противостояния вновь вернулась в плоскость отношений между США и Китаем. Как из рога изобилия посыпались взаимные обвинения в кибершпионаже. Так, китайский Национальный центр экстренного реагирования на ситуации в Интернете опубликовал информацию о том, что в 2012 г. более 30 тысяч китайских сайтов подверглись хакерским атакам американского происхождения [Жиров 2013: 2]. В ответ был опубликован сенсационный доклад частной североамериканской фирмы «Mandiant» под названием «Обнаружен один из центров кибернетического шпионажа КНР». В нем, в частности, говорилось, что группе хакеров, работающих в официальных военных структурах китайской армии, «удалось похитить данные у 141 компании по всему миру, 115 их них – американские» [Волков 2013: 5]. Взаимные обвинения не переросли в полномасштабный дипломатический конфликт, но ситуация находилась на грани срыва и были все условия для перевода «вербальной войны» в политическую плоскость.

Субъектами проведения кибероперации могут быть и негосударственные структуры, осуществляющие похищение конфиденциальной либо эксклюзивной информации, нередко связанной с военной тайной, или же информации, публичное разглашение которой может нанести имиджевый урон тому или иному государству, его институтам или отдельным политикам. Здесь наиболее заметными

игроками выступают сообщества *Anonimous* и *Wikileaks*, первое из которых носит сугубо анонимный характер, а второе можно квалифицировать как квазианонимное, поскольку его лидер Дж. Ассанж хорошо известен и находится в центре внимания мировых СМИ. Размышляя о роли киберсообществ, российский политолог П. А. Шариков отмечает: «Как представляется, в последнее время описываемая тенденция приобретает совершенно невероятные масштабы, апогеем этого явления на данный момент выступает история со скандальным сайтом Wikileaks. Сайт Wikileaks начал работать с января 2007 г., на нем уже публиковались различные разоблачения, однако инциденты с утечкой военного архива о войне в Афганистане летом 2010 г., а также дипломатической переписки осенью того же года сделали его знаменитым на весь мир» [Шариков 2011: 101]. Нельзя пройти мимо роли Дж. Ассанжа и его «детища» в предвыборной политической гонке в канун президентских выборов 2016 г., когда *Wikileaks* превратился в мощный инструмент дискредитации кандидата от Демократической партии Хиллари Клинтон. Из боязни разоблачений в октябре 2016 г. Дж. Ассанжу был даже заблокирован доступ в Интернет [Ecuador… 2016].

Здесь стоит сказать о феномене квазианонимности, которая активно реализуется сообществом *Wikileaks*. С одной стороны, участники кибервойны стремятся к анонимности с целью избежать ответственности (в частности, сайт Ассанжа проводит политику неразглашения своих источников), но, с другой, – в случае абсолютной неизвестности и анонимности может быть утрачен эффект «политического месседжа». Как иные группировки подчас принимают на себя ответственность за теракты лишь затем, чтобы донести до мирового сообщества свою политическую позицию, так и субъекты кибервойн лишь отчасти действуют в анонимном режиме.

Гибридной формой открытого и закрытого типов информационной борьбы выступают так называемые *сетевые войны*. В них элементы медиавойн и кибервойн сочетаются, базируясь на информационной платформе транснациональных социальных сетей. С одной стороны, через инфраструктуру таких платформ, как *Facebook* или *Twitter*, транслируются и внедряются в общественное мнение картины мира, создаваемые крупными массмедиа. С другой стороны, те же социальные сети служат удобным объектом для хакерских атак закрытого типа и несанкционированного получения конфиденциальной информации. Это позволяет говорить о гибридном (или синтетическом) характере сетевых войн. Весьма близким к понятию «сетевые войны» нам представляется термин «сетевая дипломатия», дефакто являющийся переводом предыдущего на язык политкорректности. В настоящее время США взяли на вооружение стратегию «сетевой дипломатии» в стремлении оказать внешнеполитическое воздействие на своих геополитических конкурентов в различных регионах мира [Алхименков 2014; Скаленко 2016].

Следует отличать понятие «сетевые войны» от концепции сетецентрической войны, характеризующей новый подход к пониманию трансформации самого феномена войны в современную эпоху. Сетецентрическая война заключается «в использовании информационно-коммуникационных технологий для перехода от операций, основанных на применении отдельных “платформ”, к операциям, проводимым в едином информационном пространстве» [Корсаков 2008: 95]. То есть

речь идет о фундаментальном переходе от парадигмы классической войны к парадигме войны неклассической. В контексте сетецентрического противостояния сетевые войны составляют отдельный фронт информационных действий, разворачивающихся в пространстве глобальных социальных сетей.

Социальные сети могут играть ключевую роль и в социально-политических процессах, что ярко продемонстрировал опыт корпорации *Facebook*, ставшей одним из решающих факторов «арабской весны» [Facebook… 2012]. Алгоритм сетевых войн может разворачиваться по разным сценариям, но обобщенно его можно свести к следующей схеме: вначале производится мощный информационный вброс в социальные сети со ссылкой на релевантный и вызывающий доверие источник; затем информация, распространяющаяся в режиме «снежного кома», становится реальным фактом и фактором политических процессов. В качестве иллюстрации можно привести следующий пример. В апреле 2013 г. со взломанного аккаунта сотрудников агентства *Associated Press* в социальные сети попала ложная информация о ранении Барака Обамы. Сетевое возбуждение достигло столь высокого градуса, что буквально через несколько часов эта информация привела к обрушению индекса Dow Jones [Попов 2013]. Именно социальные сети стали проводником этой псевдоинформации, придали ей статус правдивой и вызвали резонанс, реально отразившийся на состоянии мировой экономики.

Таким образом, можно заключить, что в современную «цифровую» эпоху информационные войны постепенно приобретают тенденцию к становлению доминирующей формой активации и протекания геополитических конфликтов. Спектр методов ведения информационных войн очень широк: от медиавойн при участии влиятельных корпораций массмедиа до прямолинейных кибератак и внедрения вирусов в компьютерные сети реального или предполагаемого противника. При этом информационные атаки нередко могут иметь непредвиденные последствия вплоть до глобальных. Особенно высоки риски в тех случаях, когда средством нападения становятся глобальные социальные сети. С ускорением процессов информационной глобализации, возможно, будут найдены и более изощренные методы ведения информационных войн, способные обеспечить анонимность и невидимость, а тем самым и безнаказанность их инициаторов. Нельзя исключать и того, что мир, погруженный в пучину геополитических конфликтов, находит в информационных войнах мирный выход накопившейся агрессии, опасаясь доводить конфликты до открытого вооруженного столкновения. Но чаще всего информационные войны становятся новым «цифровым» каналом трансляции этой агрессии, причем глобальные информационные технологии выступают в роли оружия нового типа.

### *Литература*

Алхименков М. А. Социальные сети и современная интернет-дипломатия США // США и Канада: экономика, политика, культура. 2014. № 11. С. 52–66.

Виноградова Е. А. Стратегическая коммуникация стран АЛБА на Ближнем Востоке: информационная война с Западом // Мир и политика. 2012. № 7(70).

Волков К. Америку достали хакеры // КОМПАС: Вестник международной аналитической информации. ИТАР-ТАСС. 2013. № 11.

Глобализация: Контуры XXI века: реф. сб. / под ред. Ю. Н. Игрицкого и др. М. : ИНИОН РАН, 2002.

Громыко Ю. Контрпропаганда запускает знаниевый проект. Эфир передачи «Смысл игры» на радио «Вести ФМ». 2016. 21 октября [Электронный ресурс]. URL: http://radiovesti.ru/episode/ show/episode_id/42006 (дата обращения: 10.11.2016).

Давыдов Ю. Понятие «жесткой» и «мягкой» силы в теории международных отношений // Международные процессы. 2004. Т. 2. № 1(4). С. 69–80.

Евдокимов Е. Политика Китая в глобальном информационном пространстве // Международные процессы. 2011. Т. 9. № 1(25). С. 74–83.

Жиров Ф. Китай – США: начало кибервойны? ИТАР-ТАСС. 2013. 6 марта [Электронный ресурс]. URL: http://tourpress.tv-telecom.ru/blog/9/288750 (дата обращения: 01.11.2016).

Корсаков Г. Б. Войны будущего в исследованиях американских авторов // США и Канада: экономика, политика, культура. 2008. № 6. С. 89–102.

Корсаков Г. Б. Роль информационного оружия в военно-политической стратегии США // США и Канада: экономика, политика, культура. 2012. № 1(505). С. 39–60.

Попов Е. Виртуальное покушение на Обаму подорвало веру в Интернет. 2013. [Электронный ресурс]. URL: http://www.vesti.ru/doc.html?id=1078900 (дата обращения: 02.11.2016).

Скаленко А. К. Глобальносистемный кризис трансинформационной цивилизации // Век глобализации. 2016. № 1–2 (17–18). С. 102–113.

Удовик С. Л. Глобализация: семиотические подходы. Киев : Ваклер, 2002.

Харитонова Е. Эффективность «мягкой силы»: проблема оценки // Мировая экономика и международные отношения. 2015. № 6. С. 48–58.

Шариков П. А. Герои информационной эпохи // Мир и политика. 2011. № 5(56). С. 97–103.

Шариков П. А. Российский вектор американской информационной политики // США и Канада : Экономика, Политика, Культура. 2015. № 9. С. 23–36.

Año de la ciberguerra? CNNMoney.com. 2013 [Электронный ресурс]. URL: http://cnnespanol.cnn.com/2013/01/08/2013-el-ano-de-una-ciberguerra-real/ (дата обращения: 29.10.2016).

Ecuador cuts off Internet Access for WikiLeaks Founder Julian Assange // The Washington Post. 2016. October 18 [Электронный ресурс]. URL: https://www.washingtonpost.com/world/ecuador-cuts-off-internet-access-for-wikileaks-founder-assange/2016/10/18/277281f6-95ac-11e6-9b7c-57290af48a49_story.html (дата обращения: 15.10.2016).

Facebook, trinchera de la primavera árabe // INFOBAE. 2012. URL: http://www.infobae.com/2012/02/05/1043363-facebook-trinchera-la-primavera-arabe/ (дата обращения: 01.11.2016).

Fuentes J. Guerra informática en Serbia // El Mundo. 1999. 16 abri [Электронный ресурс]. URL http://www. elmundo.es/navegante/99/abril/16/hackers.html (дата обращения: 28.10.2016).

Global Studies Encyclopedic Dictionary / Ed. by A. N. Chumakov, I. I. Mazour, W. C. Gay. With a Foreword by Mikhail Gorbachev. Amsterdam; New York, NY : Editions Rodopi B. V., 2014.

Google China Cyberattack Part of Vast Espionage Campaign Experts Say // The Washington Post. 2010. January 13 [Электронный ресурс]. URL: http://www.washingtonpost.com/wpdyn/content/article/2010/01/13/AR2010011300359.html (дата обращения: 25.10.2016).

Graham B. Hackers Attack Via Chinese Web Sites // The Washington Post. 2005. August 24 [Электронный ресурс]. URL: http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR200 5082402318.html (дата обращения: 01.11.2016).

Lynn III W. J. Defending a New Domain // Foreign Affairs. 2010. September/October [Электронный ресурс]. URL: http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-do main (дата обращения: 15.10.2016).

Nye J. Soft Power: The Means To Success In World Politics. New York, NY : Public Affairs, 2004.

Symantec. El gusano Stuxnet [Электронный ресурс]. URL: http://www.symantec.com/es/mx/theme.jsp?the meid=stuxnet (дата обращения: 19.10.2016).

Torres M. Los medios de comunicación globales y la acción exterior del Estado // La seguridad más allá del Estado. Madrid : Plaza & Valdés, 2011. Pp. 93–111.