УДК 328

АМЕРИКАНСКАЯ ШКОЛА ИССЛЕДОВАНИЙ ИНФОРМАЦИОННЫХ ВОЙН

М. С. Ермикова

Московский государственный университет им. М. В. Ломоносова,
Ленинские горы, 1, Москва, 119991, Россия

Анализируются обстоятельства трансформации форм войны в современном мире, выделяются признаки «старых войн», такие как переход на военные рельсы, мобилизация, милитаризация экономики, рост налогов для населения, дестабилизация политической системы, социально-психологический кризис в обществе, борьба за национально-политические интересы, приоритетность культурного единства, выращивание чувства чужеродности, агрессии и ненависти к иным культурам. Автор описывает «новые», или «гибридные», войны, главным отличием которых можно считать отсутствие объявления войны, т. е. целенаправленное игнорирование юридической процедуры в международном праве, заключающейся в официальном предупреждении одним государством другого о прекращении между ними мира и переходе к состоянию войны. В качестве других не менее важных характеристик можно отметить сочетание насильственных и ненасильственных средств ведения войны, т. е. использование различного вида вооружений, а также информационной войны и пропаганды. Автор рассматривает феномен информационных войн: возникновение термина в США и проблему его многозначности (“information warfare”), проводит анализ исследований по информационным войнам, которые были разделены на блоки в хронологическом порядке их разработки иностранными учеными и военными. Первый блок (начало 1990-х годов) — работы ученых Авиауниверситета ВВС США: Р. Шафрански, Дж. Стейна; второй блок (конец 1990-х годов) — исследования RAND Corporation: Дж. Аркиллы, Д. Ронфельдта, М. Либики; третий (2000-е годы) — монографии Дж. С. Най, М. Кэлдор, а также анализ системы «информационной диктатуры» Китая.

Ключевые слова: информационная война, новые войны, гибридные войны, старые войны, информационные технологии, мягкая сила, насильственные действия, невоенное противостояние.

Процессы глобализации и изменения конфигурации политических сил в международной сфере благодаря коммуникационным и информационным стратегиям обусловливают научный интерес к изучению информационных войн как одного из наиболее влиятельных мировых политических трендов нашего времени. В центре внимания оказываются вопросы функционирования институтов межгосударственной и межрегиональной областей политики, стратегий, форм и технологий их деятельности, реакции на изменения внешнеполитической среды. Напряженная международная обстановка, связанная с государственным переворотом на Украине, присоединением Крыма к России, самопровозглашением Донецка и Луганска независимыми республиками, взаимными санкциями России и Запада, войной в Сирии, взаимозависимостью

https://doi.org/10.21638/11701/spbu23.2018.110

современных государств в торгово-экономической, военно-политической, социально-гуманитарной (миграционной) сферах, достигла уровня, при котором стало необходимым регулирование отношений в этих областях.

В СМИ, в риторике политических лидеров, экспертов, исследованиях ученых можно столкнуться с такими категориями, как «гибридные войны», «асимметричные войны», «иррегулярные войны», «войны памяти», «информационные войны» и пр. У каждой из этих категорий существует множество определений, все они тесно переплетаются между собой.

Смешение понятий — только одна из существующих сложностей, но более важным представляется анализ тех аспектов военного и невоенного противостояния, которые в значительной мере меняют привычные представления об объеме насилия, ходе силового взаимодействия, масштабах и результатах конфликта. Одной из фундаментальных составляющих «гибридной войны» является информационная война.

Информационный аспект военных операций приобретает особую значимость и актуальность в условиях, когда первостепенное значение играет не только достижение конкретного боевого результата, но и легитимация данного события в глазах целевых аудиторий, к числу которых можно отнести население страны-мишени и страны-агрессора, мировую общественность, политические элиты сторон конфликта.

Благодаря информационным технологиям и манипулятивным приемам можно «превратить» агрессора в освободителя и борца за справедливость, принуждение к миру (peace-enforcement) представить как поддержание мира (peace-keeping).

Информационная война представляет собой одну из важнейших угроз для безопасности России, так как позволяет иностранным государствам достигать своих внешнеполитических целей без применения насильственных действий. Разработка концепций информационных войн и технологий военными иностранными ведомствами, их применение в локальных вооруженных конфликтах являются причинами, по которым России следует разрабатывать сдерживающие, противодействующие средства, методы и способы информационного оружия. Понимание стратегий информационной войны позволяет выявить объекты для защиты от информационных операций.

Прогнозируя развитие международной обстановки с учетом того, что с марта 2014 г. США в период внутриукраинского кризиса провозгласили курс на «системное сдерживание» России и в несколько этапов ввели санкции против российских физических и юридических лиц, а после выборов президента США в ноябре 2016 г. в Конгрессе и ФБР начались независимые расследования по поводу «вмешательства России» в эти выборы, важно изучить информационную и психологическую составляющую в современных межгосударственных конфликтах.

Цель статьи — определить характерные черты «старых» и «новых» войн, выяснить, что представляют собой «гибридная» и информационная войны, сформулировать определение информационной войны, проанализировать исследования в области информационных войн и определить особенности изучения данного феномена в США.

СТАРЫЕ И НОВЫЕ ВОЙНЫ

Смысл мира и войны формируется исходя из целей субъектов, ответственных за вступление в войну. Не так важно, какова причина участия в войне: защита и поддержка братского народа, агрессивная защита государственной целостности, помощь и обязательства по отношению к союзникам. Состояние войны обязывает корректировать привычную повестку дня, дозировать долю информационной агрессии, однако это не отменяет действий правительства, ответственного за формирование векторов развития общества и государства.

Но каковы индикаторы, позволяющие определить, что страна оказалась в состоянии войны? Еще недавно такой вопрос выглядел бы абсурдным, во всяком случае для европейской военной культуры. Война начиналась тогда, когда политическая элита объявляла о ней или внезапная атака давала отсчет военному времени. Характерными признаками «состояния войны» были переход на военные рельсы, мобилизация, милитаризация экономики, рост налогов для населения, уменьшение степени оппозиционности контрэлит и населения, рост патриотизма.

Для старых войн характерны разрушения в больших масштабах: политико-экономические и культурные потери, дестабилизация политической системы, социально-психологический кризис в обществе, борьба за национально-политические интересы, приоритетность культурного единства, выращивание чувства чужеродности, агрессии и ненависти к иным культурам.

В настоящее время можно столкнуться с менее очевидными характеристиками войны. Войны уже не всегда имеют начало и конец, государства и общества могут годами и десятилетиями жить в состоянии войны, причем другие международные политические акторы могут об этом не подозревать.

Новые войны в основном связывают с менее формальными факторами, которые сложно зафиксировать, статистически оформить. То есть мы будем иметь дело с ценностями, идеалами, культурными традициями, исторической памятью, информацией, восприятием информации. Все эти субъективные категории имеют принципиальное значение в любой войне, несмотря на исторический период, протяженность во времени и цели участников.

Предполагается, что целями новых войн выступают защита прав человека и гражданского населения, сохранение культурного многообразия, технологический прогресс, решение глобальных проблем, усовершенствование международного законодательства, строительство наднационального информационного поля (Калдор, 2015, с. 134). Все эти цели больше напоминают развитие цивилизации мирным путем, прогресс и т. п. Но, как и в любой войне, даже несмотря на то что эти войны «новые», невозможно обойтись без целей политического меньшинства, обладающего достаточным количеством ресурсов, чтобы военные действия проходили под эгидой миротворческих миссий для всего мира.

Некоторые исследователи определяют гибридную войну как военную стратегию, включающую традиционные методы ведения боевых действий и информационно-психологические технологии. Другая часть авторов считает, что гибридная война — это военные действия против внешнего противника

с использованием различного вида вооружений, а также информационной войны и пропаганды.

На настоящий момент литература по гибридным войнам немногочисленна. Большинство публикаций по новым и гибридным войнам представлено в журналах различных оборонных ведомств США, являющихся результатом исследований военных (см.: Smith, 2014). Англоязычная блогосфера по этой тематике посвящена главным образом событиям на Украине. Китайский сегмент Интернета о гибридных войнах в основном тоже связан с Украиной и военной стратегией США (см.: Dongsheng, 2010).

После холодной войны американские военные не могли точно охарактеризовать возникающие угрозы, так как они не подходили под уже существовавшие концепции. С начала в 2006 г. конфликта между Израилем и «Хезболлой» появляется термин «гибридные угрозы», который применяется для описания растущей сложности и нелинейности противостояния сторон.

Интерес США к гибридным формам войны рос и стал предметом обсуждений политических элит. Так, в 2010 г. появились два доклада: комиссии Конгресса США подкомитету по терроризму, нетрадиционным угрозам и потенциалам Комитета по делам вооруженных сил и Рэнд-Корпорэйшн. В первом говорится, что офицеры высшего командного состава использовали термин «гибридная война» для описания методов, применяемых в Ираке и Афганистане противниками США (см.: Sanchez, Miller, 2010). Цель подготовки доклада заключалась в том, чтобы выяснить, как Министерство обороны США определяет гибридную войну и чем она отличается от других типов войн, а также до каких пределов США собираются учитывать новую форму войны в своих военных доктринах и стратегическом планировании. Во втором докладе осмыслялись военные возможности гибридных войн на примере опыта, приобретенного израильской армией в Ливане (см.: Johnson, 2010).

Из академических исследований можно вспомнить работу «Гибридная война: боевой комплекс оппонентов от древнего мира до настоящего времени» под редакцией профессоров У. Муррея и П. Мансура (см.: Murray, 2012). Авторы считают, что гибридные войны существовали всегда, и только недавно были неправильно категорированы как уникальное явление. По их мнению, великие державы на протяжении всей истории сталкивались с конфронтацией своих врагов, которые использовали комбинацию регулярных и иррегулярных сил, чтобы свести на нет превосходство держав в обычной военной силе (см.: Ibid.).

Стратегии гибридных войн и рекомендации по противостоянию новым военным угрозам разрабатываются не только в США, но и в НАТО. В 2014 г. в итоговой декларации саммита НАТО впервые на высоком официальном уровне говорится о необходимости готовить альянс к участию в войнах нового типа — гибридных войнах. По мнению специалистов альянса, такие войны включают в себя проведение широкого спектра прямых боевых действий и тайных операций, осуществляемых вооруженными силами, партизанскими и иррегулярными формированиями при участии различных гражданских компонентов. В документе содержится требование налаживать тесную координацию между министерствами внутренних дел, привлекать силы полиции для обеспечения

безопасности от нетрадиционных угроз, связанных с информационными кампаниями, кибератаками и действиями сепаратистов (см.: Бартош, 2014).

Приведем примеры определений «гибридных войн и угроз», которые члены комиссии Конгресса США использовали в докладе (Sanchez, Miller, 2010, p. 17).

Гибридная война ведется либо государством, либо негосударством, представляющим угрозу, которые используют несколько режимов ведения войны, включающие обычные военные возможности, иррегулярную тактику и уголовные беспорядки (термин используется Объединенным командованием США, Объединенным центром оперативного анализа, взято из доклада «Совместная адаптация к гибридным войнам»).

Гибридная угроза исходит от противника, который одновременно использует комбинацию политических, военных, экономических, социальных и информационных средств и обычные иррегулярные, террористические и криминальные методы. Это может включать в себя комбинацию государственных и негосударственных субъектов (рабочее определение, полученное от Объединенного командования США и Объединенного центра иррегулярных войн США).

Гибридные угрозы включают в себя полный спектр различных способов ведения войны, включая обычные силы, иррегулярные тактики и формирования, террористические акты, в том числе неизбирательного насилия и принуждения, а также уголовные беспорядки, проводимые государственными и негосударственными акторами.

Что же касается информационных войн, то они значительно раньше оказались в фокусе внимания военных ведомств США и других государств.

ВОЗНИКНОВЕНИЕ ТЕРМИНА «ИНФОРМАЦИОННАЯ ВОЙНА» В США

Информационная война появилась как форма информационного противоборства, но вследствие научно-технического прогресса и расширения мирового информационного пространства стала самостоятельным видом осуществления внешней политики. Сильные в военном и информационно-техническом отношении государства приобрели новые возможности для достижения внешнеполитических целей: осуществлять несанкционированное вмешательство в работу компьютерных систем, анонимно поражать электронные вооружения противоборствующей стороны. Поэтому неслучайно в 1980-х годах американские и китайские теоретики и спецслужбы, в начале 1990-х годов — Министерство обороны США, в середине 1990-х годов — английские, немецкие, российские и другие исследователи начали активно формулировать определения информационной войны.

Толчком для обсуждения понятия «информационная война» послужило введение в оборот в документах Министерства обороны США в начале 1990-х годов термина “information warfare”, широко вошедшего вслед за этим в труды научных кругов США.

Важно отметить, что ранее, в 1976 г., уже появлялся близкий термин “information war”, употребленный западным ученым-физиком Т. Рейнером в отношении войн, основными объектами поражения в которых станут ин-

формационные системы. Однако специалисты США вместо этого термина, однозначно толкуемого как «информационная война», выбрали иной термин — “information warfare” (Манойло, 2003, с. 238).

Этот термин, наряду с переводом «информационная война» в соответствии с основными толковыми словарями “Webster’s New Collegiate Dictionary” и “The Random House Dictionary”, можно толковать следующим образом: «информационная деятельность, предпринимаемая политическим образованием (например, государством), чтобы ослабить или уничтожить другое политическое образование»; «информационная борьба между соревнующимися конкурентами» (см.: Webster’s New Collegiate Dictionary, 1978); «информационный военный конфликт между двумя массовыми врагами, например армиями»; «особенно жестокий и затяжной информационный конфликт между конкурентами, политическими соперниками» (см.: The Random House Dictionary, 1987).

Такое многозначное толкование термина “information warfare”, по мнению американских теоретиков, позволяет использовать средства и способы «жестокого» информационного противостояния не только в период боевых действий, но и в их отсутствие, «чтобы ослабить или уничтожить» политического или экономического противника законными с правовой точки зрения средствами и методами, так как “warfare” — не война в прямом смысле слова (см.: Szafranski, 1995).

В соответствии с российскими англо-русскими словарями термин “information warfare” трактуется как «информационная война» и «информационные приемы ведения войны» (Мюллер, 2012).

Многозначность термина “information warfare” породила разночтения при его переводах, что обусловило появление значительного количества существующих определений информационной войны.

В настоящее время термин «информационная война» все еще носит публицистический характер и пока не получил повсеместного признания в российских и зарубежных научных кругах, о чем свидетельствуют непрекращающиеся дискуссии по поводу того, в чем заключается сущность явлений, относимых к информационным войнам, а также споры по поводу корректности и применимости данного термина к конфликтам в сфере социальных взаимоотношений, которые принято называть информационным противоборством или конфликтами интересов в информационной сфере (Манойло, 2003, с. 204).

Российский специалист в области теории информационного противоборства доктор технических наук С. П. Расторгуев определяет информационную войну как «открытые и скрытые целенаправленные информационные воздействия информационных систем друг на друга с целью получения определенного выигрыша в материальной сфере» (Расторгуев, 1999, с. 35). По мнению С. П. Расторгуева, информационная война не отличается от обычной войны в части признаков поражения. Агрессор добивается победы в результате подчинения структур управления противника, которые являются информационной мишенью.

Отсюда, согласно С. П. Расторгуеву, следуют и основные направления организации защиты: уменьшение размера мишени; защита мишени; регулярное уничтожение «информационных сорняков»; установка собственного жесткого контроля над собственной системой управления.

Один из авторитетных специалистов в этой области В. С. Пирумов определяет информационную войну как новую форму борьбы двух и более сторон, которая состоит в целенаправленном использовании специальных средств и методов влияния на информационные ресурсы противника, а также защиты собственного информационного ресурса для достижения назначенных целей (Пирумов, 1997, с. 45). По его мнению, в мирное время информационная война носит преимущественно скрытый характер. В военный период появляются дополнительные задачи, решаемые в интересах обеспечения требуемой эффективности планируемых боевых действий. Средства информационной войны будут решать такие задачи, как массированное воздействие на информационный ресурс противника и предотвращение снижения боевых возможностей своих сил; проведение мероприятий по снижению уровня психологической устойчивости войск противника и обеспечение нейтрализации информации, воздействующей на психологическое состояние своего личного состава; ведение разведывательной деятельности и обеспечение скрытности важнейших мероприятий своих войск.

Доктор военных наук С. А. Комов определяет информационную войну в военное время как комплекс информационной поддержки, информационных контрмер, мер информационной защиты, предпринимаемых в соответствии с единым планом и нацеленных на достижение и поддержание информационного превосходства над противником во время боевых действий (Комов, 1996, с. 76). Ученый полагает, что для вооруженных сил понятие информационной войны имеет несколько основных аспектов: определение мер для получения информации о противнике, условиях боя, своих войсках; определение мер по блокированию процесса сбора информации противником о наших войсках; осуществление мероприятий по организации взаимодействия с другими воинскими контингентами, участвующими в конфликте.

Первые определения информационной войны специалисты Министерства обороны США дали в ряде документов (Директива МО США TS3600.I «Информационная война» от 21 декабря 1992 г.; Директива председателя КНШ МО США № 30 «Борьба с системами управления», 1993 г.) сразу после операции «Буря в пустыне» (1990–1991). В ходе этой операции США осуществляли целенаправленные действия против электронных информационных систем Ирака (Манойло, 2003, с. 242). В указанных документах информационная война рассматривается как особый вид военных действий, носящих манипулятивный, подрывающий или разрушающий характер. При этом первоначально в 1992 г. Министерство обороны США в качестве объектов поражения этого вида действий называло только «электронные информационные системы, обеспечивающие социальную, политическую, экономическую, индустриальную или военную сферы государства-противника».

Через год Комитет начальников штабов Министерства обороны США включил в число объектов поражения информацию и информационные системы противника в целом, независимо от того, являются они электронными или нет, тем самым добавил оборонительную составляющую информационной войны.

Обобщение военного опыта американской армии в области осуществления психологических операций и дезорганизации систем управления, приобретен-

ного в Панаме, Гренаде, на Гаити, в Сомали, привело к тому, что в 1995 г. в Армейский боевой устав Министерства обороны США «Информационные операции» к объектам поражения и защиты в информационной войне добавились процессы, базирующиеся на информации: психологические процессы человека, процессы принятия решений — автоматизированные и нет.

Все вместе разнообразные определения достаточно полно и однозначно, но пока только на прикладном уровне выделяют из многообразия существующих в современном обществе отношений те социальные явления и процессы, которые можно отнести к отдельной группе с условным названием «информационная война».

Подводя итог рассмотрению понятия информационной войны применительно к вооруженному противоборству, мы можем определить его следующим образом: информационная война — это комплекс мероприятий, насильственных и ненасильственных действий, информационных и политических технологий, используемый государством (и негосударственными акторами) с целью достижения информационного превосходства или господства над противником, а также в международном информационном поле при одновременном укреплении и защите собственной информационной системы.

ИССЛЕДОВАНИЯ В ОБЛАСТИ ИНФОРМАЦИОННЫХ ВОЙН

Автор разделил анализируемые исследования по информационным войнам по блокам в хронологическом порядке их разработки иностранными учеными и военными.

Первый блок: начало 1990-х годов — группа ученых Авиауниверситета ВВС США, изучая войны будущего, сформулировала требования к информационной войне, подчеркивая, что самым слабым местом на поле боя останется мозг солдата.

Второй блок: конец 1990-х годов — можно считать, что он полностью «сделан» Дж. Аркиллой, который первым фундаментально осветил проблемы информационной стратегии, кибервойны и сетевой войны, а также информационной войны.

Третий блок: 2000-е годы — следует отметить исследования ученых, изучающих новые формы войны, новые способы распространения силы и влияния: Дж. С. Ная, М. Кэлдор, а также реальные проекты государств по контролю информационного поля и информационной безопасности, в частности систему «информационной диктатуры» Китая.

В качестве отправной точки по формированию теории информационных войн принято считать 1976 г., когда советник по науке Министерства обороны США и Белого дома Т. Рона впервые заговорил об информационной войне в своем отчете «Системы оружия и информационная война», подготовленном для компании «Боинг» (см: Rona, 1976). В своем тексте он останавливался на таком аспекте, как важность информационных потоков для действий противника, анализируя внутренние и внешние информационные потоки. Рона, в частности, указал, что информационная инфраструктура становится ключевым компонен-

том американской экономики, но она одновременно превращается в уязвимую цель как в военное, так и в мирное время.

Т. Рона впервые акцентировал внимание на тех аспектах, которые сегодня легли в основу информационной войны: увеличение объема собственной информации, затруднение для противника доступа к правдивой информации, размещение в информационных потоках противника кажущейся достоверной, но фиктивной информации.

Воздействие на информационные потоки противника может привести, по его мнению, к следующим результатам. Во-первых, противник может прийти к осознанию неадекватности своих знаний, а благодаря этой неопределенности воздержится от агрессивных действий. Во-вторых, понимая свое незнание, противник распределит свои ресурсы, чтобы закрыть все возможные действия другой стороны, тем самым будут ослаблены шансы на победу.

Публикация отчета Т. Рона послужила началом активной кампании в СМИ. Сама постановка проблемы весьма заинтересовала тех американских специалистов, которые занимаются «секретными материалами». Военно-воздушные силы США начали активно обсуждать этот предмет с 1980 г. К тому времени сложилось общее представление о том, что информация может быть как целью, так и оружием.

Однако следует отметить, что подобные положения в классической военной теории уже были известны благодаря работам Сунь-Цзы «Искусство войны» и К. фон Клаузевица «О войне». «Искусство войны» Сунь-Цзы — древнейший военный трактат Китая, состоящий из 13 глав. Его главный смысл заключается в следующем: вступление в войну — очень ответственное решение для государства и потому должно быть взвешенным; война должна быть короткой, с минимальными потерями; «покорить войско противника, не сражаясь» — разбить замыслы противника, знать сильные и слабые стороны, использовать психологические приемы, организовать сильную разведку (см.: Сунь-Цзы, 2015). Все это подразумевает приоритетное использование ненасильственных методов ведения войны, управление информационным полем.

К. фон Клаузевиц — теоретик военных наук, заложивший основу военного стратегического мышления в течение XIX–XX вв. Клаузевиц начал писать свой трактат «О войне» в 1816 г., спустя год после окончания Наполеоновских войн, в которых он участвовал на проигравшей стороне, побывал в плену, и пережитое им оказало на книгу глубокое влияние (см.: Клаузевиц, 2009).

В трактате «О войне» представлены концепция «абсолютной войны», теория войны на истощение и теория маневренной войны. Теория войны на истощение подразумевает, что победа достигается изматыванием врага, максимизацией его издержек и потерь. Обычно она связана с высокой степенью концентрации ресурсов и оборонной стратегией. Теория же маневренной войны опирается на факторы внезапности и упреждения, создания неопределенности. Самый примечательный вывод трактата «О войне» состоит в признании двух фундаментальных положений: использовании подавляющей силы и готовности применить силу, предполагающую сочетания физических и моральных факторов.

Возвращаясь к исследованиям Т. Рона, можно сказать, что его предложения были основаны на классической военной теории, но переформатированы под новые требования времени, а именно развитие информационного пространства и переосмысление классической военной теории в XXI в.

ИССЛЕДОВАНИЯ УЧЕНЫМИ АВИАУНИВЕРСИТЕТА ВВС США ИНФОРМАЦИОННЫХ ВОЙН В НАЧАЛЕ 1990-х ГОДОВ

Р. Шафрански — один из первых исследователей, внесших вклад в формирование теории информационных войн. В своих работах он постулирует необходимость разработки теории информационных войн в более широком контексте ведения войны, т. е. предлагает вести ее на стратегическом и оперативном уровнях (см.: Szafranski, 1995). Решения, касающиеся разработки информационного оружия или преследования в судебном порядке попыток развернуть информационную войну, должны четко осознаваться правительственными институтами.

Эти решения должны быть приняты сознательно и преднамеренно, с пониманием моральных и этических рисков информационной войны. После оценки всех рисков и принятия решения о создании информационного оружия или участия в информационной войне лица, отвечающие за эти решения, должны в первую очередь иметь понимание этого оружия и теории применения оружия прежде, чем такая война начнется, а не после того, как оружие развернуто или уже использовано.

Информационная война имеет конечной целью использование информационного оружия, чтобы повлиять (воздействовать, манипулировать) на знания и систему верований внешнего противника.

Системы знаний — это системы, организованные и управляемые для того, чтобы понимать или замечать проверяемые феноменологические индикаторы и обозначения, переводить эти показатели в осознаваемую действительность, использовать эти представления для принятия решений и прямых действий.

В отличие от систем знаний, системы верований весьма индивидуальны, потому что включают в себя обширный пласт бессознательных и подсознательных элементов, о которых сам носитель может не догадываться. Несмотря на это, целью информационной войны является разум руководства противника, хотя противник представляет собой «множество умов», что лишь немного усложняет задачу.

Р. Шафрански убежден, что к 2020 г. более половины людей на планете будут жить в городских комплексах, а значит, будут использовать информационные технологии, благодаря чему можно будет воздействовать на множество разумов одновременно. Тем не менее цель войны — покорить враждебную волю лидеров и лиц, принимающих решения (см.: Szafranski, 1997).

В 1995 г. выходит работа Дж. Стейна «Информационная война», в которой в центре внимания снова оказывается разум: информационная война — это война о том, как люди думают и принимают решения (см.: Stein, 1995).

В широком смысле, по определению Дж. Стейна, война представляет собой просто использование информации для достижения целей государства. Как

и дипломатия, экономическая конкуренция или использование военной силы, информация сама по себе, один из ключевых аспектов власти и, что более важно, национальный ресурс, который как раз и поддерживает дипломатию, экономическую конкуренцию и эффективность вооруженных сил.

И наконец, информационная война может быть пространством, в котором проводятся иные, чем традиционные, военные действия, что может позволить Соединенным Штатам добиться некоторых важных целей национальной безопасности без необходимости расположения военных баз в каждом уголке планеты. Информационная война может определить будущую войну или быть в центре внимания для осмысления состоявшегося конфликта.

Дж. Стейн и Р. Шафрански своими исследованиями стремились показать, какие угрозы могут ждать США, если руководство страны не будет развивать стратегию информационной войны. Даже несмотря на отсутствие этой стратегии, нерешенные вопросы реорганизации, переобучения и переоборудования, американским властям необходимо осознавать насущную потребность в разработке концепции, которая производит стратегию. Именно информационная стратегия будет определять технологии, организационные изменения и новые концепции военных операций.

ИССЛЕДОВАНИЯ RAND CORPORATION ИНФОРМАЦИОННЫХ ВОЙН В КОНЦЕ 1990-х ГОДОВ

Еще одним источником новых концепций стала корпорация RAND Corporation. В тот момент в корпорации работали Дж. Аркилла и его соавтор Д. Ронфельдт. Дж. Аркиллу привлекали к консультациям Пентагона во время всех больших операций. Он практически первым привлек внимание как к кибервойне, так и к сетевой войне. Соответственно, он смог реинтерпретировать использование этих новых феноменов под нужды военных.

В этой связи обоснованным будет вспомнить классическую работу современного теоретика постмодерна Ж. Бодрийяра «Дух терроризма. Войны в заливе не было», посвященную войне в Персидском заливе в 1990–1991 гг. между многонациональными силами во главе с США и Ираком за освобождение и восстановление независимости Кувейта (см.: Бодрийяр, 2016). По мнению Ж. Бодрийяра, война в Персидском заливе была, но то, как действовали стороны конфликта, как освещалась их деятельность, не имело ничего общего с реальным положением дел. Новшеством этой войны было то, что все события транслировались ведущими телеканалами мира буквально в прямом эфире, повестку дня составляли лишь новости, комментарии, репортажи, выступления аналитиков и экспертов о войне в заливе.

Первая война в Ираке представляла собой протоверсию сетецентрической войны, принцип которой является одним из ключевых в военной реформе Пентагона с 1990-х годов. Согласно этому принципу, командование, а также каждая часть на поле боя, каждый танк и даже каждый солдат будут объединены в одну информационную сеть, будут обмениваться информацией, получать все необходимые сведения о противнике, что должно повысить боеспособность как всей армии, так и каждого ее компонента.

После распада СССР в 1991 г. одной из главных целей США стало поддержание своего статуса сверхдержавы и военного превосходства, а значит, недопущение появления равноценного соперника. Благодаря успешной реализации данной стратегии США по объему «мягкой силы» также стали иметь преимущество по сравнению с большинством других стран. Такое положение вещей позволило США вести масштабные войны на периферии без серьезного сопротивления в идеологической сфере и тем самым добиваться полного либо подавляющего контроля над интерпретацией этих войн в информационном пространстве.

Возвращаясь к научному обоснованию политических действий США в мировой политике, следует отметить, что в 1999 г. Дж. Аркилла и Д. Ронфельдт выступили с исследованием по американской военной стратегии и предложили отказаться от стратегии открытости, которая хоть и помогла, по их мнению, развалить Советский Союз, но позже оказалась не нужна. Новый подход, ограничивающий открытость, они обозначили как «охраняемая открытость» (см.: Arquilla, Ronfeldt, 1999).

Ряд прорывных работ Дж. Аркилла и Д. Ронфельдт сделали в сфере информационной войны. В своей известной статье о начале эры кибервойны они подчеркивают, что сегодня побеждает не тот, кто вложит больше капитала, труда или технологий, а тот, кто имеет лучшую информацию о поле боя.

Исследователи были убеждены, что информационная революция будет иметь большое влияние на военно-организационные формы и боевые учения. Ключ к пониманию этих изменений, как они полагали, можно найти в кибернетике. Их мнение заключалось в том, что информационное преимущество, если его умело использовать, позволит более мелким единицам победить более крупные, что и представляло собой сетевой подход.

В книге о роении как способе атаки противника авторы подчеркивают: то, как люди воюют, зависит не только от технологий (см.: Arquilla, Ronfeldt, 2005). Информационная революция изменила организационный дизайн атакующих единиц. Дж. Аркилла и Д. Ронфельдт выделяют четыре варианта атаки: схватка как бой лицом к лицу, массирование, маневрирование и роение. Масса, к примеру, является важной и для маневра, и в решающей точке. Информационное объединение позволяет победить противника, который будет думать, что это простая схватка, хотя на самом деле это было роением. Роение характеризуется следующими характеристиками: автономные или полуавтономные единицы, аморфный, но координируемый удар по всем направлениям, постоянное использование силы или огня, множество разбросанных, имеющих интернет-связь маневренных единиц, общее наблюдение и координация на самом верху, направление атак на разрушение единства противника.

Оборотной стороной этой точки зрения стала уязвимость информационных систем, в частности основанных на киберпространстве: они стали более восприимчивы к разрушительным кибервторжениям (см.: Arquilla, Ronfeldt, 1997).

Лучший способ изобразить спектр кибервойн — это сгруппировать эти конфликты по типу. Есть три основных области: военная, включающая вооруженные

силы и столкновения; социальная, в которой идеи используются для мотивации действий; и экономическая, где целями являются инфраструктура, коммерция и интеллектуальная собственность. Эти категории могут пересекаться.

В целом все три измерения кибервойны имеют множество проблем. Вооруженным силам еще только предстоит актуализировать весь потенциал кибервойны, но террористы уже продемонстрировали свое мастерство в социальной сфере. Некоторые страны уже ведут экономические киберкампании, нанося серьезный ущерб соперникам — увеличение расходов, понесенных в связи с постоянно растущей проблемой киберпреступности (см.: Arquilla, 2011). По мнению Дж. Аркиллы, нет сомнений, что кибервойна будет существовать и дальше во всех трех формах. В связи с этим первостепенной задачей для американских лидеров становится нахождение способов по урегулированию конфликтов в указанных областях.

Другой исследователь из RAND, математик и экономист М. Либики считал, что информационной войны как отдельной техники ведения войны не существует. Вместо этого есть несколько различных форм информационной войны, каждая из которых претендует на более широкую концепцию (см.: Libicki, 2007). Он выделил семь форм информационной войны, связанных с защитой, манипуляцией, деградацией и отрицанием информации:

1) командно-контрольная война (физическое воздействие на соперника);
2) разведывательная война (состоящая из проектирования систем, которые стремятся получить знания и информацию для доминирования на поле боя, защиты от них и их воспрещения);
3) электронная война (радиоэлектронная или криптографическая техника);
4) психологическая война (в которой информация используется для изменения умов друзей, нейтралов и противников);
5) «хакерская» война (в которой атакуются компьютерные системы);
6) экономическая информационная война (блокирование информации для достижения экономического доминирования);
7) кибервойна.

М. Либики в своей работе задает главный вопрос — является ли информационная война борьбой за контроль над информационным пространством битвы? Имеет ли первостепенное значение доминирование в информационной сфере в качестве цели, наподобие морского превосходства, превосходства в воздухе или территориального контроля? М. Либики делает следующие выводы.

Во-первых, доля происходящих информационных войн намного меньше, чем кажется на первый взгляд. Хотя информационные системы становятся все более значимыми, они также оказываются все более разбросанными, расфокусированными, лишь целенаправленные, структурированные действия могут обеспечить целостность информационных сообщений. Если в конфликте одной стороне четко ясны логика и закономерность деятельности правительственных структур другой стороны (соперника), то ее легко можно победить, заполняя информационную систему дополнительной информацией, с которой она не сможет справиться.

Во-вторых, США в информационной войне больше способны к защите собственной системы, нежели к наступлению на другие информационные системы, которые по своей природе представляются более закрытыми и сложными для воздействия.

ИССЛЕДОВАНИЯ НОВЫХ ВОЙН В 2000-х ГОДАХ

Поворотным моментом в осмыслении информационных войн стало признание, что сами войны, в рамках которых ранее выделяли информационный аспект, приняли совершенно иной облик. Мир столкнулся с новыми формами войны, и чтобы эффективно решать политические задачи, нужно научиться работать с поствойнами. Что такое новые войны и новы ли они?

В ряду исследователей, продвигающих мнение о новых формах войны, находится Джозеф Най, известный, помимо прочего, своей концепцией «мягкой силы» (см.: Най, 2014). Смысл концепции заключается в том, что «твердая сила», представляющая собой весь спектр принудительных ресурсов, начиная от военной области и заканчивая финансово-экономической, перестала быть настолько эффективной, чтобы не нуждаться в развитии каких-то новых государственных стратегий. В силу меняющихся условий, связанных с глобализацией и информационной революцией, наиболее адекватным становится распространение «мягкой силы» государства. «Классические войны перестали быть главным способом достижения политических целей, они преобразовались и стали гибридными, представляя собой “войны четвертого поколения”, в которых иногда не существует четких границ сражений, исчезают отличия между гражданским и военным» (Там же, с. 73). В гибридных войнах участвуют не только государства, но и негосударственные игроки: повстанцы, террористы, боевики, криминальные организации, которые рассматривают любой политический конфликт как ожесточенные операции нерегулярных вооруженных формирований, проводимые в течение длительного срока и позволяющие им устанавливать принудительный контроль над местным населением.

По убеждению Дж. Ная, в ходе гибридных войн такие понятия, как «военнослужащие» и «гражданские», «обычные» и «нерегулярные войска», «физическое уничтожение» и «информационная война», смешиваются. Информационные войны становятся реальностью, с которой общество сталкивается ежедневно, чему способствует наличие у каждого человека мобильного телефона с фотокамерой и компьютера с графическим редактором вроде Photoshop.

На настоящий момент власть над информацией распространяется гораздо шире, чем это было несколько десятилетий назад. В отличие от СМИ (радио, телевидение, газеты), находящихся под контролем издателей, Интернет все еще, несмотря на попытки правительств ввести механизмы контроля, дает возможность неограниченного общения между пользователями. Информация становится ключевым ресурсом силы, все большее количество людей получают доступ к этому ресурсу, а значит, политика больше не является прерогативой лишь правительств. Информационная революция объективно ведет к трансформации силы, ее размыванию, однако более крупные государства

по-прежнему будут иметь больше ресурсов для войны, информационной войны, для мягкой силы. Фундаментальными элементами мягкой силы являются культура, политические ценности, внешняя политика. Трансляция мягкой силы одного государства другим, всему мировому сообществу происходит с помощью информации, именно здесь открываются новые возможности информационных войн, которые, помимо деструктивных целей, могут решать совершенно иные вопросы: нахождение путей сочетания ресурсов в успешную государственную стратегию в новой обстановке «распыления силы» и «подъема остальных» политических акторов (Най, 2014, с. 278).

Дж. Най выдвигает концепцию «умной силы», которая объединяет твердую и мягкую силу, т. е. использование насильственных методов, например в борьбе с террористами, но мягкую силу — для привлечения и завоевания доверия массы мусульман. США должны руководствоваться представлениями о пределах американской силы, применять насильственные или ненасильственные методы в зависимости от ситуации. Там, где речь идет об аксиологической стороне политики (распространение американских ценностей), прагматичнее использовать мягкую силу, т. е. убеждение, влияние, манипулирование, стимулирование. Там, где задействованы интересы национальной безопасности, следует прибегать к «твердой силе», что предполагает военные действия, представляемые в качестве миротворческих операций или принуждения к миру.

Для Палаты лордов Институт бихевиористской динамики подготовил анализ возможностей применения мягкой силы для продвижения Британии (см.: Wein, Berg). Авторы исследования Т. Вайн и Г. Берг считают, что мягкая сила может быть эффективной, но это происходит достаточно редко.

Во-первых, мягкая сила слишком сфокусирована на коммуникации. Традиционный маркетинг крайне неэффективен в некоммерческом секторе.

Во-вторых, недостатки концепции мягкой силы заключаются в отсутствии сосредоточения внимания на цели, целевых задачах, выборе целевой аудитории, стремления к согласованности в отношении целевых групп.

В-третьих, требуется экспертная оценка, которую в настоящее время только пытаются обеспечить.

По мнению Т. Вайна и Г. Берга, общей ошибкой всех американских информационных кампаний является акцент на изменении отношений, а не поведения. В этом ошибка и традиционного маркетинга. С точки зрения британских ученых, изменив отношение, можно получить реальные изменения в поведении (Wein, Berg, p. 16).

В заключение следует отметить, что эффективная мягкая сила является сложным, техническим процессом, требующим детального понимания методов исследования и результатов социальной психологии, а также значительной гибкости для достижения целей в сложных политических условиях. Поэтому часто требуется экспертная оценка и следует иметь в виду, что многие так называемые специалисты в области коммуникации в частном и государственном секторах также испытывают недостаток в подобном опыте и совершают многие из перечисленных ошибок.

Британская исследовательница М. Калдор в своей работе «Новые и старые войны. Организованное насилие в глобальную эпоху» представляет мнение, согласно которому в настоящий момент существуют две точки зрения на войну: оптимистическая и пессимистическая (см.: Калдор, 2015). Оптимистическая точка зрения подразумевает, что произошло устаревание войны, т. е. появились новые войны, а армии, военно-воздушные силы не более чем ритуальные символы, свидетельствующие о снижающейся роли национального государства. Оптимизм заключается в том, что, по мнению автора, появляется все больше возможностей для установления «вечного мира» — это глобализация и развитие космополитической парадигмы управления.

Пессимистическая точка зрения заключается в том, что войну можно «переизобрести». То есть хотя форма война и изменится, она останется таким же разрушительным явлением, каким была многие столетия. И несмотря на то что способность национальных государств продуцировать «справедливое насилие» стала значительно сокращаться, общества стали сталкиваться со случаями низкоуровневого насилия, т. е. новые войны ведутся не только государствами, но и террористическими группировками, любыми силами, способными организовать насилие при помощи различных средств, в первую очередь информационных технологий.

Несмотря на противоположность приведенных точек зрения, по мнению М. Калдор, существуют подлинно новые элементы, которые характеризуют новые войны, порожденные глобализационными процессами и развитием технологий.

М. Калдор отмечает, что в симметричной войне, т. е. в войне между равнозначными противниками, одинаково обеспеченными военной техникой, практически невозможно победить. Военные технологии стали обладать большей разрушительной силой, а также доступностью. Такая война несет лишь экономические и физические потери.

Помимо развития военных технологий, имеется целый ряд эффектов, с которыми приходится сталкиваться вследствие появления новых форм коммуникаций: информационные технологии, телевидение и радио, Интернет, скрытые сети Интернета, дешевые авиаперелеты. Все эти новые средства помогают еще эффективнее, т. е. быстрее и менее затратно, мобилизовать сторонников вокруг своих целей. При этом сами средства сообщения все больше оказываются орудием войны, позволяя распространять страх и панику мгновенно. Как, например, террористы, организовавшие теракт, могут выпустить видеообращение с предупреждающими угрозами и выложить его в Интернете или же потерпевшие, наблюдатели имеют возможность написать о происходящем в своем интернет-аккаунте, что тут же окажутся в поле зрения подписчиков, а значит, «новость» будет распространяться намного стремительнее, чем телевизионный репортаж по официальным федеральным каналам.

Что же происходит с государствами в новых условиях? М. Калдор приходит к заключению, что государства в традиционном смысле не исчезают, а трансформируются: самые важные изменения касаются роли государства в отношении организованного насилия. Монополия на насилие претерпевает изменения

«сверху», что связано с обязательствами членства в международных организациях, международными институтами и правилами. Также можно отметить тенденции «снизу»: криминальные группировки, террористические организации благодаря информационной революции могут противостоять государствам в их когда-то исключительном праве на насилие. Свои качественные данные исследователь подтверждает количественными показателями, основными источниками которых являются Уппсальская программа данных о конфликтах, которую используют ежегодник Стокгольмского международного института исследований проблем мира (СИПРИ), проект "Human Security Report" (Доклад о безопасности человека) и Всемирный банк; проект «Корреляты войны» в Мичиганском университете; выходящий раз в два года обзор "Peace and Conflict Survey", выпускаемый Центром международного развития и управления конфликтами в Университете Мэриленда (Калдор, 2015, с. 391).

Вышесказанное касается ведения информационной войны между политическими акторами: государствами, международными организациями, негосударственными участниками, террористическими группировками.

Совершенно другой подход к проблеме информации в современном обществе принадлежит китайским исследователям и политической элите Китая, стремящимся при помощи современных технологий обеспечить тотальный контроль над информационными потоками внутри самого общества, гражданского населения страны, а конкретнее, построить «цифровую диктатуру» (Ковачич, 2017).

В Китае с приходом к власти Си Цзиньпина Госсовет КНР в 2014 г. опубликовал новый документ — «Программу создания системы социального кредита (2014–2020)». Система социального доверия представляет собой процесс оценивания деятельности компаний и жителей Китая, позволяющий каждому физическому лицу создать индивидуальный рейтинг, который будет публиковаться в централизованной базе данных в Интернете в свободном доступе. Граждане с высоким рейтингом смогут пользоваться благами во всех сферах жизнедеятельности общества, например поддержкой и преференциями в образовании, трудоустройстве, открытии бизнеса, социальных гарантиях. Граждане с низкими показателями столкнутся с различными ограничениями и санкциями, начиная от штрафов, административных санкций и заканчивая ограничениями в покупке недвижимости, авиабилетов, билетов на высокоскоростные поезда, выезда за границу и проживания в отелях класса «люкс». Критерии оценки представляются вполне конкретными и ясными, они будут заложены в соответствующие программы, т. е. будут оцениваться автоматически, а значит, «исключений», «неоднозначных» ситуаций для программного обеспечения не будет, только зачисление или снятие баллов. Очевидно, что с недостатками автоматизированного подхода столкнутся миллионы китайских граждан.

Кто будет задавать параметры системы доверия? Насколько правомерно использование компаниями личных данных клиента в пользу третьей стороны, которой в данном случае является государство? Все эти вопросы пока остаются юридически не обоснованными.

ЗАКЛЮЧЕНИЕ

В качестве выводов можно отметить, что война сегодня представляет собой сочетание военных и невоенных средств противоборства. Это широкая совокупность различных феноменов, объединенных государством для достижения своих целей в условиях глобализации и развития информационных технологий. Трансформация форм войны позволяет надеяться, что смысл военных действий кардинально изменился благодаря возможностям, предоставленным информационной революцией, способствующей размыванию монополии на насилие. Это утверждение может быть подкреплено следующими заключениями, основанными на количественных данных Уппсальского университета о конфликтах (см.: Melander) и Центра международного развития и управления конфликтами Университета Мэриленда (Center for International Development): фактическое исчезновение войн между государствами; спад войн высокой интенсивности, в которых боевые потери превышают тысячу человек в год; спад смертоносности войны, измеряемой в единицах боевых потерь; увеличение продолжительности и/или рост количества рецидивов войн; территориальная близость к другим войнам как фактор риска.

Между тем новые формы войны несут множество опасностей. В первую очередь усиленное воздействие на консциентальный уровень общества, т. е. на его массовое сознание, ценности, глубинные установки, историческую память.

Гибридные войны представляют собой обоюдные действия, общую заинтересованность воюющих сторон в предприятии войны, у которой нет окончания. Такие войны способствуют воспроизведению политической идентичности и достижению экономических целей.

Информационная же война из компонента войны, в котором военных и ученых интересовала лишь сторона воздействия на разум солдата и на лиц, принимающих решения, стала равноправным партнером военных действий, более того, информация выступает как основа любой системы, структурирующая процессы действительности. Развитие технологий и средств связи позволило иначе взглянуть на информационное поле: информационная стратегия стала неотъемлемой частью политической стратегии целых государств, а значит, информация стала решать проблемы тактического характера в условиях мирного времени.

Американские исследователи информационных войн стремились предугадать, каким образом информация будет влиять на ведение войны в будущем, а значит, сделать из США лидера в области коммуникаций и информационных технологий, как это было, по мнению американцев, с военно-воздушными силами, военно-морским флотом и т. п. В качестве еще одной особенности можно отметить особое внимание исследователей к проблеме принятия решений и к лицам, принимающим решения.

Следует сделать вывод о соотношении новых войн и информационных. Информационная революция, информационные технологии сделали новые войны возможными. Новые войны — это результат тенденций современного мира: глобализационных процессов, изменившейся роли национальных государств, появления новых политических акторов в международной политике, распро-

странения ненасильственных способов решения военных конфликтов, развития технологий, а равно неспособности технологий старых войн решать задачи современных демократических государств.

Запущен механизм переосмысления существующих форм войны, анализ преимуществ и недостатков старых и новых войн: предпринимаются попытки классификации войн «четвертого поколения».

В научный дискурс проникли вопросы, касающиеся столкновения проблемы информационной войны и социальной практики, когда информационная (цифровая, технологическая) война начинает разворачиваться внутри общества, против самого общества, превращая свободу информации из постулатов современного демократического общества постиндустриальной эпохи в инструмент закрепощения граждан и самих политических элит, и, как следствие, ведет к формированию нового тоталитаризма.

Литература

Бартош А. А. Гибридные войны в стратегии США и НАТО // Независимое военное обозрение. 10.10.2014. URL: http://nvo.ng.ru/concepts/2014-10-10/1_nato.html (дата обращения: 03.04.2015).

Бодрийяр Ж. Дух терроризма. Войны в заливе не было. М.: Рипол-Классик, 2016. 224 с.

Калдор М. Новые и старые войны. Организованное насилие в глобальную эпоху. М.: Институт Гайдара, 2015. 416 с.

Клаузевиц К. О войне. М.: Римис, 2009. 400 с.

Ковачич Л. Большой брат 2.0. Как Китай строит цифровую диктатуру // Московский центр Карнеги. 18.07.2017. URL: http://carnegie.ru/commentary/71546 (дата обращения: 13.11.2017).

Комов С. А. Информационная борьба в современной войне: вопросы теории // Военная мысль. 1996. № 3. С. 76–80.

Манойло А. В. Государственная информационная политика в особых условиях. М.: МИФИ, 2003. 388 с.

Мюллер В. Новый англо-русский, русско-английский словарь. М.: Эксмо, 2012. 880 с.

Най Дж. Будущее власти: как стратегия умной силы меняет XXI век. М.: АСТ, 2014. 444 с.

Пирумов В. С., Родионов М. А. Некоторые аспекты информационной борьбы в военных конфликтах // Военная мысль. 1997. № 5. С. 24–47.

Расторгуев С. П. Информационная война. М.: Радио и связь, 1999. 416 с.

Сунь-Цзы. Искусство войны. М.: Эксмо, 2015. 452 с.

Arquilla J., Ronfeldt D. Cyberwar is coming // In Athena's camp. Preparing for conflict in the information age. Santa-Monica: RAND, 1997. 60 p.

Arquilla J., Ronfeldt D. The emergence of noopolitik. Toward an American information strategy. Santa Monica: RAND, 1999. 352 p.

Arquilla J., Ronfeldt D. Swarming and the future of conflict. Santa Monica: RAND, 2005. 98 p.

Arquilla J. Insurgents, raiders, and bandits. How masters of irregular warfare have shaped our world. Chicago: Ivan. R. Dee, 2011. 311 p.

Center for International Development and Conflict Management. URL: https://cidcm.umd.edu/research/journal-conflict-resolution (дата обращения: 12.02.2018).

Dongsheng Xu. Meiguo xin fangwu baogao qiantiao hunhexin zhanzheng zhongdian fang Zhongguo // Sing Tao Global Network. 03.04.2010. URL: http://bjwljr.blog.hexun.com/51884198_d.html (дата обращения: 11.02.2018).

Johnson D. E. Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza. Prepared for the United States Army // RAND Army Research Division, 2010.

URL: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP285.pdf (дата обращения: 13.02.2018).

Libicki M. Conquest in cyberspace. National security and information warfare. Santa Monica: RAND, 2007. 307 p.

Murray W. Hybrid Warfare. Fighting Complex Opponents from the Ancient World to the Present. New York, Cambridge University Press, 2012. 309 p.

Melander E. Organized Violance in the World 2015. An assesment by the Uppsala Conflict Data Program. URL: https://www.pcr.uu.se/digitalAssets/654/c_654446-l_1-k_ucdp-paper-9.pdf (дата обращения: 10.02.2018).

Rona T. Weapon Systems and Information War. WA: Boeing Aerospace Co., 1976. 73 p.

Sanchez L., Miller J. Hybrid Warfare. Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Service, House of Representatives. United States Government Accountability Office // Homeland Security Digital Library. 10.09.2010. URL: https://www.hsdl.org/?abstract&did=7433 (дата обращения: 10.02.2018).

Szafranski R. Theory of Information Warfare. Preparing For 2020, USAF // Published Airpower Journal. 1995. Spring. URL: https://www.hsdl.org/?view&did=439843 (дата обращения: 10.02.2018).

Szafranski R. Neocortical warfare? The acme of skill // In Athena's camp. Preparing for conflict in the information age / ed. by J. Arquilla, D. Ronfeldt. Santa Monica: RAND, 1997. P. 41–55.

Smith M. Airpower in Hybrid Wars: Ethical implications for the joint force commander // Journal of national security studies. 2014. P. 106–115.

Stein G. Information warfare. AWC // The information warfare site. 1995. Spring. URL: http://iwar.org.uk/iwar/resources/airchronicles/stein.htm (дата обращения: 12.10.2017).

The Random House Dictionary of the English Language / ed. by S. B. Flexner. 2nd ed. New York: Random House, 1987. 2478 p.

Webster's New Collegiate Dictionary. US.: Merriam Webster, 1976. 1565 p.

Wein T., Berg G. Submission of evidence by the behavioral dynamics institute. URL: http://www.bdinstitute.org/wp-content/uploads/2014/01/BDI-Evidence-Submission.pdf (дата обращения: 13.01.2018).

Ермикова Мария Сергеевна — аспирант; ermikova@gmail.com

Статья поступила в редакцию: 22 января 2018 г.;

рекомендована в печать: 17 мая 2018 г.

Для цитирования: *Ермикова М. С.* Американская школа исследований информационных войн // Политическая экспертиза: ПОЛИТЭКС. 2018. Т. 14, № 1. С. 117–138. https://doi.org/10.21638/11701/spbu23.2018.110

AMERICAN SCHOOL OF INFORMATION WARS STUDIES

Maria S. Ermikova

Moscow State University named after M. V. Lomonosov,
Leninskie gory, 1, Moscow, 119991, Russia; ermikova@gmail.com

In the article the author analyzes the circumstances influencing the change in the form of war in the modern world, determines the features of the "old wars": transition to military service, mobilization, militarization of the economy, tax growth, destabilization of the political system, social-psychological crisis in society, political interests, priority cultural unity, the cultivation of allogeneity, aggression and hatred of other cultures. The author describes the wars of a "new kind" also known as "hybrid wars". The main differences of that kind of wars are the declaration of war absence, a purposeful course of international laws ignorance which consisting in the official warning by one state of another about the termination of the peace between them and the transition to a state of war. Equally, important features can be named as a combination of violent and non-violent

means of warfare, in other words, usage of different kinds of weapons, as well as information war and propaganda. The author considers the phenomenon of information wars: the emergence of the term in the United States and the problem of its ambiguity ("information warfare"), carry out a review of researches on information warfare, which was divided into blocks in its chronological order of invention of foreign scientists and military-grade. The first block (the early 1990's) — the work of scientists at the Air University of the United States Air Force: R. Shafransky, J. Stein; the second block (the late 1990s) — studies by RAND Corporation: J. Arquilla, D. Ronfeldt, M. Libika; the third (the 2000s) — the monographs of JS Nye, M. Keldor, as well as an analysis of the system of "information dictatorship" of China.

Keywords: information war, information warfare, a new war, old war, hybrid wars, information technologies, soft power, violent actions, non-military confrontation.

References

Arquilla J. *Insurgents, raiders, and bandits. How masters of irregular warfare have shaped our world*. Chicago, Ivan. R. Dee, 2011, 311 p.

Arquilla J., Davis P. K. *Modeling decisionmaking of potential proliferators as art of developing a counter proliferation strategies*. Santa Monica, RAND, 1994, 35 p.

Arquilla J., Ronfeldt D. *Cyberwar is coming. In Athena's camp. Preparing for conflict in the information age*. Santa-Monica, RAND, 1997, 60 p.

Arquilla J., Ronfeldt D. *Swarming and the future of conflict*. Santa Monica, RAND, 2005, 98 p.

Arquilla J., Ronfeldt D. *The emergence of noopolitik. Toward an American information strategy*. Santa Monica, RAND, 1999, 352 p.

Bartosh A. A. Gibridnye voiny v strategii SShA i NATO [Hybrid Wars in US and NATO Strategies]. *Nezavisimoe voennoe obozrenie* [*Independent Military Review*], 10.10.2014. Available at: http://nvo.ng.ru/concepts/2014-10-10/1_nato.html (accessed: 04.03.2015). (In Russian)

Bodriyyar Zh. *Dukh terrorizma. Voiny v zalive ne bylo* [*The spirit of terrorism. The Gulf War did not take place*]. Moscow, Ripol-Classic, 2016, 224 p. (In Russian)

Center for International Development and Conflict Management. Available at: https://cidcm.umd.edu/research/journal-conflict-resolution (accessed: 12.02.2018).

Dongsheng Xu. Meiguo xin fangwu baogao qiantiao hunhexin zhanzheng zhongdian fang Zhongguo. *Sing Tao Global Network*. 03.04.2010. Available at: http://bjwljr.blog.hexun.com/51884198_d.html (accessed: 11.02.2018).

Johnson D. E. Military Capabilities for Hybrid War. Insights from the Israel Defense Forces in Lebanon and Gaza. *Prepared for the United States Army. RAND Army Research Division*, 2010. Available at: https://www.rand.org/content/dam/rand/pubs/occasional_papers/2010/RAND_OP285.pdf (*accessed:* 13.02.2018).

Kaldor M. *Novye i starye voiny. Organizovannoe nasilie v global'nuiu epokhu* [*New and Old Wars. Organized violence in a global era*]. Moscow, Institute of Gaidar, 2015, 416 p. (In Russian)

Klauzevits K. *O voine* [*On war*]. Moscow, Rimis, 2009, 400 p. (In Russian)

Komov S. A. Informatsionnaia bor'ba v sovremennoi voine: voprosy teorii [Information warfare in modern war: theory issues]. *Voennaia mysl'* [*Military thought*], 1996, no. 3, pp. 76–80. (In Russian)

Kovachich L. Bol'shoi brat 2.0. Kak Kitai stroit tsifrovuiu diktaturu [The Big Brother 2.0. How China Builds a Digital Dictatorship]. *Moskovskii tsentr Karnegi* [*The Carnegie Moscow Center*], 18.07.2017. Available at: http://carnegie.ru/commentary/71546 (accessed: 13.11.2017). (In Russian)

Libicki M. *Conquest in cyberspace. National security and information warfare*. Santa Monica, RAND, 2007, 307 p.

Manoylo A. V. *Gosudarstvennaia informatsionnaia politika v osobykh usloviiakh* [*State information policy in special conditions*]. Moscow, MIPhI, 2003, 388 p. (In Russian)

Melander E. Organized Violence in the World 2015. *An assessment by the Uppsala Conflict Data Program*. Available at: https://www.pcr.uu.se/digitalAssets/654/c_654446-l_1-k_ucdp-paper-9.pdf (accessed: 10.02.2018).

Murray W. *Hybrid Warfare. Fighting Complex Opponents from the Ancient World to the Present*. New York, Cambridge University Press, 2012, 309 p.

Myuller V. *Novyi anglo-russkii, russko-angliiskii slovar'* [*New English-Russian, Russian-English dictionary*]. Moscow, EKSMO, 2012, 880 p. (In Russian)

Nay Dzh. *Budushchee vlasti: kak strategiia umnoi sily meniaet XXI vek* [*The Future of Power: How the strategy of clever force changes the 21st century*]. Moscow, AST, 2014, 444 p. (In Russian)

Pirumov V. S., Rodionov M. A. Nekotorye aspekty informatsionnoi bor'by v voennykh konfliktakh [Some aspects of information warfare in military conflicts]. *Voennaja mysl'* [*Military thought*], 1997, no. 5, pp. 24–47. (In Russian)

Rastorguev S. P. *Informatsionnaia voina* [*Information war*]. Moscow, Radio and Communication, 1999, 416 p. (In Russian)

Rona T. *Weapon Systems and Information War*. WA, Boeing Aerospace Co., 1976, 73 p.

Sanchez L., Miller J. Hybrid Warfare. Briefing to the Subcommittee on Terrorism, Unconventional Threats and Capabilities, Committee on Armed Service, House of Representatives. *United States Government Accountability Office. Homeland Security Digital Library*. 10.09.2010. Available at: https://www.hsdl.org/?abstract&did=7433 (accessed: 10.02.2018).

Smith M. Airpower in Hybrid Wars: Ethical implications for the joint force commander. *Journal of national security studies*, 2014, pp. 106–115.

Stein G. Information warfare. AWC. *The information warfare site*. 1995. Spring. Available at: http://iwar.org.uk/iwar/resources/airchronicles/stein.htm (accessed: 12.10.2017).

Sun-Tszyi. *Iskusstvo voiny* [*Art of War*]. Moscow, EKSMO, 2015, 452 p. (In Russian)

Szafranski R. Neocortical warfare? The acme of skill. *Athena's camp. Preparing for conflict in the information age*. Eds J. Arquilla, D. Ronfeldt. Santa Monica, RAND, 1997.

Szafranski R. Theory of Information Warfare. Preparing For 2020, USAF. *Published Airpower Journal,* 1995. Spring. Available at: https://www.hsdl.org/?view&did=439843 (accessed: 10.02.2018).

The Random House Dictionary of the English Language. Ed. by S. B. Flexner. 2nd ed. New York, Random House, 1987, 2478 p.

Webster's New Collegiate Dictionary. US.: Merriam Webster, 1976, 1565 p.

Wein T., Berg G. *Submission of evidence by the behavioral dynamics institute*. Available at: http://www.bdinstitute.org/wp-content/uploads/2014/01/BDI-Evidence-Submission.pdf (accessed: 13.01.2018).

For citation: Ermikova M. S. American school of information wars studies. *POLITEX: Political Expertise.* 2018, vol. 14, no. 1, pp. 117–138. https://doi.org/10.21638/11701/spbu23.2018.110 (In Russian)