

СОВРЕМЕННЫЕ КОММУНИКАТИВНЫЕ ТЕХНОЛОГИИ

Наталья Рудольфовна Красовская

Кандидат психологических наук,
аппарат Государственной Думы ФС РФ
Москва, Россия
e-mail: goulina@gmail.com



Андрей Анатольевич Гуляев

кандидат философских наук, доцент МГУТУ
им. К. Г. Разумовского
Москва, Россия
e-mail: andrey.gulyaev1966@yandex.ru



УДК: 32.019.51

DOI: 10.24411/2079-0910-2019-12002

К вопросу классификации информационных войн

В статье рассматриваются современные интерпретации и различные по своим основаниям классификации информационных войн. В результате проведенного сравнения различных классификаций информационных войн российскими и западными специалистами можно сделать следующие выводы. С одной стороны, у исследованных классификаций информационных войн имеются многочисленные недостатки, а с другой стороны, у них имеются общие моменты, объединяющие эти столь разные классификации. В результате проведенного исследования удалось выявить наиболее типичные основания для классификации информационных войн и основополагающие виды информационной войны. Предложено дополнение классификации информационных войн с позиций политической психологии, что может служить более глубокому познанию исследуемого феномена. В статье исследуются случаи информационного противоборства, ставится вопрос о необходимости психологических исследований, направленных на минимизацию вредных последствий информационного воздействия на население.

Ключевые слова: информационная война, информационная операция, психологическая война, поведенческая война, кибервойна.

Информационные войны имеют длительную предысторию, но целенаправленно стали изучаться сравнительно недавно. Одним из родоначальников изучения проблемы информационных войн был американский социолог и психолог Гарольд Лассуэлл, считавший пропаганду едва ли не самым действенным орудием в современной войне, к которым он относил Первую мировую войну. «Ведение войны, понимаемое как психологическая задача, может быть успешно лишь при соответствующем моральном уровне населения» [Lasswell, 1929, p. 27]. В своей книге «Техника пропаганды в мировой войне» он рассматривает различные методы пропагандистской работы, которая поднимает моральный дух собственного населения и понижает его у противника.

Единого общепризнанного определения информационной войны на данный момент нет. Очевидно одно — информационная война представляет собой очень сложное и многогранное явление. Мы в своей работе рассматриваем информационную войну лишь в аспекте противоборства государств, обществ и геополитических систем. Формулируя определение, необходимо учесть все факторы этого противоборства, целью которого является достижение неоспоримого преимущества над противником посредством получения, обработки и использования разнообразной информации.

Российский ученый А. В. Манойло предлагает характеризовать информационную войну как информационную деятельность, предпринимаемую политическим образованием (например, государством) для ослабления, уничтожения другого политического образования; как информационную борьбу между соревнующимися конкурентами; как информационный военный конфликт между двумя массовыми врагами, например армиями [Манойло, 2003, с. 9].

По определению, предложенному исследователем Г. Г. Почепцовым, «информационная война — коммуникативная технология по воздействию на массовое сознание с кратковременными и долговременными целями. Целями воздействия является внесение изменений в когнитивную структуру, чтобы получить соответствующие изменения в поведенческой структуре» [Почепцов, 2001, с. 20]. На наш взгляд, данное определение наилучшим образом отражает психологический аспект информационных войн, который можно выделить в отдельный класс информационных войн — «психологическая война» [Почепцов, 2000, с. 14]. Термин «психологическая война» тесно связан со словом «пропаганда» и может интерпретироваться как «пропагандистская война».

Можно констатировать неоднозначность типологизации термина «информационная война». В нашей работе мы рассматриваем проблему классификации информационных войн. По каким основаниям и на какие виды и подвиды можно разделить информационные войны?

Здесь важно отметить различие подходов российских и западных исследователей в изучении проблемы информационных войн. Российские ученые рассматривают понятие «информационные войны» в более широком плане, как информационное противоборство, включающее в себя и пропагандистское противостояние, психологическое и манипулятивное воздействие, информационные операции (например, хищение информации и дезинформацию), а также кибервойну. При этом российские ученые делают упор на первом аспекте понятия «информационная война» — война за умы людей (психологическая война), тогда как западные ученые в основном рассматривают информационную войну в более узком милитаристском плане как кибервойну. Во втором случае информационная война или кибервойна —

это военная стратегия, направленная на создание неблагоприятной обстановки, в частности путем вывода из строя компьютеров противника, управляющих жизненно важными функциями государства или отдельной фирмы, перехвата и искажения информации, внедрением в ПО вирусов, закладок и логических бомб. Такое понимание информационной войны характерно для американских исследователей Кронина и Кроуфорда. Они отмечают будущее превосходство «цифрового Давида» над «бронированным Голиафом». Но также эти исследователи отмечают гражданско-цивилизационный контекст информационной войны, включающий в себя «пропаганду и дезинформацию» [Cronin, Crawford, 1999, p. 260]. Классическим примером такого подхода является пропагандистская акция в американских СМИ против режима Саддама Хусейна в 2003 г. и демонстрация в ООН вещества в пробирке — якобы образца химического оружия, имеющегося у Ирака. Таким образом, для западных специалистов по информационным войнам характерно рассматривать *information war*, во-первых, как отдельный вид боевых действий и, во-вторых, как пропагандистскую подготовку к ним.

Другой западный исследователь, Мартин Либики, считающийся одним из первых теоретиков информационных войн, дал определение информационным войнам как информационному воздействию, элементами которого являются защита, манипулирование, искажение и опровержение информации. М. Либики предложил и первую классификацию форм информационного противодействия (информационной войны) [Libicki, 1995]:

- командно-управленческое — воздействие направлено на каналы связи между командованием и подчиненными им войсками, лишая возможности осуществлять управление и координацию действий;
- разведывательное — воздействие, при котором осуществляется сбор и защита информации, имеющей военное значение;
- электронное — при данном воздействии происходит выведение из строя электронных средств связи и компьютерной техники;
- психологическое — психологическая обработка населения территории противника с помощью информации, аналог «промывки мозгов»;
- хакерское — воздействие посредством компьютерных вирусов, осуществляемое специалистами соответствующего профиля, чьи действия приводят к сбоям в работе связи;
- экономико-информационное — перекрытие каналов осуществления торговых операций, информационная блокада;
- кибервойна — действия, аналогичные хакерским, но с иной целью, а именно с целью захвата информации.

Предложенная Либики классификация, на наш взгляд, является слишком громоздкой; при этом некоторые пункты вполне можно объединить — например, электронное противодействие и кибервойну.

Д. Деннинг предлагает разделять информационную войну по своему характеру на наступательную и оборонительную (защитную) [Denning, 1999]. Это основание для классификации информационных войн можно считать одним из важнейших.

С позиции социологов Ю. П. Сурмина и Н. В. Туленкова информационные войны подразделяются:

- на информационную агрессию, подразумевающую разрушение информационной системы противника и навязывание иной системы ценностей;

- на информационную экспансию, в основе которой лежит длительное эволюционное воздействие, посредством собственных информационных средств на противника с целью его подчинения;
- на информационно-психологическую гражданскую войну, которая предполагает противоборство различных социальных групп внутри самого общества.

Также Ю. П. Сурмин и Н. В. Туленков предлагают выделять следующие виды информационных войн по предмету конфликта:

- психика населения противника является предметом психологической войны;
- система информационных коммуникаций является предметом коммуникационной войны;
- борьба за обладание информацией — представляет собой информационную войну;
- политические, духовные, этические и иные ценности являются предметом ценностной или мировоззренческой войны [Сурмин, Туленков, 2004, р. 113].

К недостаткам данной классификации можно отнести смешение оснований классификации и недостаточно убедительное разделение понятий: например, «агрессия» и «экспансия».

Следует отметить, однако, что в последние годы термин «информационная война» нередко заменяется термином «информационная операция». Многие западные исследователи отмечают, что в военное время информационная война является войной в прямом смысле этого слова, то есть видом боевых действий. В мирное время для информационной войны больше подходит понятие «информационная операция». Таким образом, специалисты призывают классифицировать информационную войну на два вида по такому важнейшему основанию, как «мирное/военное время».

Информационные операции также имеют свою классификацию, предложенную В. Г. Крысько:

1. Психологические операции, которые представляют собой спланированное информационно-психологическое воздействие, оказываемое на население зарубежных стран, с целью вызвать желаемую эмоциональную реакцию, изменить мотивацию и внутренние задачи, внести нужные коррективы в действия правительства, общественных и иных организаций, различных групп и граждан.
2. Операции дезинформации, которые представляют собой действия по преднамеренному введению в заблуждение лиц, принимающих решения, что должно побудить противника предпринять шаги, соответствующие целям инициатора операции.
3. Контрразведывательные операции или операции по обеспечению безопасности — действия по выявлению критически важной для целей осуществления военных, политических и экономических действий информации, а также участков, являющихся уязвимыми для разведки противника и его действий.
4. Электронное противоборство — действия военного характера, при которых используется электромагнитное излучение либо производятся иные действия, посредством которых устанавливается контроль над электромагнитным диапазоном, либо достигается цель поражения противника.

5. Операции в компьютерных сетях, в число которых входят сетевые атаки, защита компьютерных сетей и мероприятия содействия, направленные на сбор и анализ информации о компьютерных сетях противника и способов организации сетевых атак [Крысько, 1999, с. 96].

Эта классификация представляет собой определенный шаг вперед, но при этом не лишена и недостатков. Например, 4-й пункт необходимо убрать как не соответствующий данной классификации.

Как видно из вышеприведенных классификаций, информационные войны в настоящий момент активно исследуются и классифицируются с точки зрения политологии, военных и технических наук, но недостаточно исследований с позиции психологии, хотя воздействие в процессе информационных войн ведется с применением психологических методов, что делает необходимым глубокое и детальное изучение инструментов, применяемых противником с целью создания адекватной системы противодействия.

На наш взгляд, интересна классификация, предложенная В. С. Овчинским и Е. С. Лариной, которые выделяют три основных типа информационных войн:

1. Ментальные (психологические) — по сути, представляющие собой войны контента, целью которых являются изменение сознания или психики масс, групп и/или личности, то есть объектом воздействия являются ценности и установки [Овчинский, Ларина, 2015, с. 25].

Американские ученые П. Лазерсфельд и Р. Мертон предлагают разделять ментальные (психологические войны) на два типа — ведущиеся в военное и мирное время. Так, в мирное время психологическая война обретает черты психологической операции. При проведении психологической операции должен осуществляться контроль над информационными потоками: как формальными (СМИ, образовательные структуры, социальные сети и т. д.), так и неформальными, распространяемыми посредством слухов, мнений и т. д. Важную роль здесь играет привлечение лидеров мнений, оказывающих определяющее влияние на формирование мнения в пределах своей группы. Моделью здесь служит концепция многоступенчатого потока информации П. Лазерсфельда [Lazarsfeld, Merton, 2004].

2. Следующим типом информационной войны авторы работы «Мировойна. Война всех против всех» считают кибервойны. Это система действий одного государства с целью проникновения в компьютеры или сети другого государства для нанесения ущерба или разрушения. Известный американский специалист Р. Кларк считает кибервойну отдельным видом информационной войны, по сути тождественным с военными действиями [Klark, 2011, p. 48].

Другой западный ученый П. Корниш предлагает следующую классификацию кибервойны. Кибервойна состоит из кибератак, киберобороны и киберразведки. Кибератака направлена на информационные системы, обеспечивающие функционирование энергетических, промышленных, военных и других объектов, в результате чего они выходят из строя. Кибероборона заключается в возможности отражения кибератак противника. Киберразведка имеет своей целью добычу полезной информации, проникновение в информационную систему противника. Также предлагается классифицировать кибервойну на два вида: это государственная кибервойна и частная кибервойна. Государственная кибервойна проводится под эгидой государства и означает объявление или продолжение объявленной одним государством (группой государств) войны другому государству (группе государств).

Частная кибервойна может быть начата отдельным лицом (группой лиц) или негосударственной частной организацией против государственных, экономических институтов [Kornish, 2010]. Сложность последней классификации заключается в том, например, что спонсируемая государством кибератака может проводиться частной структурой, и крайне нелегко установить их взаимосвязь. Как считает американский журналист и писатель Ш. Харрис, кибервойна может принимать самые различные гибридные формы [Harris, 2016, p. 78].

Переход от тривиальной информационной войны к кибервойне грозит непредсказуемыми последствиями. Поэтому здесь коллективным способом при помощи международного сообщества должны быть выработаны определенные правила и ограничения и приняты на конференции наподобие Гаагской конференции 1899 и 1907 гг.

3. И наконец, согласно В. С. Овчинскому и Е. С. Лариной, третьим типом информационной войны являются поведенческие войны — войны, основанные на технологиях манипуляции алгоритмами поведения, привычками, стереотипами деятельности, вложенными в нас социумом. Инструментарий поведенческих войн состоит в том, чтобы отделить привычку от сложившегося вида деятельности, сформировавшей ее ситуации, и использовать поведенческие паттерны для достижения иных целей. Именно тема «поведенческих» войн, их сущности, содержания и, главное, практических методов реализации в наибольшей мере табуирована и засекречена в мировом информационном пространстве, покрыта мощным информационным шумом СМИ, обыгрывающих данную тему либо как очередную конспирологическую «страшилку», либо доказывающих технологическую невозможность ведения такого типа войн. Но вот пример: из 500 суперкомпьютеров в мире 233 находятся на территории США. Для сравнения Россия занимает девятое место — с 8 суперкомпьютерами [Овчинский, Ларина, 2015, с. 45]. Для каких же целей нужны такие мощные вычислительные мощности и хранилища данных? Наиболее правдоподобным объяснением появления таких избыточных вычислительных мощностей и хранилищ является их использование для реализации технологий формирования и управления поведением человека.

Как отмечает М. Калдор, пример некоторых современных азиатских и африканских государств, на территории которых годами и даже десятилетиями не затихают гражданские войны одновременно с вмешательством других государств, не является уникальным. Эта же участь в принципе может ждать любое государство [Kaldor, 2015, p. 197]. Как отмечают западные исследователи, средством поведенческой войны служит поведенческое оружие. В его основе лежит технология, получившая название «надж» (от англ. nudge — «подталкивание»). Суть его проста — используя привычки и стереотипы, при помощи создания определенных ситуаций можно подтолкнуть человека или группу людей к принятию определенных решений и осуществлению на их основе определенных действий. По сути, речь идет о новой технологии программирования и внешнего управления человеческим поведением [van Creveld, 2005, p. 236].

Американские военные специалисты вводят еще один вид информационной войны — сетцентрические войны. Концепция «сетцентрической войны» разработана в конце 90-х гг. прошлого века военными теоретиками США А. Себровски и Дж. Гарстка. В основе сетцентрической войны лежит увеличение суммарной боевой мощи воинских формирований путем соединения их в единую сеть, для которой

характерны две основных характеристики: быстрота управления и самосинхронизация. Быстрота управления достигается за счет информационного превосходства путем внедрения новых систем управления, слежения, разведки, контроля, компьютерного моделирования. В результате противник лишается возможности проводить эффективные операции, так как все его действия будут запаздывать. Под самосинхронизацией подразумевается способность организационной структуры воинских формирований, форм и методов выполнения ими боевых задач видоизменяться по своему усмотрению, но в соответствии с потребностями вышестоящего командования. В результате военные действия приобретают форму непрерывных высокоскоростных действий (операций, акций) с решительными целями. Таким образом, сеть позволяет географически рассредоточенные силы (относящиеся к разным видам и родам войск) объединить в едином замысле операции и за счет информационного превосходства использовать эти силы с большей эффективностью путем обеспечения единства взглядов командующих (командиров) разнородных войск (сил) на содержание, роль и место взаимодействия в операции, а также путем самосинхронизации своих действий в интересах достижения общей цели операции [Cebrowski, Garstka, 1998].

Данное описание подчеркивает свойства сетецентрической войны как проявления кибервойны. Поэтому мы не можем выделить сетецентрическую войну в качестве отдельного вида информационной войны и считаем ее разновидностью кибервойны.

Мы предлагаем дополнить эту классификацию информационных войн посредством введения территориального признака. Определить территории, на которых информационная война ведется относительно источника информационного воздействия, очень важно, поскольку цели и задачи информационных войн, ведущихся с собственным населением в качестве объекта воздействия и с населением страны-противника в качестве объекта воздействия, будут принципиально различаться. С этой позиции сначала необходимо выделить территории:

- внешние по отношению к источнику. В этом случае воздействию будет подвергаться либо население страны-противника, либо население нейтральных по отношению к источнику стран;
- внутренние территории. В этом случае воздействию будет подвергаться население страны, к которой источник принадлежит.

Рассмотрим цели психологического воздействия при данном разделении информационных войн по территориальному признаку. При воздействии на население страны-противника могут вестись следующие типы ментальных войн, приводящих к постепенному ослаблению страны-противника:

1. Психологическая/пропагандистская война. Цель — изменение картины мира и установок у объекта воздействия, то есть у населения страны-противника. В этом случае на территории противника посредством использования доступных коммуникационных каналов ведется трансляция информации, посредством которой создается необходимое источнику общественное мнение. Общественное мнение, в свою очередь, способно влиять на принятие элитой государства политических решений и на поведение населения, как активное (протестные мирные акции или, например, действия по подготовке к эмиграции), так и пассивное (апатия, бездействие, отсутствие планирования будущего и действий по достижению ранее

поставленных жизненных целей), что, безусловно, ведет к дальнейшему ослаблению страны-противника.

В качестве примера можно привести проявления психологической войны некоторых СМИ на собственной территории. В 1990-е годы многие СМИ в России принадлежали олигархам. Вместо здорового плюрализма мнений и дискуссий, в основе которых в нормальном цивилизованном обществе патриотизм выступает как естественное чувство и убеждение граждан, в олигархических, клановых СМИ велось разнузданное очернение российской действительности, вызывающее у граждан уныние и депрессию, неверие в собственные силы и чувство стыда за свою родину. За последние 15 лет в России подобную функцию дискредитации всего российского переняли отдельные организации и лица. Зачастую источниками подобной коммуникации выступают популярные медийные персоны, блогеры и т. п.

Проявлением психологической войны является ценностно-идентичностная (мировоззренческая) война. Существует термин «консциентальная война», но, на наш взгляд, он недостаточно точен. Консциентальная война предполагает, что воздействие оказывается на сознание человека, меняя его. На наш взгляд, воздействие в данном виде войны является трехуровневым:

- искажение и разрушение системы ценностей;
- разрушение идентичности;
- формирование новой идентичности.

Изменения же сознания вторичны по отношению к данным процессам.

Примером разрушения старой и навязывания новой идентичности являются события, происходящие на территории Восточной и Центральной Украины в течение 2014–2018 гг. Героизация нацистских коллаборационистов С. Бандеры и его приспешников, терпимость и принятие частью общества ультраправого радикального национализма западноукраинского происхождения привели к масштабным изменениям массового сознания в Украине. Эти изменения формируют новую «бандеровскую» идентичность, совершенно не совместимую с традиционной идентичностью восточноукраинцев.

В микромасштабе примером ценностно-идентичностной войны является вербовка, осуществляемая, например, ИГИЛ (запрещена в России).

В масштабах всего общества в целом такая война чуть было не закончилась поражением России после крушения Советского Союза. И резко повысившаяся смертность, в том числе, безусловно, связана с тем, что часть населения не смогла пройти до третьего этапа, утратив ценности и идентичность: люди просто погибали, запустив процессы самоуничтожения — пассивные (психосоматика) либо активные (саморазрушающее поведение).

В. Овчинским и Е. Лариной отдельно выделяется поведенческая война. Она также ведется, прежде всего, на территории противника. Путем сбора и анализа больших данных выявляются паттерны поведения населения и триггеры их запуска. Посредством использования связки «стимул–реакция» подбираются соответствующие стимулы, вызывающие выявленные реакции в других, не аналогичных изначальным, условиях, что приносит источнику возможность получить преимущество. В настоящее время данный вид информационного воздействия по косвенным данным, имеющимся в открытых источниках, активно разрабатывается в Великобритании и США. В определенной мере к данному виду войн можно отнести «цветные революции», когда посредством информационных вбросов и провокативных

действий вызывалась активно-агрессивная реакция масс, которая запускала процесс противостояния с властными структурами, что заканчивалось либо свержением существующей власти, либо кровопролитным подавлением волнений. Это в любом случае резко ослабляло позиции страны-противника по отношению к источнику информационного воздействия. Информация, усиленная воздействием сильных эмоций, получает распространение и используется на местном уровне в самых разных вариантах для повышения градуса «мобилизационного возмущения». Распространение такой информации в социальных сетях осуществляется при помощи SMS, местных блогов, образов и видеofilmов, для чего используются, например, камеры на мобильных телефонах.

Цель внешних ментальных войн, объектом воздействия которых является население нейтральных стран, — это усиление влияния страны — источника воздействия на население, в том числе на политическую элиту нейтральной страны, посредством чего в дальнейшем достигается ослабление страны-противника. Задачами такой войны является разрушение контактов страны, население которой подвергается воздействию, со страной-противником источника информационного воздействия на всех возможных уровнях, от политического до бытового.

В данной ситуации война ведется, прежде всего, посредством информационных атак в СМИ, с использованием интернет-каналов и личного воздействия с передачей информации (международные мероприятия, форумы, конференции), следствием чего является формирование негативного общественного мнения, которое приведет к сокращению контактов. Сокращение контактов является основой минимизации поступления объективной информации, возникновения барьеров на пути применения инструментов «мягкой силы», усиление экономической изоляции и т. д., что создает возможности для усиления влияния источника информационного воздействия на общество данной страны. Пример такой войны — действия коллективного Запада на территории стран бывшего СССР по формированию негативного имиджа России.

При воздействии на население собственной страны ключевой целью является создание основы для принятия политических решений — формирование общественного мнения и создание условий, чтобы это общественное мнение не подверглось коррекции при ответном воздействии противника.

Примером создания негативного общественного мнения при ведении психологической войны на собственной территории является война против талибов на территории Афганистана. Для подготовки принятия решения о вторжении в Афганистан население США активно обрабатывалось ведущими СМИ.

Информационные войны стали всеобъемлющими в эпоху распространения СМИ (газет, журналов, радио, телевидения) и всеобщей грамотности. Вопреки устоявшемуся мнению, умело манипулировать легче образованным человеком, чем необразованным или малообразованным. Манипулятор в этом случае точнее достигнет своей цели, поскольку образованный человек будет более эффективным орудием в руках манипулятора. Это требует от манипулятора нестандартных, креативных подходов в формировании такой информации и способов ее распространения, чтобы проникнуть в сознание манипулируемого образованного человека и подтолкнуть его к желаемому поведению. Зачастую используется метод сравнения — вот так это обстоит «у них» (обычно на Западе), а вот так у нас. Такие сравнения обычно не выдерживают никакой критики, поскольку крайне некорректны.

С появлением современных медиасредств, социальных сетей и других интернет-платформ возможности для информационных войн выросли многократно. Фейковые новости, многотысячные репосты непроверенной информации, провокационные видеоролики в «Ютубе» и т. д. способны взорвать стабильность и консолидацию в обществе. Современные «цветные революции» уже во многом являются детищем интернет-платформ.

Подводя итоги исследованию классификации информационных войн, следует отметить, что в качестве первичного деления информационных войн мы берем такое основание, как мирный/военный, а также духовный/технический. В этом случае информационные войны делятся на два главных типа — психологическая война и кибервойна. Психологическая война имеет три направления: в отношении собственного населения; в отношении нейтрального населения; в отношении населения страны-противника. Кроме того, термин «информационная война» в мирное время часто заменяется выражением «информационная операция». Кибервойна также ведется в отношении собственного населения (например, в форме шпионажа), нейтрального населения и населения страны-противника. В свою очередь, стоит заметить, что в мирное время помимо пропаганды используются скрытные кибероперации, а в военное время используется и пропаганда. Поэтому такое деление все же является условным. Каждый тип информационной войны имеет свои виды. Психологическая война включает в себя ментальную войну и поведенческую войну. Оба вида могут выступать в двух качествах — нападения и обороны.

Второй тип информационной войны — кибервойна — может иметь три вида: кибератака (как разновидность, хакерские атаки), киберразведка (кибершпионаж), киберзащита.

Информационные войны фактически стали неотъемлемой частью нашей жизни. Изошренность методов воздействия будет лишь нарастать, что обуславливает высокую актуальность исследований рассматриваемой проблемы и необходимость дальнейшего ее изучения с различных сторон, в том числе с точки зрения психологии с выявлением используемых в данной области инструментов, способов внушения и манипуляций и выработкой адекватных инструментов противодействия.

Литература

- Ван Кревельд М.* Трансформация войны. М.: ИРИСЭН, 2005. 343 с.
- Калдор М.* Новые и старые войны: организованное насилие в глобальную эпоху. М.: Изд-во Института Гайдара, 2015. 412 с.
- Кларк Р., Нейк Р.* Третья мировая война. Какой она будет. СПб.: Питер, 2011. 336 с.
- Крысько В. Г.* Секреты психологической войны: Цели, задачи, методы, формы, опыт. Минск: Харвест, 1999. 446 с.
- Лассуэл (Ласвель) Г.* Техника пропаганды в мировой войне. М.: Госиздат, 1929. 200 с.
- Манойло А. В., Петренко А. И., Фролов Д. Б.* Государственная информационная политика в условиях информационно-психологической войны. М.: Горячая линия — Телеком, 2003. 541 с.
- Овчинский В., Ларина Е.* Мировойна. Война всех против всех. Новейшие концепции боевых действий англосаксов. М.: Книжный мир, 2015. 416 с.
- Почепцов Г. Г.* Информационные войны. М.: Рефл-бук, 2001. 576 с.
- Почепцов Г. Г.* Психологические войны. М.: Рефл-бук, Киев: Ваклер, 2000. 528 с.

Сурмин Ю. П., Туленков Н. В. Теория социальных технологий: учебное пособие. Киев: МАУП, 2004. 605 с.

Харрис Ш. Кибервойн@: пятый театр военных действий. М.: Альпина нон-фикшн, 2016. 389 с.

Cebrowski A. K., Garstka J. J. Network-Centric Warfare: Its Origins and Future // U. S. Naval Institute Proceedings. 1998. January. P. 5–48.

Cronin B., Crawford H. Information Warfare: It's Application in Military and Civilian Contexts // The Information Society. 1999. Vol. 15. № 4. P. 257–263.

Denning D. E. Information warfare and security. Washington: GPG, 1999. 260 p.

Kornish P. On Cyber Warfare. London: The Royal Institute of International Affairs, 2010. 124 p.

Lazarsfeld P., Merton R. Mass Communication, Popular Taste, and Organized Social Action. New York: JohnWileyandSons, Inc., 2004. 432 p.

Libicki M. What is information warfare? Washington: GPG., 1995. 280 p.

Concerning the Classification of Information Wars

NATALIA R. KRASOVSKAYA

Central Office of the State Duma of the Federal Assembly of the Russian Federation,
Moscow, Russia
e-mail: goulina@gmail.com

ANDREY A. GULYAEV

K. G. Razumovsky Moscow State University of Technologies and Management,
Moscow, Russia
e-mail: andrey.gulyaev1966@yandex.ru

The article considers some modern interpretations and various classifications of information wars. As a result of comparing different classifications of information wars by Russian and Western experts the following conclusions can be drawn. On the one hand, the information wars classifications have numerous disadvantages, and, on the other hand, they have common points that unite these so different classifications. As a result of research, it became possible to identify the most typical grounds for classifying information wars and the basic types of the information war. The addition of the classification of information wars from the standpoint of political psychology is offered, which can contribute to a deeper understanding of the phenomenon under consideration. The article investigates the cases of information confrontation; the authors raise the question of the necessity of psychological research aimed at minimizing the harmful consequences of information impact on the population.

Keywords: information war; information operation; psychological war; behavioural war; cyberwarfare.

References

Cebrowski, A., Garstka, J. (1998). Network-Centric Warfare: Its Origins and Future, *Naval Institute Proceedings*, January, USA.

Cronin, B., Crawford, H. (1999). Information Warfare: It's Application in Military and Civilian Contexts, *The Information Society*, vol. 15, no 4, October, pp. 257–263.

Denning, D. (1999). Information warfare and security, Washington: GPG, 260 p.

- Harris, S. (2016). *Kibervoyn@: pyatyy teatr voennykh deystviy [Cyberwar@: fifth theatre of war]*, per. s angl., Moskva: Al'pina non-fikshn, 392 p. (in Russian).
- Kaldor, M. (2015). *Novye i starye voyny: organizovannoye nasiliye v global'nyuyu ehpokhu [New and Old Wars: organized violence in a global era]*, per. s angl., Moskva: Izd-vo Instituta Gaydara, 416 p. (in Russian).
- Klark (Clarke), R., Knake, R. (2011). *Tret'ya mirovaya voyna. Kakoy ona budet [Third world war. What it will be]*, per. s angl., S. Peterburg: Piter, 336 p. (in Russian).
- Kornish P. (2010). *On Cyber Warfare*, London: The Royal Institute of International Affairs, 124 p.
- Krys'ko, V.G. (1999). *Sekrety psikhologicheskoy voyny [The secrets of psychological warfare]*, Minsk: Harvest, 208 p. (in Russian).
- Lasswell, H.D. (1929). *Tekhnika propagandy v mirovoy voynе [Propaganda technique in the World War]*, per. s angl., Moskva: Gosizdat, 200 p. (in Russian).
- Lazarsfeld, P., Merton, R. (2004). *Mass Communication, Popular Taste, and Organized Social Action*, New York: JohnWileyandSons, Inc., 432 p.
- Libicki, M. (1995). *What is information warfare?* Washington: GPG, 280 p.
- Manoylo, A.V. (2003). *Gosudarstvennaya informatsionnaya politika v osobykh usloviyakh [State information policy in special conditions]*, MIFI, Moscow, 388 p. (in Russian).
- Ovchinskiy, V., Larina, E. (2015). *Mirovovoyna. Voyna vseh protiv vseh [World. The war of all against all]*, Moskva: Knizhnyy mir, 416 p. (in Russian).
- Pocheptsov, G.G. (2001). *Informatsionnye voyny [Information wars]*, Moskva: Refl-buk, 576 p. (in Russian).
- Pocheptsov, G.G. (2000). *Psikhologicheskiye voyny [Psychological warfare]*, Moskva: Refl-buk, Kiev: Vakler, 528 p. (in Russian).
- Surmin, Yu.P., Tulenkov, N.V. (2004). *Teoriya social'nykh tekhnologiy [Theory of social technologies]*, Kiev: MAUP, 608 p. (in Russian).
- Van Creveld, M. (2005). *Transformatsiya voyny [The Transformation of War]*, per. s angl., Moskva: IRISEHN, 344 p. (in Russian).