■ ■ ■ Сущность информационной войны в региональном политическом конфликте и основные формы ее проявления

Муратова Ю.Д.

Казанский федеральный университет, Казань, Российская Федерация.

Аннотация. В научной статье рассмотрена роль информационной войны в современной политической практике и ее возможностей воздействия на ход политического конфликта. В ходе изучения проблематики сущности информационных войн в рамках политического конфликта автором были проанализированы одни из самых авторитетных в научном сообществе концепций отечественных и зарубежных теоретиков, среди которых большой вклад в исследование данной проблематики внесли И.Н. Панарин, А.В. Манойло, С.П. Расторгуев, С. Манн, Ф. Хоффман. Изучены подходы к понятию информационной войны в рамках научной дискуссии об уровне самостоятельности этого явления как отдельного вида войны. Информационная война рассматривается как инструмент «мягкой силы» для воздействия региональными политическими субъектами на иные суверенные государства с целью осуществления внешнеполитических задач. Исследованы компоненты информационной войны, в том числе современные технологии воздействия в киберпространстве, хакерские атаки на компьютерные системы, пропаганда.

Ключевые слова: информационная война, информационно-психологическое воздействие, кибернетическая война, политический конфликт, хакерские атаки, электронная война, информационные технологии, гибридная война

Для цитирования: Муратова Ю.Д. Сущность информационной войны в региональном политическом конфликте и основные формы ее проявления // Коммуникология. 2018. Том. 6. №1. С. 34-45. DOI 10.21453/2311-3065-2018-6-1-34-45.

Сведения об авторе: Юлия Джамилевна Муратова, аспирант кафедры конфликтологии Казанского федерального университета. Адрес: 420008, Казань, ул. Кремлёвская, 18. E-mail: iuliia_muratova@mail.ru.

Статья поступила в редакцию: 08.02.2018. *Принята к печати:* 13.02.2018.

Информационные технологии на современном уровне развития создают широкие возможности управления политическими конфликтами как в масштабах одного государства, так и на региональном уровне. Данные технологии, активно применяющиеся в информационных войнах, имеют ряд преимуществ перед традиционными средствами борьбы благодаря своему массированному воздействию на моральное – психологическое состояние населения страны-противника или отдельных партий, движений и политический объединений. Особое преимущество информационной борьбы заключается в том, что спецслужбы неспособны своевременно выявить подобный вид воздействия и принять защитные меры

для обеспечения информационной безопасности. Информационная пропаганда, как неотъемлемая и значимая часть информационной войны, создает атмосферу безнравственности и бездуховности, дезориентирует население, контроль над которым становится невозможно установить мирными средствами. Самым опасным последствием подобного воздействия становится падение авторитета и легитимности государственных властей, против которых, зачастую, и направлены информационные атаки. Информационные технологии все чаще применяются с целью дестабилизации политических отношений между отдельными субъектами современной политики, провоцирования политического конфликта. Информационная война в политическом конфликте ориентирована, прежде всего, на внесение раскола в гражданское общество. Следствием ряда таких информационных мероприятий становится гражданская война, которая в условиях сложной внешнеполитической обстановки затрудняет принятие решений политической элитой из-за беспорядочных массовых протестных акций и беспорядков. Искусственно инициируемые столкновения на религиозной, этнической и национальной основе становятся фундаментом для возможного уничтожения существующего политического строя в данном государстве. Длительная пропаганда не только ведет к разрушению государства изнутри, но и снижает международный авторитет страны-противника, что впоследствии отражается на его отношениях с региональными партнерами. Информационная война все больше доказывает свою эффективность в достижение политических целей в регионе и способна нанести непоправимый ущерб тому, против кого она ведется.

Концептуальной основой теории информационной войны, по мнению автора научной статьи, является теория «мягкой силы» С. Мана. Термин «мягкая сила» широко вошел в лексикон политиков и ученых. Следует дополнить, что концепция внешней политики Российской Федерации от 12 февраля 2013 г. также основывается на идее, что «неотъемлемой составляющей современной международной политики становится «мягкая сила»[1]. В данном случае, «мягкая сила» становится комплексным инструментарием для достижения политических целей, которую можно использовать перманентно как в условиях открытого вооруженного конфликта, так и в мирные периоды сотрудничества. «Мягкая сила» включает прежде всего те технологии, которые наименее затратны, обладают слабой распознаваемостью и высокой эффективностью в трансформации поведения политического противника не силовыми методами.

Но, вместе с тем, необходимо отметить, что в условиях усиления глобальной конкуренции, использование «мягкой силы» в целях оказания политического давления на суверенные государства приобретает деструктивный и противоправный характер. Подобную политику с использованием информационных технологий как метода «мягкой силы» можно интерпретировать как противоправное

[1] Концепция внешней политики Российской Федерации (утверждена президентом Российской Федерации В.В. Путиным 12 февраля 2013 г.) [электронный ресурс]: http://www.mid.ru/foreign_policy/official_documents/.

вмешательство во внутренние дела других государств, следствием чего является дестабилизация внутриполитической обстановки, манипулирования общественным мнением и сознанием.

«Мягкая сила» рассматривается теоретиком как способность влиять на другие государства с целью реализации собственных целей через сотрудничество в определенных сферах, направленное на убеждение и формирование положительного восприятия [Mann]. Таким образом, информационные войны с их возможностями манипулирования общественным сознанием, политической обстановкой и эмоциональным климатом в других государствах дают возможности для разрушения его политических и социальных ценностей без применения физического насилия.

Необходимо выделить три основные группы для определения понятия «информационной войны», представленные современными исследователями.

Авторы первой группы связывают «информационную войну» с отдельными информационными операциями. Необходимо отметить, что В.С. Пирумов определяет информационную войну не только как политическое противостояние с использование информационно-коммуникативных методов, но и как совокупность мероприятий по защите информационного пространства собственной страны [Пирумов, Родионов]. Таким образом, информационная война становится новым видом борьбы, в котором не менее важным становится защита своего информационного ресурса. Важно также подчеркнуть, что в данном случае информационная защита в отличие от технологий информационной агрессии имеют более высокую значимость, так как не в зависимости от желания политического субъекта информационное воздействие может быть осуществлено даже в периоды благополучной и перспективной международной политики. В отличие от традиционной войны, информационная война всегда остается необъявленной и носит непредсказуемый характер. По мнению автора статьи, важно обратить внимание на тот факт, что периоды международного сотрудничества потенциально опаснее явных конфликтов, так как информационное вмешательство в «открытую» для международного контакта систему более осуществимо по сравнению с периодом острых противоречий, когда государства максимально активизируют все защитные механизмы физических и информационных ресурсов. Исходя из того, что информационная война носит перманентный характер, проблема информационной безопасности становится ключевой. Так, В.И. Цымбал добавляет, что информационная война являет собой новый способ политического противостояния [Цымбал]. Следовательно, с этой точки зрения информационная война становится инструментом политической борьбы во всех ее формах.

Авторов второй группы представляют специалисты по информационным технологиям военных ведомств.

Согласно мнению представителей военной науки, информационная война является процессом, который сопровождает вооруженное противоборство и не проводится в мирные периоды. Информационные операции являются дополнительным средством борьбы при активном применении военного оружия, которое позволяет в короткие сроки деморализовать противника. Во время боевых

действий важным является охранять информационное превосходство над противником, которое достигается своевременным принятием информационных контрмер, выработкой технологий информационной поддержки и защиты. Комов С.А., исследуя роль информационных операций в ходе боевых действий, обращает внимание на то, что они повышают эффективность военных действий, а процесс достижения политических целей становится более ускоренным [Комов].

Авторы третьей группы определений «информационной войны» считают ее явлением внешне мирного периода, целью которой является решение политических задач не силовым методом и предупреждение возможного политического конфликта [Крынина]. Таким образом, мнения о понятии «информационной войны» разделились по принципу: является ли это явление самостоятельным процессом или составной частью более широкого понятия. Обобщив вышеизложенные взгляды, нужно отметить, что информационная война одновременно может сопровождать военные действия и осуществляться, заменяя их. По мнению автора, информационная война является самостоятельным понятием. Несмотря на то, что она является одним из возможных путей поражения противника, и с этой точки зрения является средством, она имеет свои механизмы воздействия, приемы, средства и техники и, более того, ее возможности выходят далеко за пределы противостояния в политических конфликтах.

Мы видим, что единое мнение в научном мире относительно формирования точной характеристики такого явления как «информационная война» на данном этапе не завершено. Подобные дискуссии развиваются в рамках поиска единого терминологического подхода. Так, С.Н. Гриняев, С.А. Модестов, М.А. Родионов обращают внимание на то, что сам термин «информационная война» не совсем адекватен, и было бы более правильно называть этот вид военных действий информационной борьбой. Склоняясь к мнению второй группы, данный термин они объясняют тем, что информационная война является составной частью военного противоборства, а не самостоятельным процессом [Гриняев].

Военно-политическое руководство США на официальном уровне заменили термин «информационная война», таким термином, как «информационные операции» [Костюхин, Горбунов]. Это связано с тем, что в 1998 г. Генеральному секретарю ООН было направлено специальное послание, касающееся проблемы международной информационной безопасности от министра иностранных дел РФ. В послании особый акцент был сделан на необходимости предотвращения появления принципиально нового информационного оружия. Информационное оружие было отнесено к оружию массового поражения для решения принципиально новых конфликтов. Согласно исследованиям РФ, США уже владеет этим оружием, в то время как другие государства еще только осваивают информационные технологии[1]. Таким образом, США может стать мировым лидером, имея

[1] Совместное заявление об общих вызовах безопасности на рубеже XXI века от 2 сентября 1998 г. // Дипломатический вестник МИД России, 1998 г., Октябрь, №10 [эл. ресурс]: http://www.businesspravo.ru/Docum / DocumShow_DocumID_62942.html.

монопольное владение этим оружием, с возможностью уничтожать национальные государства. Подобные заявления могли послужить причиной тому, что США прекратили использовать термин «информационная война», а в место него стали использовать термин «информационные операции».

В странах Западной Европы, термин «информационная война» заменен на термин «кибервойна», но наделяется он тем же содержанием и смыслом, которые приписывают «информационным войнам». Что касается русских специалистов, то здесь ситуация совершенно обратная: термином «кибервойна» пользуются осторожно [Антонович: 39-44].

Панарин И.Н. в своих работах больше применяет понятие «информационное противоборство», которое направлено на поддержание особого темпа проведения операции, превосходящего любой возможный темп противника. Такое превосходство позволяет доминировать во все время проведения информационной операции и оставаться непредсказуемым. Иными словами, информационное противоборство – это действие, направленное на опережение противника. [Панарин] И.Н. Панарин отмечает, что информационное противоборство – это не новое явление, и в своем развитии оно прошло множество этапов.

Также необходимо отметить, что в настоящее время имеется множество классификаций информационной войны и сфер ее применения, что создает сложности в том, чтобы дать ей точное определение, но, несмотря на это, эффективность информационных технологий остается бесспорной. Так, учитывая высокую роль информационных технологий в политических конфликтах, в число сфер ведения боевых действий, помимо земли, моря, воздуха и космоса теперь включается информационная сфера. Основными объектами поражения в данной сфере являются информационная инфраструктура и психика человека [Harley].

Однако, не смотря на разнообразие подходов, наиболее исчерпывающее определение «информационной войны», которое имеет высокий уровень признания в научных кругах, предложил американский теоретик М. Либики, выделив семь ее разновидностей: противоборство разведок и контрразведок, противоборство в электронной сфере, психологические операции, организованные стихийные хакерские атаки на информационные системы, информационно-экономические войны за контроль над торговлей, военное противостояние, кибернетические войны в виртуальном пространстве [Libicky]. Иными словами, можно сказать, что информационная война включает в себя интегрированное использование возможностей, среди которых выделяются психологические и компьютерные сетевые операции в качестве электронного оружия. В условиях военного политического конфликта информационные технологии способны обеспечивать операции с военной дезинформацией и дезорганизацией.

Психологический и идеологический аспекты информационной войны наиболее подробно рассмотрены в работах С.П. Расторгуева [Расторгуев]. По его мнению, основное преимущество информационной войны заключается непосредственно «в работе с глубинными смыслами и представлениями человека» [Расторгуев: 16]. По мнению автора статьи, такой вид воздействия, который можно

было бы назвать войной ценностей, меняя представления человека способен программировать его на определенный вид поведения в конкретной политической ситуации. Результатом таких процессов становится то, что «масса, убежденная в навязанных извне политических идеалах, становится практически неуправляемой для государственных властей» [Расторгуев: 32]. Исходя из этого, можно утверждать, что данный вид воздействия приводит к самым опасным социальным явлениям в условиях политического конфликта – выходу народных действий из-под контроля и началу массовых протестов. Иными словами, информационное воздействие и манипуляция политическими установками населения создает ситуацию нестабильности и резко сокращает шансы политического противника на выгодное для него разрешение политического конфликта. Но основной целью смыслового информационного воздействия в политическом конфликте, опираясь на взгляды Г.Г. Почепцова, является изменение расстановки политических сил в обществе.

Согласно концепции Манойло А.В., информационно-психологическая война с неограниченными возможностями воздействия на отельного человека служит «средством достижения политических целей в масштабах одного государства или даже целого региона» [Манойло, Петренко, Фролов: 52]. В основе информационно-психологической войны, согласно рассматриваемой концепции, лежит «конфликт интересов субъектов геополитической конкуренции, целью которого является разрешение противоречий по поводу осуществления политического руководства в информационном пространстве и по поводу перераспределения их роли и функций в политической системе информационного общества» [Манойло, Петренко, Фролов: 22]. Таким образом, мы можем сделать вывод, что все открытые и скрытые информационные воздействия направлены на достижение информационного превосходства над противником, что находит свое выражение в нанесении ему идеологического и морального ущерба.

Данные положения идеально согласовываются с концепцией Почепцова, в которой «информационную войну нельзя рассматривать только как возможность технического вмешательства в информационные системы противника», так как она способна действовать на более сложных уровнях и вносить изменения в когнитивные, поведенческие и мыслительные процессы человека [Почепцов: 87]. В своей монографии «информационные войны» теоретик определяет цель такой войны как «внесение изменений в когнитивную структуру для того, чтобы получить соответствующие изменения в поведенческой структуре» [Почепцов: 96]. Согласно позиции автора, объектом информационной агрессии является поведенческий стереотип, доступ к которому открывается через когнитивную сферу. Исходя из этого, необходимо признать, что изменение поведенческой структуры могут реализовать как краткосрочные планы, которые могут быть связаны с формированием общественного мнения по отношению к государственным деятелям или политическим событиям, так и решать более сложные задачи, которые возможно осуществить с помощью информационно-коммуникативных технологий. Если поведенческая структура формируется на когнитивном уровне, вклю-

чая навыки и приемы мышления, то внесение любых изменений в когнитивную структуру общественного сознания на уровне целой страны, способно привести к непредсказуемым последствиям в поведенческом стереотипе населения.

Любая социальная система поддается разрушению, если «через когнитивный механизм меняется поведенческая структура, так как эти изменения способны парализовать системное управление» [Почепцов: 41]. Рассматриваемая теория использует категории «пропаганда», «психологические операции», «психотропное воздействие» в качестве форм ведения информационной войны. Геополитическая модель информационной войны не может быть рассмотрена вне базовых подходов политической психологии и конфликтологии, так как информационная война имеет человеческий фактор, так как ведется людьми и направлена на людей, в том числе и представителей политического или военного руководства.

Сравнивая несколько концепций, необходимо подчеркнуть, что Манойло А.В. в своих трудах рассматривал информационную войну с точки зрения ее возможностей осуществлять политическое противостояние в рамках геополитической конкуренции, в то время как Почепцов и Расторгуев исследовали явление информационной войны, прежде всего, как процесс воздействия на когнитивные структуры психики человека, анализируя глубинный механизм процесса трансформации психики человека, не ставя вопрос о целях подобных информационных мероприятий, так как в рамках указанных концепций, они могут широко варьироваться и выходить за пределы политических интересов. Данные концепции дают в симбиозе дают представления о направленности информационной войны, целях и методах ведения.

Рассмотренный психологический аспект информационной войны становится также составной части другой разновидности информационной войны, выделенной Либики – кибернетической войны. Снова обращаясь к идеям данного теоретика, необходимо обратить внимание на одну из его фундаментальных работ, изданной в 2009 году. В монографии «Киберсдерживание и кибервойна» В М. Либики выдвигает основную свою идею: киберпространство является совершенно особым типом пространства, так как в нем атака осуществляется «не за счет порождения силы, а за счет использования уязвимости противника» [Libicky: 93].

Так, киберконфликт условно можно охарактеризовать как совокупность нескольких сфер: социальные медиа, стратегическая война, промышленный шпионаж с нанесением ущерба по информационной инфраструктуре и идеологическая борьба [Jajodia, Shakarian, Subrahmanian, Swarup, Wang]. Так, киберпространство становится новым полем борьбы для достижения военно-политического преимущества. Следствием является наблюдаемая тенденция во многих странах инвестировать финансовые ресурсы в контроль над интернет-пространством, особенно, в государствах с авторитарным режимом, где предпосылки для народных восстаний уже проявились. Интернет в таких случаях становится форумом для организации крупномасштабных акций.

Так, автор книги «Кибервойна: техника, тактика и инструменты для специалистов по безопасности» Дж. Андресс отмечает, что «программы контроля распро-

страняются только на оружие массового поражения: ядерное, биооружие, химическое оружие, в то время как кибероружие не признано опасным, так как не приводит непосредственно к смерти». Автор считает данную позицию ошибочной, потому что кибероружие способно подорвать национальную безопасность, экономический и политический базис. В данной работе предлагаются некоторые меры для защиты государства от кибероружия: выделять часть бюджета на обеспечение кибербезопасности, поддерживать образовательные программы и научные исследования в области кибертехнологий, расширение возможностей ситуационной осведомленности о возможных информационных инцидентах, разработка сценариев по управлению рисками и предотвращению угроз, обеспечение связи в чрезвычайных ситуациях, оставляя сеть нейтральной, разработка механизмов для получения информации о кибербезопасности [Andress, Winterfeld]. Важно признать, что на сегодняшний день планомерно ведется война с терроризмом, наркотиками, но практически ни одно государство не ведет серьезную борьбу с кибертерроризмом, что может обернуться международной катастрофой.

Автор рассматриваемой работы также выделяет то, что кибер-преступления чаще всего организовываются негосударственными акторами, способными подорвать политический порядок. К ним он относит террористические группы, хакеров, хактивистов и мошенников [Andress, Winterfeld]. Результатом становится ситуация, в которой новые современные технологии все больше заменяют физическое оружие и становятся доступными для негосударственных сил, что осложняет возможности контроля над ними. Такие группы могут преследовать как собственные цели, занимая ту или иную сторону в конфликте, либо тайно обеспечивать государственные интересы. По мнению автора, «основная цель кибертерроризма – нанесение ущерба крупномасштабной электрической сети или выведение из строя диспетчерского управления» [Andress, Winterfeld: 101] Все это вызывает волнение и беспокойство среди целевого населения, что открывает большие возможности для террористов.

Рассматривая техническую сторону информационной войны, необходимо сказать, что она также представляет собой форму конфликта, в процессе которой осуществляется прямая атака на информационные системы противника. Успех информационной компании зависит от эффективности выполнения ее стратегической и оперативной стороны. На оперативном уровне важно влияние на возможности врага принимать решения оперативно и эффективно, то есть создать условия для организации помех принятия решений противником. В результате таких операций противник не может действовать или вести войну координировано. На военном уровне техническими формами реализации цели становятся: война с использованием средств разведки, радиоэлектронная борьба, хакерская война. Радиоэлектронная борьба связана с созданием помех радиолокационным системам противника, что не позволяет ему получать информацию о боевых действиях и дезориентирует.

Необходимо отметить, что совокупность различных форм информационной войны, включая техническую, кибернетическую, электронную, психологи-

ческую, делает ее частью более широкого понятия – «гибридной войны». Теорию «гибридных» войн вывел бывший офицер морской пехоты и научный сотрудник министерства обороны США Ф. Хоффман. Автор концепции утверждает, что конфликты будут мультимодальными и вестись разными способами. По Ф. Хоффману, будущие угрозы можно охарактеризовать как «гибридное сочетание традиционных и нерегулярных тактик с использованием одновременно простых и сложных технологий, использующихся как государствами, так и негосударственными акторами» [Hoffman]. Ф. Хоффман в статье, вышедшей в июле 2014 г., пришел к выводу, что первые разработки «гибридной» войны принадлежат России, так как именно она впервые использовала ее методы в 2008 году в Грузии [Hoffman]. В более ранних работах Ф. Хоффман доказывает, что «гибридная» война отличается своей связью с терроризмом, преступностью и криминальным порядком». Также автор подчеркивает, что нередко наркотики, контрабанда и торговля людьми становятся инструментами для подрыва легитимности правительства [Hoffman].

Выводы

Подводя итог, необходимо сказать, что информационная война в региональном политическом конфликте, которую также называют информационным противоборством или борьбой, включает в себя достаточно широкий арсенал средств информационного подавления политического противника. Новейшие разработки в области информационных технологий позволили вести борьбу на совершенно новых уровнях геополитического пространства: кибернетическом и электронном. Воздействие информационного оружия становится все сложнее контролировать, что ставит перед международным сообществом проблему информационной безопасности и защиты информационных ресурсов в отдельных странах. В политический конфликт, который изначально может вестись двумя сторонами, по причине широких возможностей информационных технологий, может включаться все большее количество участников, что значительно отодвигает границы конфликтного региона. Данный вид войны особо опасен своим деструктивным воздействием на все сферы общества, включая более тонкие материи, такие как психика человека, его ценности, чувство патриотизма и национального самосознания, которые, в свою очередь, являются важной составляющей политического выбора и поведения. Манипуляция сознанием населения политического противника и мирового сообщества в рамках регионального конфликта становится одной из самых важных технологий информационной войны, так как позволяет не только спровоцировать противоположную сторону конфликта на определенные политическое шаги, но и создать выгодные внешние условия, при которых государства, имеющие к конфликту опосредованное отношение будут воспринимать его так, как это необходимо «провокатору» для повышения легитимности и признания собственных действий. Рассматриваемый вид борьбы позволяет странам, обладающим информационным превосходством, достигать своих политических целей как в военные, так и относительно мирные периоды.

Информационная война как технология мягкой силы становится неотъемлемой частью политического конфликта на региональном и глобальном уровне, благодаря своему «мягкому» воздействию, возможностью без применения силовых средств радикально менять политическую обстановку внутри страны-противника, снижая уровень легитимности действующих в ней властей, экономя материальные средства на традиционные виды борьбы и обеспечивая параллельно алиби от возможных обвинений в национальной агрессии и экспансионистских устремлений.

Источники

Антонович П.И. (2011). О сущности и содержании кибервойны // *Военная мысль.* №7. С. 39-46

Гриняев С.Н. (2000). Война в четвертой сфере // *Независимое военное обозрение.* №42. С. 7.

Комов С.А. (1996). Информационная борьба в современной войне: вопросы теории // Военная мысль. №3. С. 73

Костюхин А., Горбунов Г. (2007). Информационные операции в планах командования ВС США // *Зарубежное военное обозрение*. № 5. С. 14.

Крынина О.Ю. (2009). Дефиниции понятия «Информационная война» анализ российского и зарубежного опыта // *Новые технологии*. № 3. С. 68–70.

Манойло А.В., Петренко А.И., Фролов Д.Б. (2003). Государственная информационная политика в условиях информационно-психологической войны. Москва

Панарин И.Н. (2006). Информационная война и геополитика. Москва

Пирумов В.С., Родионов М.А. (1997). Некоторые аспекты информационной борьбы в военных конфликтах // *Военная мысль.* № 5. С. 44-47.

Почепцов Г.Г. (2006). Информационные войны. Москва.

Расторгуев С.П. (1998). Информационная война. Москва.

Цымбал В.И. (1995). О концепции информационной войны // Безопасность (информационный сборник). № 9. С.35

Andress J., Winterfeld S. (2011). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners / ed. by A. Ward. Elsevier.

Harley I.A. (1996). Role of Information Warfare. Truth and Myths. USA.

Hoffman F.G. (2005) Future Warfare: The Rise of Hybrid Wars. USA. P. 18–19.

Hoffman F.G. (2006). How Marines are Preparing for Hybrid Wars // *Armed Forces Journal*. JFQ: Joint Force Quarterly. P. 34–48.

Jajodia S., Shakarian P., Subrahmanian V.S., Swarup V., Wang C. (ed.) (2015). Cyber Warfare: Building the Scientific Foundation. Springer Int. Publishing.

Libicky M.C. (2009) Cyberdeterrence and Cyberwar [electronic source]: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf. RAND, USA.

Mann S.R. (1997). The Reaction to Chaos. In: Complexity, Global Politics, and National Security / ed. by David S. Alberts and Thomas J. Czerwinski. National Defense University, Washington, D.C.

■ ■ ■ The Essence of Information Warfare in Regional Political Conflicts and the Main Forms of its Manifestation

Yulia D. Muratova

Kazan Federal University, Kazan, Russian Federation.

Abstract. The paper dwells upon the examination of role of information warfare in contemporary political practice and its ability to influence political conflict. The author analyses of some of the most authoritative concepts in the scientific community of domestic and foreign theorists. Besides, the author reveals the principal approaches to the concept of information warfare through scientific discussion on the level of independence of this phenomenon as a substantive type of warfare. The information warfare is as a tool of 'soft power' used by the regional political actors to influence on other sovereign states with a view to achieve certain objectives of foreign policy. The author explores all the components of the information warfare including modern technologies of influence in cyberspace, hacker attacks on computer systems and traditionally known information and psychological propaganda.

Keywords: information warfare, information-psychological impact, cybernetic war, political conflict, hacker attacks, electronic warfare, information technologies, hybrid warfare

For citation: Muratova Y.D. The Essence of Information Warfare in Regional Political Conflicts and the Main Forms of its Manifestation. *Communicology (Russia)*. 2018. Vol. 6. No.1. P. 34-45. DOI 10.21453 / 2311-3065-2018-6-1-34-45.

Inf. about the author: Yulia Djamilevna Muratova, postgraduate student at the department of conflict management, Kazan Federal University. Address: 420008, Kazan, Kremlyovskaya st., 18. E-mail: iuliia_muratova@mail.ru.

Received: 08.02.2018. *Accepted*: 13.02.2018.

References

Andress J., Winterfeld S. (2011). Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners / ed. by A. Ward. Elsevier.

Antonovich P.I. (2011). On the essence and content of cyber warfare. *Military thought*. No.7. P. 39-46 (In Rus.).

Grinyaev S.N. (2000). War in the fourth sphere. *Independent Military Review*. No. 42. P.7 (In Rus.).

Harley I.A. (1996). Role of Information Warfare. Truth and Myths. USA.

Hoffman F.G. (2005) Future Warfare: The Rise of Hybrid Wars. USA. P. 18–19.

Hoffman F.G. (2006). How Marines are Preparing for Hybrid Wars. *Armed Forces Journal*. JFQ: Joint Force Quarterly. P. 34–48.

Jajodia S., Shakarian P., Subrahmanian V.S., Swarup V., Wang C. (ed.) (2015). Cyber Warfare: Building the Scientific Foundation. Springer Int. Publishing.

Komov S.A. (1996). Information warfare in modern war: theory issues. *Military thought*. No. 3. P. 73 (In Rus.).

Kostyukhin A., Gorbunov G. (2007). Information operations in the plans of the US Armed Forces. *Foreign Military Review.* No. 5. P.14 (In Rus.).

Krynina O.Y. (2009). Definitions of the Concept of 'Information War': analysis of Russian and foreign experience. *The New Technologies.* No. 3. P. 68-70 (In Rus.).

Libicky M.C. (2009) Cyberdeterrence and Cyberwar [electronic source]: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf. RAND, USA.

Mann S.R. (1997). The Reaction to Chaos. In: Complexity, Global Politics, and National Security / ed. by David S. Alberts and Thomas J. Czerwinski. National Defense University, Washington, D.C.

Manoilo A.V., Petrenko A.I., Frolov D.B. (2003). State information policy in the context of information-psychological warfare. Moscow (In Rus.).

Panarin I.N. (2006). Information War and Geopolitics. Moscow (In Rus.).

Pirumov V.S., Rodionov M.A. (1997). Some aspects of information warfare in military conflicts. *Military thought*. No. 5. P. 44-47 (In Rus.).

Pocheptsov G.G. (2006). Information wars. Moscow (In Rus.).

Rastorguev S.P. (1998). Information warfare. Moscow (In Rus.).

Tsymbal V.I. (1995). On the concept of information war. *Security*. No. 9. P. 35 (In Rus.).