Виловатых А.В.,
Михеев Е.А.

СТРАТЕГИЧЕСКИЕ УСТАНОВКИ США И НАТО ПО ОРГАНИЗАЦИИ И ПРОВЕДЕНИЮ ОПЕРАЦИЙ ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОГО ВОЗДЕЙСТВИЯ

STRATEGIC INSTALLATIONS OF THE USA AND NATO ON THE ORGANIZATION AND CARRYING OUT OPERATIONS OF INFORMATION AND PSYCHOLOGICAL INFLUENCE

Виловатых Анна Вячеславовна, кандидат политических наук, старший научный сотрудник Российского института стратегических исследований, e-mail: vilkavulkan@yandex.ru
Михеев Евгений Александрович, аспирант Института психологии РАН, e-mail: mih-news@mail.ru
Vilovatykh Anna, PhD of political sciences, senior research associate of the Russian institute of strategic researches, e-mail: vilkavulkan@yandex.ru
Mikheyev Evgeny, post-graduate student of Institute of psychology of RAS, e-mail: mih-news@mail.ru

Аннотация. В данной статье исследованы некоторые научные разработки американских ученых в сфере информационно-психологического воздействия. На основе анализа стратегических документов США и военного альянса НАТО предпринята попытка выявить тенденции использования информационно-коммуникационных технологий в военно-политических целях.
Abstract. In this article some scientific developments of the American scientists in the sphere of information and psychological influence are investigated. On the basis of the analysis of strategic documents of the USA and military alliance NATO an attempt to reveal tendencies of use of information and communication technologies in the military-political purposes is made.

Ключевые слова: информационно-коммуникационные технологии, информационно-психологическое воздействие, информационные операции, психологические операции, США, НАТО, безопасность.
Key words: information and communications technologies, indoctrination, information operations warfare, psychological operations, USA, NATO, security.

Наблюдаемая в последние годы тенденция увеличения частоты и доли применения информационно-коммуникационных технологий (ИКТ) в военно-политических целях привела к совершен-

ствованию процессов использования информации посредством ресурсов телекоммуникации и вычислительной техники. Появились новые виды средств массовой коммуникации (Интернет, социальные сети и блоги), где апробируются методы информационно-психологического воздействия на общественное сознание. В данный процесс вовлечены легитимные и нелегитимные политические акторы, и в этой связи обеспечение национальной безопасности становится все более сложной и многоаспектной деятельностью.

Учитывая тот факт, что современные ИКТ рассматриваются участниками мировой политики (в частности, США и НАТО) в качестве инструмента раскачки военно-политической ситуации в отдельной стране или целом регионе, целесообразным представляется проанализироватьроль и место операций информационно-психологического воздействия в американских стратегических документах, равно как и документах Североатлантического альянса.

К терминологии

В документах Минобороны США под *информационной операцией* понимается интегрированное использование определенных возможностей и действий, поддерживаемых разведкой для воздействия на лиц, принимающих решения со стороны противника, для достижения или продвижения особых целей.

Информационные операции включают: обман, психологические операции, электронное противоборство, физические атаки и/или разрушения, специальные информационные операции, в том числе компьютерные сетевые операции.

В работе «Что такое информационное противоборство?» специалист американской корпорация RAND Мартин Либики предложил, как представляется, оптимальную классификацию методов информационно-психологического воздействия. К ним относятся:

— борьба с системами управления;
— информационно-разведывательные операции;
— электронное противоборство;
— «хакерское» и кибернетическое противоборство;
— экономическое информационное противоборство;
— психологическое противоборство;

Рассмотрим данные приемы более подробно.

Борьба с системами управления — военная стратегия с применением информационной среды на поле боя, направленная на физическое разрушение командной структуры противника.

Информационно-разведывательные операции — операции, в результате которых полученные сведения о целеуказании или нанесенном военном ущербе поступают непосредственно участникам операции. Проводятся с помощью автоматизированных систем, которые, в свою очередь, являются потенциальными объектами атак методов борьбы с системами управления. В связи с этим выделяются «наступательные» и «оборонительные» информационно-разведывательные операции.

Электронное противоборство — военные действия, включающие использование электромагнитной и направленной энергии для контроля электромагнитного спектра и/или атака противника. Состоит из трех подразделений: электронная атака, защита и поддержка электронного противоборства.

Экономическое информационное противоборство — применение информационно-технических средств и методов борьбы для установления контроля, воздействия и дестабилизации экономическо-финансовой системы государства или ее отдельных элементов. Выделяются две формы: информационная блокада и информационный империализм.

Хакерское и кибернетическое противоборство — разновидность вооруженной борьбы, в ходе которой осуществляется целенаправленное и организованное воздействие аппаратно-программными средствами на аппаратно-программные комплексы автоматизированных систем управления военного и гражданского назначения противника, направленное на нарушение их нормального функционирования.

В качестве примера кибернетической операции может служить кибератака на ядерные объекты Ирана в 2008 года с помощью вредоносной программы Stuxnet. Одной из задач Stuxnet являлось получение дополнительной информации о функционировании основных узлов этих стратегических объектов, которая впоследствии могла быть использована для нарушения или остановки процесса работы оборудования. По некоторым данным, атака была тщательно спланирована и подготовлена специальными службами США и Израиля.

Психологическое противоборство — способы ведения военных операций, оказывающие воздействие на психическое состояние человека. Специалисты RAND выделяют 4 объекта такого воздействия: структуры государственного управления, структуры военного командования, морально-психологическое состояние личного состава, культура.

Таким образом, американские исследователи дают весьма подробную терминологию операций по ведению информационно-

го противоборства. Не менее детальной в их наработках выглядят технологии проведения такого рода операций.

Операции информационно-психологического воздействия: взгляд зарубежных исследователей

В 2016 г. американские специалисты по информационной безопасности Facebook подробно описали этапы проведения информационных операций посредством потенциала социальных сетей:

— *целенаправленный сбор данных (Targeteddatacollection)* — хищение, а зачастую разглашение не публичных сведений, которые могут способствовать извлечению выгоды в политическом дискурсе;

— *создание контента (Contentcreation),* «фэйкового» или настоящего через информационного оператора, либо путем распространения историй журналистами и другими третьими лицам, в том числе «фэйковыми пользователями».

— *усиление лжи (Falseamplification)* — скоординированная деятельность фэйковых аккаунтов с целью манипуляции политическим дискурсом (например, недопущение для участия в политическом диалоге представителей определенных политических партий, усиление сенсационности одной информации над другой и пр.).

Симптоматично, но с проведением подобного рода исследований, страны Запада все чаще пытаются обвинить Россию во вмешательстве с применением ИКТ в политические процессы ряда стран. Широко обсуждаются формы пропаганды, дезинформации и гибридных операций, инициатором которых якобы выступают подконтрольные российской власти политические акторы.

Так, например, в 2016 г. исследователи американской корпорации RANDK. Пол и М. Мэтьюз опубликовали материал под названием «Российская модель пропаганды: пожарный шланг с потоками лжи».

По мнению аналитиков, отличительной особенностью «пропаганды Кремля» являются: большой объем информации и многоканальность; скорость, непрерывность и повторение; отсутствие освещения объективной реальности; отсутствие логики и последовательности. Целями воздействия, как отмечают авторы документа, являются изменение норм и ценностей западного общества, дестабилизация политической обстановки.

Несмотря на привязку указанного выше исследования к определенной стране, выводы авторов данной работы схожи с результатами социально-психологических исследований, посвященных

ИПВ в социальных сетях в целом. Так, например, эффект множественности источников заключается в том, что различные аргументы от разных пользователей воспринимаются личностью как более весомые, чем один и тот же аргумент от разных источников или разные аргументы от одного пользователя.

Ученые уже давно установили, что феномен множественности источников имеет конкретные предпосылки: во-первых, большее количество материалов повышают интерес у целевой аудитории и вероятность привлечения других потенциальных аудиторий; во-вторых, при необходимости большее количество сообщений может затмить другую информацию; в-третьих, множественность каналов распространения увеличивает эффективность усваивания информации; в-четвертых, получение информации из множества источников повышают уровень доверия к информации, особенно если адресант идентифицирует себя с источником информации.

В ходе недавнего исследования социальной сети Facebook в Италии было установлено, что вне зависимости от страны распространения пользователи чаще комментируют и ставят «лайки» в конспирологических новостях, чем в научных. Внимание общественности привлекают такие формы подачи информации как «мемы». Это продемонстрировано в сводной таблице ниже.

Таблица 1.

	Всего	**Наука**	**Конспирология**
Страницы	73	34	39
Посты	271,296	62,705	208,591
Лайки	9,164,781	2,505,399	6,659,382
Комментарии	1,017,509	180,918	836,591
Поддерживает	17,797,819	1,471,088	16,326,731
Те, кому понравилось	1,196,404	332,357	864,047
Комментаторы	279,972	53,438	226,534

Также исследователи обнаружили, что распространяемая в период экономических трудностей, социально-политической нестабильности и предвыборных кампаний альтернативная информация, а также информация, содержащая выражение недовольства к принятию решений правительством, имеют наибольший эффект воздействия на пользователей социальных сетей, особенно тех, кто изначально не доверял официальным государственным средствам массовой информации (СМИ).

Помимо научных и аналитических разработок, посвященных использованию ИКТ в военно-политических целях, все большая роль

информационным, психологическим и кибероперациям отводится в официальных документах США и НАТО.

Документальный массив организации и проведения операций информационно-психологического воздействия

Термин «информационные операции» используется в официальных американских документах уже длительное время. Благодаря разработке и последующему редактированию концепции информационных операций были уточнены цели, задачи и основные принципы информационно-психологического воздействия, а также разработаны обязанности должностных лиц по подготовке и проведению информационных и психологических операций — как в мирное, так и в военное время.

В Доктрине психологических операций, выпущенной в 2003 г. под эгидой Комитета начальников штабов ВС США, приводится концепция *информационных операций (ИО)*. Она включает три вида ИО: стратегические, операционные и тактические.

К *стратегическим ИО* относится международная информационная деятельность, направленная на изменение отношений, восприятия и поведения иностранных государств с выгодных для США позиций.

Операционные ИО проводятся одновременно с военными операциями в определенном регионе с целью поддержания кампаний и стратегий Объединенных командных сил.

Тактические ИО проводятся одновременно с военными операциями для поддержки тактической миссии против сил противника.

В 2007 г. разработки американских специалистов нашли отражение в Доктрине психологических операций НАТО, где выделены три вида психологических операций: стратегические психологические операции, психологические операции в рамках операций в кризисных ситуациях, боевые психологические операции.

Стратегические психологические операции (СПО) (Strategic-psychologicaloperations (SPO) — это высокий уровень (уровень национальных правительств). СПО направлены на аудитории дружественные и нейтральные, а также на вероятных или явных противников альянса. Термин «страны» в рамках СПО имеет более широкое понятие и включает отдельные группы внутри страны, например религиозные оппозиционные официальному правительству группы. Цели СПО являются долгосрочными и носят политический характер; они направлены на подрыв готовности явно-

го или вероятного противника к конфликту, вооруженной борьбе и возможности получения поддержки от дружественных или нейтральных альянсу аудиторий населения.

Психологические операции в рамках операций в кризисных ситуациях (ПОКС) (Crisisresponsepsychologicaloperations (CRPO) — ПОКС проводятся на оперативном и тактическом уровнях, ответственность за их проведение несет командование НАТО. ПОКС являются составными частями военных операций, которые направлены на достижение стратегических целей. ПОКС проводятся в объединенном операционном районе (Jointoperationsarea) и направлены на одобренные целевые аудитории с целью создания благоприятных условий для сил НАТО и поддержки готовности этих аудиторий к сотрудничеству. Цели ПОКС — оказание помощи при выполнении поставленных задач и организация защиты сил.

Боевые психологические операции (БПО) (Combatpsychologicaloperations (CPO) — БПО проводятся наоперативном и тактическом уровнях. Они находятся в зоне ответственности командования НАТО, планируются и проводятся в соответствии со стратегическими целями Альянса. ПОКС проводятся с целью понижения уровня боеспособности противника, подавления его воли и обеспечения условий оперативной свободы командованию Альянса.

В 2014 г. Доктрина психологических операций НАТО доработана специалистами из Великобритании в части, касающейся определения понятия «стратегическая коммуникация», «аттрибуции». Особый интерес вызывает пункт 0109, так называемый «раздел повышения эффективности планирования операций с учетом специфики целевой аудитории».

В новой редакции, в частности, дается определение анализу целевой аудитории, как систематическому изучению социальных групп с целью улучшения понимания и определения доступности, уязвимости и восприимчивости к поведенческому и установочному воздействию. Кроме того, там отмечается, что информация, получаемая из Интернета, относится к самому «низшему» уровню анализа.

Между тем, недавние социально-психологические исследования демонстрируют следующее: «компьютерные оценки людей, основанные на цифровых следах, более точны и достоверны, чем суждения, сделанные их близкими или знакомыми (друзьями, семьей, супругом, коллегой и пр.)». Как отмечают ученые, апробировавшие данные исследования на практике, личностные характеристики пользователей социальных сетей могут выявляться автоматически специальной программой без участия человека.

Одновременно с утверждением Доктрины психологических операций НАТО 2014 г. произошло объединение ответственных за проведение психологических операций специальных подразделений вооруженных сил Великобритании. В частности, в состав 77-ой бригады британских сил была включена 15-я группа психологических операций. Ранее группа выполняла задачи на территории Афганистана в провинции Гильменд, занималась воздействием на политические убеждения местных жителей относительно власти в регионе. Для ИПВ был использован канал СМИ (в основном радио), формы массовых культурных и театрализованных мероприятий (ток-шоу, представления) и печатаные текстовые формы наглядной агитации и плакатов.

В новой *Доктрине психологических операций НАТО 2016 г.* описываются цели информационно-пропагандистского сопровождения военной деятельности альянса, которые достигаются в ходе информационно-психологических операций и включают решение трех взаимосвязанных задач. К ним относятся:

— изменение мировоззрения и формирование требуемой линии поведения целевых аудиторий (InfluenceActivity);

— защита собственной информации (InformationProtection-Activity); дезорганизацию системы управления противника (CounterCommandActivity).

Особое внимание в документе уделено такому методу ИПВ, как общественная дипломатия. Субъектами воздействия общественной дипломатии являются политические лидеры, парламентарии, журналисты, научные и экспертные сообщества, неправительственные организации, учащаяся молодежь и другие социальные группы в районах применения войск (сил) альянса и за их пределами. Данная деятельность направлена на формирование «правильного понимания» целевыми аудиториями политики и практических шагов НАТО в интересах поддержания стабильной обстановки, исключающей проявления враждебности со стороны местного населения по отношению к военнослужащим коалиционных группировок.

Таким образом, командование Организации Североатлантического договора предусматривает широкий спектр ИПВ на противника с применением потенциала ИКТ, причем далеко не в мирных целях. Тем не менее, исходя из многочисленных принятых концепций, стратегий, доктрин передовиками достижения военно-политических целей посредством ИКТ будут, видимо, непосредственно американцы.

В *Киберстратегии Минобороны США 2015 г. (TheDoDCyber-Strategy)* отмечается, что в период с 2013 по 2015 г. главной стра-

тегической угрозой для страны являлась киберугроза. С целью минимизации рисков и защиты интересов Соединенных Штатов в этой сфере, национальное военное ведомство определило главные стратегические задачи на перспективу:

— создание киберсил и поддержание их готовности и способности выполнять операции в киберпространстве;

— защита информационной сети МО США, обеспечение безопасности баз данных МО США, минимизация рисков в ходе выполнения МО США задач;

— поддержание готовности защищать страну и отстаивать жизненно важные интересы от подрывных и разрушительных кибератак;

— создание, поддержание киберопций и плана по их использованию для контроля за эскалацией конфликта и регулирования конфликтной среды на всех этапах его развития;

— создание и поддержание прочных международных альянсов и партнерств с целью нейтрализации общих угроз и повышения международной безопасности и стабильности.

В Киберстратегии также обозначено, что созданные киберсилы США разделяются на три группы: подразделения киберзащиты (защита информационной инфраструктуры Министерства обороны), подразделения государственной обороны (защита государства и государственных интересов от атак высокого уровня) и боевые подразделения. Кроме этого, более четкое оформление получили концептуальные основы сдерживания в киберпространстве.

В рамках реализации данной стратегии проводятся постоянные проверки и совершенствование адаптивного механизма управления, контроль за проведением кибероперациий. В 2016 году Агентством перспективных оборонных исследований и разработок (DARPA) МО США был реализован проект Plan-X по созданию полуавтоматической системы, позволяющей упростить использование вредоносных программ и снизить требования к квалификации обслуживающего персонала. Единая архитектура АПК и интерфейса позволяет объединять множество вредоносных программ, разрабатываемых сторонними организациями. В мае 2016 года система была испытана в ходе учений CyberGuard и CyberFlag, и внедрена в работу Киберкомандования США в 2017 г.

В *Стратегии национальной обороны США 2015 г.* отмечена тенденция к изменению на современном этапе характера вооруженной борьбы. Обращается внимание на так называемые «гибридные войны», которые содержат элементы «классических» войн и действий повстанческих сил, партизанских формирований и Сил специальных операций (ССО).

В Концепции развития ССО Сухопутных войск США предпочтение также отдается принципу непрямого воздействия на противника, который подробно раскрыт в Концепции политической войны (PoliticalWarfare) и включает следующие методы:

— поэтапное введение экономических санкций;

— принятие дипломатических мер;

— поддержка правительства дружественного государства представлением ему необходимой разведывательной информации;

— ведение психологической борьбы.

В рамках концепции определены угрозы: регулярные вооруженные силы государства-противника (специальные войска и силы общего назначения), государственные военизированные формирования (силы внутренней безопасности, полиция, пограничные войска), повстанческие группировки, партизанские формирования, преступные группировки (в том числе хакеры).

В *Стратегии национальной безопасности США, выпущенной администрацией Д. Трампа в декабре 2017 г.,* также большое внимание уделяется ведению боевых действий в киберпространстве. По утверждению американских стратегов, кибератаки теперь объективно являются главной особенностью современных военных конфликтов. Особо отмечается, что ряд стран рассматривают кибервозможности в качестве инструментов информационного влияния, а некоторые государства используют киберинструменты для защиты и расширения своей «зоны ответственности».

Приоритетными направлениями в документе при обеспечении кибербезопасности Америки указаны:

— инвестирование в средства поддержки и атрибуции кибератак с целью повышения скорости реагирования.

— повышение эффективности киберинструментов для охвата всего спектра конфликтной среды, защиты критической инфраструктуры США, обеспечения безопасности баз данных и информации.

Минобороны США и подчиненные военные ведомства планируют набор и обучение личного состава для выполнения задач в данном направлении.

Открытая часть новой *Стратегии национальной обороны США, опубликованной в январе 2018 г.,* обращает усиленное внимание на ведение в перспективе боевых действий в киберпространстве [и космосе]. Одновременно американская военная доктрина ставит в приоритет сдерживание России и Китая, настаивая в этой связи на существенном увеличении расходов на перспективные системы вооружений. В случае реализации такая документально подкрепленная оборонная политика американцев будет пред-

ставлять серьезную угрозу безопасности Российской Федерации, как впрочем, и другим государствам мирового сообщества.

В целом, проведенный в статье анализ свидетельствует, что государства Запада отводят особое место операциям информационно-психологического воздействия для достижения собственных военно-политических целей. Для этого активно применяются современные информационно-коммуникационные технологии. Разработаны соответствующие методики, позволяющие получить информацию о социально-психологических характеристиках населения, настроениях отдельных социальных групп с целью в перспективе смоделировать развитие социально-политической обстановки с учетом интересов субъекта управления.

В ряде концептуальных документов США и Североатлантического альянса отмечается, что киберпространство является новой сферой ведения боевых действий. В рамках реализации государственных программ и стратегий создаются регулярные воинские формирования, специализирующиеся на информационных, психологических и кибероперациях. Продолжает увеличиваться число специальных операций по принципу непрямого воздействия с использованием методов санкций, публичной дипломатии, психологической борьбы.

С учетом сказанного выше важным представляется противодействовать действиям Вашингтона по продвижению американской концепции о неизбежности возникновения конфликтов в информационном пространстве при отсутствии минимального корпуса норм международного права, регламентирующего использование информационно-коммуникационных технологий в военных целях. Очевидно, что такие стратегические установки и политика их реализации нанесут непоправимый урон системе международной безопасности и поставят под сомнение хрупкую стратегическую стабильность.

Библиографический список

1. *Газетов В., Хоменко В.* Группа захвата умов. Британия концентрирует силы на информационном фронте // Военно-промышленный курьер, 28 марта 2016 URL: https://vpk-news.ru/articles/29958 (дата обращения 22.01.2018).
2. *Карасев П.А.* США наращивают киберсилы // Журнал «Эксперт», январь 2018. URL: http://expert.ru/2017/08/2/ssha-naraschivayut-kibersilyi/ (дата обращения 22.01.2018).
3. Проблемы информационной безопасности в международных военно-политических отношениях. Под ред. А.В. Загорского, Н.П. Ромашкиной.

М.: ИМЭМО РАН, 2016, С. 48. URL: https://www.imemo.ru/index.php?page_id=645&id=3499 (дата обращения 21.01.2018).
4. Allied Joint Doctrine for Psychological Operations. AJP-3.10.1 (A) October, 2007. URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf. (дата обращения 21.01.2018).
5. Allied Joint Doctrine for Psychological Operations. AJP-3.10.1. September, 2014. URL: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/450521/20150223-AJP_3_10_1_PSYOPS_with_UK_Green_pages.pdf (дата обращения 22.01.2018).
6. *Bessi A., Petroni F., Del Vicario M. et al.* Viral misinformation: The role of homophily and polarization // Proceedings of the 24th International Conference on World Wide Web Companion 18 May 2015. P. 355–356. URL: https://arxiv.org/abs/1411.2893 (датаобращения 21.01.2018).
7. *Carpenter D., Ko M.* Online astroturfing: A theoretical perspective // Proceedings of the Nineteenth Americas Conference on Information Systems, Chicago, Illinois, August 15–17, 2013. URL: https://www.researchgate.net/profile/Darrell_Carpenter/publication/286729041 (дата обращения 21.01.2018).
8. *Harkins G.S., Szymanski K.* Social Loafing and Self-Evaluation with a social standard. Journal of Personality and social psychology. USA, 1987. URL: https://pdfs.semanticscholar.org/65c6/162ff35fc61ea7b59945858f1235e80cdbc3.pdf (дата обращения 21.01.2018).
9. *Harkins, S. G., Petty, R. E.* «The multiple source effect in persuasion,» Personality and Social Psychology Bulletin 1981a. URL: http://journals.sagepub.com/doi/abs/10.1177/014616728174019 (дата обращения 21.01.2018).
10. Joint Publication 1-02. Department of Defense Dictionary of Military and Associated Terms 8 November 2010. URL: https://fas.org/irp/doddir/dod/jp1_02.pdf. (дата обращения: 14.01.2018).
11. Joint Publication 3-53. Doctrine for Joint Psychological Operation. 5 September 2003. URL: https://www.hsdl.org/?abstract&did=472329. (дата обращения 21.01.2018).
12. National Security Strategy of the United States of America. December, 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения 22.01.2018).
13. Summary of the 2018 National Defense Strategy // US Department of Defense, December, 2017. URL: https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (дата обращения 22.01.2018).
14. The Department of Defense Cyber Strategy, April, 2015. URL: https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (дата обращения 22.01.2018).
15. *Weedon J., Nuland W., Stamos A.* Information Operations and Facebook. April 27, 2017. Facebook, Inc., 2017. URL: https://fbnewsroomus.files.wordpress.com/2017/04/facebook-and-information-operations-v1.pdf (дата обращения 21.01.2018).
16. *Youyou W., Kosinski M., Stillwell D.* Computer-based personality judgments are more accurate than those made by humans. PNAS. January 27, 2015. URL: http://www.pnas.org/content/112/4/1036.full (дата обращения 22.01.2018).
17. *Zhang J.,* Paul C., Matthews M. The Russian «Firehose of Falsehood» Propaganda Model. URL: https://www.rand.org/pubs/perspectives/PE198.html (дата обращения 21.01.2018).