■ ■ Место интернет-коммуникациив практике информационного противоборства

Яблонских А.В.¹, Дробышев Д.В.², Чаленко Д.А.¹

1. Российский университет дружбы народов (РУДН), Москва, Российская Федерация. 2. Московский государственный технический университет (МГТУ) имени Н.Э. Баумана, Москва, Российская Федерация.

Аннотация. В статье представлен авторский анализ исторических и современных подходов к определению понятия «информационные войны» и к инструментарию их ведения. Исследованные в материале системы классификации были учтены при проведении структурированного контент-анализа кейсов информационных войн в России и за рубежом. В качестве ключевого маркера контент-анализа были выбраны интернет-технологии (цифрового и социального характера), их значение в различных типах информационных войн. Авторами выдвинута и подтверждена гипотеза об интенсификации практики информационных войн в условиях развития интернеткоммуникаций, при этом необходимо отметить, что рожденные в интернет-среде технологии (как цифровые, так и социальные) могут являться как инструментом нападения, так и средством защиты в современной информационной войне.

Ключевые слова: информационное противоборство, информационная война, информационные конфликты, контент-анализ, интернет-технологии

Для цитирования: Яблонских А.В., Дробышев Д.В., Чаленко Д.А. Место интернет коммуникации в практике современного информационного противоборства // Коммуникология. 2023. Том 11. № 2. С. 28-39. DOI 10.21453/2311-3065-2023-11-2-28-39.

Сведения об авторах: Яблонских Андрей Викторович – кандидат филол. наук., доцент кафедры массовых коммуникаций РУДН. Адрес: 117198, Россия, г. Москва, ул. Миклухо-Маклая, 6. E-mail: yablonskikh-anv@rudn.ru. Дробышев Дмитрий Вадимович – начальник управления международного научно-образовательного сотрудничества МГТУ им. Н.Э. Баумана. Адрес: 105005, Россия, г. Москва, ул. 2-я Бауманская, 5/1. E-mail: d.v.drobishev@gmail.com. Чаленко Даниил Анатольевич – аспирант филологического факультета РУДН. Адрес: 117198, Россия, г. Москва, ул. Миклухо-Маклая, 6. E-mail: chalenko.da@gmail.com.

Статья поступила в редакцию: 25.04.2023. Принята к печати: 07.06.2023.

Введение. Явление информационных войн в современной научной и отраслевой литературе исследуется уже более 20 лет. Первые публикации о сути информационной войны, ее причинах и инструментарии проведения в российских источниках появились еще в 90-ые годы XX века [Володенков]. В материале авторами рассмотрены и структурированы современные подходы к определению понятийного аппарата информационных войн и технологий их ведения.

Ретроспективный анализ развития теории и практики информационных войн по сути можно вести с трудов Н. Макиавелли («Государь») или Сунь Цзы («Искусство войны»), но лишь в последние 10-15 лет развитие социальных и информационных технологий привели к скачку технологической основы и инструментальной базы их ведения [Чумиков].

Понятие «информационной войны». Понятия информационного противоборства и информационной войны не являются новым и являются предметом исследований многих авторов [Володенков; Манойло; Панарин; Цыганов; Libicki, и др.]. Существенными для понимания феномена информационного противоборства также являются работы в области теории и практики пропаганды [Conserva; Лассуэлл], теории коммуникации, массмедиа [Lasswell; Rogers; Rubin & Windhall; Шарков; Коломиец, и др.], и других смежных направлений.

Для проведения структурного анализа понятия информационной войны в качестве базового определения было выбрано наиболее универсальное: Информационная война – это противоборство сторон посредством распространения специально подготовленной информации и противодействия аналогичному внешнему воздействию на себя¹.

Данная трактовка менее комплексная, чем например распространенное в настоящее время в определение А.В. Манойло, который относит к информационному противоборству «любые формы социальной и политической конкуренции, в которых для достижения конкурентного преимущества предпочтение отдается средствам и способам информационно-психологического воздействия» [Манойло]. Понятие информационного противоборства включает в себя весь спектр конфликтных ситуаций в информационно-психологической сфере — от межличностных конфликтов до открытого противостояния социальных систем. Информационно-психологическая война — это, безусловно, также один из видов информационного противоборства» [Там же].

Выбор более простой трактовки в рамках этого по сути прикладного исследования связан с трансформацией пространства ведения информационных войн и появлением новых практик управления информацией. Учитывать эти факторы, отталкиваясь от сложного, комплексного определения объекта управления, крайне сложно, так как комплексность неизбежно накладывает ряд ограничений любые исследования [Василенко, Игнатченко].

Характеристики информационной войны. Изменения в практиках ведения информационных войн и модификация их инструментария носит на сегодняшний день не эволюционный, а скорее революционный характер. С нашей точки зрения, ключевое значение в столь значительном ускорении сыграла глобальная

¹ Информационная война // Википедия [эл. pecypc]: https://ru.wikipedia.org/wiki/Информационная_война (дата обращения 20.03.2023).

сеть, причем не только и не столько как технологическое, сколько как социальное явление. В рамках анализа столь быстрых, интенсивных и комплексных преобразований, авторы отталкивались от трех базисных принципов:

- 1. Степень и скорость изменения инструментов и технологий ведения информационных войн напрямую коррелирует с их классификацией, поскольку в условиях информационной экономики и так называемой «новой нормальности», комплексность данного понятия не позволяет сформулировать единые универсальные подход к оценке эффективности инструментария.
- 2. В рамках исследования и анализа необходимо дискретно учитывать социально-политическую и социально-экономическую сферы ведения информационных войн, в силу того, что несмотря на всё большее сопряжения экономических и социально-политических процессов, реализация интегральной, единовременной оценки двух данных полей информационных военных действий, может привести к потери причинно-следственных связей, что, безусловно, скажется на чистоте анализа.
- 3. Исследования инструментария ведения информационных войн необходимо так же проводить с учетом страновой специфики. Данный принцип связан с развитием различных школ коммуникационного менеджмента в США, России, Европе и на Востоке, отличающимися подходами к основам социальной инженерии и возможности использования информационных технологий в социальных процессах.

Как уже было отмечено, интернет явился катализатором ускорения развития инструментария ведения информационных войн в последние 5-10 лет. И на первой стадии оценки «информационного вооружения» нами была поставлена задача провести контент-анализ влияния интеренет-инструментария на развитие различных типов информационных войн, в соответствии с четырьмя классификационными признаками.

Американский ученый Мартин Либики [Libicki] определяет семь видов информационной войны:

- Командно-управленческая ставит перед собой цель лишить контроля налаженную связь между командованием и исполнителем.
- Разведывательная война предусматривает сбор ценной информации для нападения и собственной защиты.
- Электронная война целью является вывод из строя всех электронных коммуникаций.
- Психологическая война пропаганда и информационное зомбирование населения.
- Хакерская война взлом и доступ к любым данным (электронная почта, банковские карты, личные файлы, переписки и так далее) и несанкционированное их использование.
- Экономическая война информационная блокада (ограничение коммерческой деятельности) или информационный империализм (политическая информационная атака).

• Кибервойна – ставит перед собой цель захватить компьютерные данные, выследить объект, нарушить работу инфраструктуры, полагающейся на информационные технологии.

По сфере ведения информационных военных действий эксперты выделяют [Панарин]:

- вооруженная, сопровождающая вооруженные конфликты как их «холодное обрамление»;
- торгово-маркетинговая, предмет которой позитивный или негативный имидж товаров, услуг, фирм, компаний и т. п.;
 - политическая как особая форма информационного политического конфликта;
- культурологическая, суть которой состоит в информационной борьбе за навязывание культурных образцов, норм и ценностей.

Не менее важным признаком классификации информационных войн является различие подходов в зависимости от предмета конфликта [Ласуэлл]:

- психологическая информационная война, предмет конфликта в которой психика населения противника;
- коммуникационная информационная война, предмет борьбы в которой система информационных коммуникаций;
- собственно информационная, предмет конфликта в которой собственно борьба за обладание информацией;
- ценностная информационная война, предмет борьбы в которой различные политические, духовные, этические, эстетические и другие ценности.

Наконец, еще одним значимым критерием классификации являются особенности типа конфликта [Сулейманова, Назарова]:

- информационная агрессия разрушение информационной системы противника и быстрое навязывание своей системы ценностей;
- информационная экспансия длительное эволюционное воздействие своими информационными средствами и потоками на противника в целях его подчинения;
- информационно-психологическая гражданская война информационно-психологическое противоборство между различными социальными группами общества.

Результаты исследования. Приведенные системы классификации были учтены при проведении структурированного контент-анализа кейсов информационных войн в России и за рубежом. В качестве ключевого маркера контентанализа были выбраны интернет-технологии (цифрового и социального характера), их значение в различных типах информационных войн, а также используемые технологии и носители информации.

На первой стадии была определена степень вовлечения интернет-технологий с детализацией их использования. В качестве ключевых носителей информации были выбраны следующие:

• (псевдо)новостной контент (фейковые новости) в web;

- лонгриды / расследования;
- социальные сети / мессенджеры;
- блогерский контент (ЛОМы);
- дубль-порталы;
- маркетплейсы;
- блокчейн-технологии.

Авторами было проанализировано более 80 российских и зарубежных кейсов, контент-таблица на выходе включает в себя как шкалу измерения влияния интернет-технологий, так и систему конкретных инструментов (Таблица 1).

На втором этапе были детально рассмотрены три кейса, отражающих использование интернет-технологий для ведения информационных войн различного типа. В качестве наиболее показательных примеров, выбраны варианты противостояний, где интернет выступил, как технологической основой, так и площадкой для ведения информационной войны, более того, в большей части основной контекст предмета информационных конфликтов так же связан с интернет-экономикой и интернет-социологией.

Первый анализируемый кейс – противостояние корпорации Apple и компании Epic Games – производителя сверхпопулярной игры Fortnite в 2020 году. Классическое торгово-маркетинговое противостояние, смещенное за счет информационного инструментария в категорию ценностной войны. Конфликт, развитый вокруг так называемого «яблочного налога» – существенного процента, который корпорация Apple берет с разработчиков, размещаемого в Apple Store программного обеспечения сформирован по модели борьбы «малой независимой компании, стремящейся отстоять свободы разработчиков» с «крупной корпорацией – монополистом». В ходе войны компании применяли как стандартные рыночные технологии, свойственные скорее классическим маркетинговым войнам (диверсификация каналов продаж с одной стороны и перекрытие рыночных ниш – с другой), так и инструментарий современных информационных конфликтов, доступный для компаний. Показательным и интересным видится ролик выпущенный компанией Epic Games, обыгрывающий антиутопию Джорджа Оруэлла «1984» и являющийся по сути калькой с знаменитой, выпущенной к выходу первого компьютера Macintosh рекламы самой Apple. В ролике Apple, снятом Ридли Скоттом ненавистную роль «Большого брата» сыграла корпорация IBM, в видео от Epic Games позиция антагониста – диктатора досталась самой «яблочной корпорации». Столь эффектно выстроенная параллель обеспечила видео максимальную виральность, что безусловно является важным факторов ведения информационной войны и было бы невозможно без современных интернет-технологий.

Следующий, разобранный авторами исследования кейс среди десятков других примечателен интеграцией информационной и технологической составляющих. С одной стороны – данный пример можно отнести к классическому кейсу кибервойны или кибератаки, с другой – атакующая сторона опиралась на маркетинговые основы – быстро растущий канал продаж маркетплэйса, а так же реа-

Коммуникология. 2023. Том 11. № 2. С. 28-39

Таблица 1. Виды информационных войн, влияние интернет технологий и носители информации (составлено авторами) / Types of information wars, the impact of Internet technologies, and the media

Система (признак) классификации	Виды информационных войн	Степень интеграции интернет-технологий	Носители информации
Целевая ориентация	Командно- управленческая	Средняя	блогерский контент;дубль-порталы;блокчейн-технологии.
	Разведывательная	Высокая	 блогерский контент; социальные сети / мессенджеры; дубль-порталы; маркетплейсы; блокчейн-технологии.
	Электронная	Средняя	социальные сети / мессенджеры;дубль-порталы;маркетплейсы;блокчейн-технологии.
	Психологическая	Высокая	• (псевдо)новостной контент; • лонгриды / расследования; • социальные сети / мессенджеры.
	Хакерская	Высокая	• социальные сети / мессенджеры; • дубль-порталы; • блокчейн-технологии.
	Экономическая	Средняя	• (псевдо)новостной контент; • лонгриды / расследования; • социальные сети/мессенджеры; • дубль-порталы; • маркетплейсы; • блокчейн-технологии.
	Кибервойна	Высокая	 блогерский контент; социальные сети / мессенджеры; дубль-порталы; блокчейн-технологии.

Продолжение табл. 1

Система (признак) классификации	Виды информационных войн	Степень интеграции интернет-технологий	Носители информации
Сфера ведения «ин- формационных воен- ных действий»	Сопровождение воо- руженных конфликтов	Средняя	(псевдо)новостной контент; лонгриды / расследования; блогерский контент; дубль-порталы; блокчейн-технологии.
	Торгово- маркетинговая	Высокая	(псевдо)новостной контент; лонгриды / расследования; блогерский контент; социальные сети / мессенджеры; дубль-порталы; маркетплейсы; блокчейн-технологии.
	Политическая	Высокая	(псевдо)новостной контент; лонгриды / расследования; блогерский контент; социальные сети / мессенджеры; дубль-порталы.
	Культурологическая	Средняя	лонгриды/расследования; блогерский контент; социальные сети / мессенджеры;
Предмет конфликта	Психологическая	Высокая	(псевдо)новостной контент; блогерский контент; социальные сети / мессенджеры.
	Коммуникационная	Средняя	(псевдо)новостной контент социальные сети/мессенджеры; дубль-порталы; маркетплейсы; блокчейн-технологии.

Коммун
икология.
2023.
Том
11.1
Nº 2.
C
C. 28-39

Система (признак) классификации	Виды информационных войн	Степень интеграции интернет-технологий	Носители информации
	За обладание инфор- мацией	Высокая	(псевдо)новостной контент; блогерский контент; социальные сети/мессенджеры; дубль-порталы; блокчейн-технологии.
	Ценностная	Высокая	лонгриды / расследования; блогерский контент; социальные сети/мессенджеры; маркетплейсы.
Тип конфликта	Информационная агрессия	Высокая	(псевдо)новостной контент; социальные сети / мессенджеры; дубль-порталы; блокчейн-технологии.
	Информационная экс- пансия	Низкая	(псевдо)новостной контент; блогерский контент; социальные сети / мессенджеры; лонгриды / расследования; дубль-порталы; маркетплейсы; блокчейн-технологии.
	Информационно- психологическая	Средняя	(псевдо)новостной контент; социальные сети / мессенджеры.

лизовывала технологию информационной мимикрии – создавая по сути хорошо замаскированный фейковый контент о сделках. Речь идет об атаке на корпорацию Wildberries в 2021 году, ущерб от которой превысил 380 миллионов рублей. Схема «военных действий» оказалась весьма простой: злоумышленники регистрировались на площадке в качестве продавца и в роли покупателя пытались провести несуществующий платёж по заведомо некорректным реквизитам. Как уже упоминалось важным фактором является то, что операция проводилась в условиях пандемических ограничений и существенного роста онлайн-продаж, а сама сделка была качественно «замаскирована» под наиболее популярные итерации на платформе. Wildberries переводила деньги продавцу, но на свой счёт ничего не получала. Примечательно то, что блокчейн-технология, исследуемая авторами могла бы стать в описанном конфликте одним из инструментов противодействия злоумышленникам.

Наконец, третий комплексный отраслевой кейс показательного использования различных интернет-технологий в современных информационных конфликтах произошел уже в 2022 году. По сути – это комплекс информационных атак на мировую траспортную отрасль, который, по мнению отдельных экспертов носит трендовый характер.

В результате целой череды информационных атак на траснпортные компании Европы и Азии в первом квартале 2022 года было затруднено передвижение пассажиров, возникали перебои с поставками продукции и сырья. И если из-за атаки на итальянскую железнодорожную компанию Ferrovie dello Stato Italiane, основанной на интеграции вредоносных составляющих в систему маркетплесов, была приостановлена продажа билетов, то белорусские железные дороги ждали более серьезные последствия. В результате первой кибератаки злоумышленники зашифровали серверы «Белорусской железной дороги», что заблокировало работу онлайн-кассы. Повторная кибер-атака сопровождалась формированием фейкового новостного контента (на белорусских форумах и в социальных сетях множились сообщения о перебоях с движением поездов в Минске), что парализовало движение поездов в столице и городе Орше.

Проблемы с транспортом касались не только железных дорог: в интегральном кейсе необходимо рассмотреть информационные атаки на системы авиасообщения. Так, в начале 2022 года компания Swissport International, оказывающая услуги по обслуживанию аэропортов, сообщила об атаке программы-вымогателя, которая привела к задержке рейсов.

Как видно из исследования, последствия информационных атак на транспортную отрасль могут затрагивать цепочку поставок сырья и продукции: например, кибератаки на крупные нефтяные терминалы SEA-invest (Бельгия) и Evos (Нидерланды) повлияли на работу портов во всей Европе и Африке и привели к задержкам в поставках топлива.

Заключение. Проанализированные кейсы, часть из которых представлена в тексте статьи, позволяют подтвердить гипотезу об интенсификации практики информационных войн в условиях развития интернет-коммуникаций, при этом необходимо отметить, что рожденные в интернет-среде технологии (как цифровые, так и социальные) могут являться как инструментом нападения, так и средством защиты в современной информационной войне.

Источники

Василенко Т.В. Игнатченко П.Д. (2019). Языковые средства в PR-текстах как фактор влияния на целевую аудиторию (на примере корпоративных СМИ) // Социально-гуманитарные знания. № 8. С. 115-122.

Володенков С.В. (2016). От информации к коммуникации: коммуникационные технологии в условиях современного пост-информационного общества // Вестник Московского государственного областного университета. № 4. С. 4-13.

Коломиец В.П. (2014). Медиасоциология: теория и практика. М.: Восход-А.

Лассуэлл Г.Д. (2021). Техника пропаганды в мировой войне / Пер. с английского В.Г. Николаева; отв. ред. Д.В. Ефременко, вступ. статья Д.В. Ефременко, И.К. Богомолова. М.: Институт научной информации по общественным наукам РАН.

Манойло А.В. (2005). Информационно-психологическая война: факторы, определяющие формат современного вооруженного конфликта // Материалы V Международной научнопрактической конференции «Информационные технологии и безопасность». №8. С. 73-80.

Панарин И.Н. (2009) Информационная война, PR и мировая политика. Учебное пособие для вузов. М.: Горячая линия.

Сулейманова Ш.С., Назарова Е.А. (2017). Информационные войны: история и современность: Учебное пособие. М.: Международный издательский центр «Этносоциум».

Цыганов В.В, Бухарин С.Н. (2007). Информационные войны в бизнесе и политике: Теория и методология. М.: Академический проект.

Чумиков А.Н. (2021).Конфликтные коммуникации в медийном поле // Коммуникология. Том 9. № 2. С. 125-142.

Шарков Ф.И. (2015). Генезис социологических школ и теории коммуникации // Коммуникология. Т. 3. № 4. С. 15-30.

Conserva H.T. (2003). Propaganda Techniques. 1st Books Library.

Lasswell H. (1948). The Structure and Function of Communication in Society. In L. Bryson (ed.) The communication of ideas. N. Y.: Harper. P. 37-51.

Libicki M. (2007). Conquest in Cyberspace: National Security and Information Warfare. New York: Cambridge University Press.

Rogers E.M. (1994). A history of communication study. A biographical approach. N.Y.: Free Press. Rubin A.M., Windhall S. (1986). The uses and dependency model of mass communication. Critical Studies in Mass Communication. Vol. 3. No. 2. P. 184-199.

■ ■ The Place of Internet Communication in Information Warfare

Yablonskikh A.V.1, Drobyshev D.V.2, Chalenko D.A.1

- 1. Peoples' Friendship University of Russia (RUDN University), Moscow, Russia.
- 2. Bauman Moscow State Technical University (BMSTU), Moscow, Russia.

Abstract. The article represents the authors' analysis of historical and modern approaches to the definition of the concept of information warfare and to the tools of its conduct. The classification systems studied in the material were taken into account when conducting a structured content analysis of cases of information wars in Russia and abroad. Internet technologies (of a digital and social nature), their significance in various types of information wars and the tool base were chosen as the key marker of content analysis. The authors have made and confirmed the hypothesis about the intensification of the practice of information warfare in the context of the development of Internet communications, while it should be noted that technologies born in the Internet environment (both digital and social) can be both an instrument of attack and a means of protection in modern information warfare.

Keywords: information warfare, information conflicts, content analysis, Internet technologies

For citation: Yablonskikh A.V., Drobyshev D.V., Chalenko D.A. (2023). The place of internet communication in information warfare. *Communicology (Russia)*. Vol. 11. No. 2. P. 28-39. DOI: 10.21453/2311-3065-2023-11-2-28-39.

Inf. about the authors: Yablonskikh Andrey Viktorovich – CandSc (Philology), associate professor at the Department of Mass Communications of RUDN – University. Address: 117198, Russia, Moscow, Miklukho-Maclay st., 6. E-mail: yablonskikh-anv@rudn.ru. Drobyshev Dmitry Vadimovich – Head of the Department of International Scientific and Educational Cooperation, BMSTU. Address: 105005, Russia, Moscow, 2nd Bauman st., 5/1. E-mail: d.v.drobishev@gmail.com. Chalenko Daniil Anatolyevich – doctoral student at the Faculty of Philology of RUDN– University. Address: 117198, Russia, Moscow, Miklukho-Maclay st., 6. E-mail: chalenko.da@gmail.com.

Received: 25.04.2023. Accepted: 07.06.2023.

References

Chumikov A.N. (2021). Conflict Communications in the Media Field. *Communicology*. V. 9. No. 2. P. 125-142 (in Rus.).

Conserva H.T. (2003). Propaganda Techniques. 1st Books Library.

Kolomiets V.P. (2014). Media sociology: theory and practice. M.: Voskhod-A (in Rus.).

Lasswell G.D. (2021). Propaganda technique in the world war / Transl. V.G. Nikolaev; ed. D.V. Efremenko. M.: Institute of Scientific Information on Social Sciences of the Russian Academy of Sciences (in Rus.).

Lasswell H. (1948). The Structure and Function of Communication in Society. In L. Bryson (ed.) The communication of ideas. N. Y.: Harper. P. 37-51.

Libicki M. (2007). Conquest in Cyberspace: National Security and Information Warfare. New York: Cambridge University Press.

Manoilo A.V. (2005). Information and psychological warfare: factors determining the format of modern armed conflict. In: Proceedings of the 5th International Scientific and Practical Conference "Information Technologies and Security". No. 8. P. 73-80 (in Rus.).

Panarin I.N. (2009) Information war, PR and world politics. Textbook for universities. M.: Hotline (in Rus.)

Rogers E.M. (1994). A history of communication study. A biographical approach. N.Y.: Free Press. Rubin A.M., Windhall S. (1986). The uses and dependency model of mass communication. Critical Studies in Mass Communication. Vol. 3. No. 2. P. 184-199.

Sharkov F.I. (2015). Genesis of sociological schools and communication theory. *Communicology*. V. 3. No. 4. P. 15-30 (in Rus.).

Suleymanova Sh.S., Nazarova E.A. (2017). Information wars: history and modernity: Textbook. M.: International Publishing Center "Ethnosocium" (in Rus.).

Tsyganov V.V., Bukharin S.N. (2012). Information wars in business and politics: Theory and methodology. M.: Academic project (in Rus.).

Vasilenko T.V. Ignatchenko P.D. (2019). Language means in PR-texts as a factor of influence on the target audience (on the example of corporate media). *Social and humanitarian knowledge*. No. 8. P. 115-122 (in Rus.).

Volodenkov S.V. (2016). From information to communication: communication technologies in the conditions of modern post-information society. *Bulletin of the Moscow State Regional University*. No. 4. P. 4-13 (in Rus.).