УДК 355.40

doi: 10.53816/20753608_2025_1_24

# ИНФОРМАЦИЯ КАК СРЕДСТВО ПОРАЖЕНИЯ ПРОТИВНИКА

# INFORMATION AS A MEANS OF DEFEATING THE ENEMY

***А.Н. Зыков,*** *чл.-корр. РАРАН* ***А.В. Морозов***

*Военный инновационный технополис «ЭРА»*

***A.N. Zykov, A.V. Morozov***

В настоящей статье рассматриваются актуальные вопросы информационного воздействия на противника. Обобщен исторический опыт зарождения и становления информационного воздействия как средства поражения, выявлена суть данного явления. Рассмотрены некоторые методы информационного воздействия в целях достижения политического влияния, экономического давления и военного преимущества над противостоящей стороной.
***Ключевые слова***: информация, информационное воздействие.

The present article deals with the topical issues of information influence on the enemy. The historical experience of origin and formation of information influence as a means of defeat is generalized, the essence of this phenomenon is revealed. Some methods of information influence in order to achieve political influence, economic pressure and military advantage over the opposing party are considered.
***Keywords***: information, informational impact.

В процессе эволюции человеческое общество все в большей степени осознавало ценность, значимость и действенность информации, не только как инструмента познания окружающего мира и основы для выстраивания коммуникативных связей, но и как мощного орудия консолидации, созидания, а также и как невероятно действенного все разрушающего оружия, по своей мощности порой превосходящего все известные виды вооружения.

Истоками идей информационного поражения противника можно считать первоначальное осмысление правителями древнего мира физически не насильственного управления массами людей. О понимании важности информационного воздействия на противоборствующую сторону свидетельствуют взгляды египетских и ассирийских военачальников, прямо связывающих развитие хода сражения с психическим состоянием бойцов и результатами дезинформационного воздействия на противника.

Первое упоминание удачного применения информационного воздействия относится еще к III тысячелетию до н.э. В поэме «Энмеркар и верховный жрец Аратты» повествуется о том, как правитель шумерского города-государства Урука без применения военной силы добился выплаты дани от жителей города Аратта, путем преднамеренного и систематического запугивания жителей и правителя этого города [3].

Одним из лучших специалистов античного мира по дезинформации противника считается Ганнибал (III–II вв. до н.э.). Примером может служить подготовка Ганнибала к битве с римскими легионерами при реке Треббии, в ходе которой он активно распускал слухи о несокру-

шимой мощи нового оружия карфагенян, чем способствовал формированию психологической готовности римлян к поражению.

Анализ научной литературы [1–4] позволяет сделать вывод, что исторически роль информационного воздействия на противника отводилась в качестве обеспечения боевых и повстанческих действий. Объектом такого воздействия всегда было внутреннее состояние человека, определяющее направленность его деятельности.

В процессе развития форм и способов военного противоборства информация становится все более опасным и всеобъемлющим средством поражения. Как правило, целью воздействия информации на противника становится стремление ослабить волю противоборствующей стороны, подорвать способность к активному сопротивлению. Такое воздействие, в отличие от других средств поражения, способствует более быстрому уничтожению противника и сохраняет как собственные материальные и физические силы, так и завоеванные трудовые и материальные ресурсы [4].

По мере накопления практического опыта потребовалось его теоретическое осмысление. Первыми документально зафиксированными трудами в области информационного воздействия можно считать труды китайских исследователей, которые связаны с именами философов Конфуция и Сунь-Цзы (VI–V вв. до н.э.). В своем «Трактате о военном искусстве» Сунь-Цзы ставит информационное воздействие на противника на одно из первых мест в военном противоборстве [5]. Особое внимание он уделяет именно психологической составляющей противника как объекта поражения, необходимости знания личностных характеристик противостоящих полководцев. В трудах военного теоретика Чжугэ Лян (III в. н.э.) определяется, что атака на умы — главная задача, атака на укрепления — второстепенная задача. В свою очередь древнегреческий писатель Ксенофонт (IV в. до н.э.), римский полководец Ю. Цезарь (I в. до н.э.) и ученый Н. Макиавелли (XV–XVI вв.) в своих трудах особое внимание уделяли обеспечению психологической устойчивости своих воинов в бою и вопросам дезинформации. Платон и Аристотель считали необходимостью, с целью упрочнения социально-политического строя и законного порядка, внушение населению комплекса философско-мифологических воззрений [6, 7]. Этих же воззрений придерживался римский оратор и государственный деятель Цицерон (I в. до н.э.) и хорватский мыслитель Ю. Крижанич, указывавшие на отрицательное воздействие чужеземных нравов и языков, нарушающих отечественные установления и стабильность строя.

Обобщение исторического опыта зарождения и становления информационного воздействия как средства поражения противника показывает, что его суть заключается в скрытом воздействии на сознание людей путем замены объективной реальности искусственно создаваемыми виртуальными моделями (массовые мнения, представления, предпочтения, реакции и отношения к конкретным событиям) и в последующем управление их поведением, побуждение к конкретным поступкам, чуждым их взглядам.

Особое значение в свете решения задачи понимания феномена «информации как средства поражения противника» приобретает изучение механизмов и методов, с помощью которых происходит это воздействие. Важно учитывать, что информационное воздействие включает в себя широкий спектр технологий и стратегий, начиная от пропаганды и дезинформации до психологических операций и кибероперациий.

Так, в различных странах приблизительно с середины XX века существуют специализированные агентства и структуры, занимающиеся информационными операциями. Эти организации занимаются изучением и обобщением боевого и клинического опыта психологического воздействия на людей в различных условиях. Они разрабатывают и адаптируют методы, направленные на изменение массового сознания, формирование определенных установок и поведенческих реакций и применяют их на практике в различных регионах мира для достижения политических и стратегических целей, или иными словами: нанести информационное поражение.

Информационное поражение — это стратегия, направленная на изменение восприятия и поведения целевой аудитории путем воздействия на информационное пространство.

Наиболее часто встречаются следующие способы информационного поражения: пропаганда, дезинформация, кибероперации и информационные войны.

Помимо этого, также необходимо отметить, что эти способы зачастую не используются по отдельности. Как и любое потенциально успешное действие, оно требует системного подхода и комплексного применения. Например, пропаганда может сопровождаться дезинформацией для создания ложного нарратива, который затем усиливается с помощью кибератак, направленных на подрыв доверия к основным источникам информации. Информационные войны включают в себя все эти элементы, создавая многослойную стратегию, направленную на долговременное влияние и подрыв стабильности целых стран.

Разберем по отдельности перечисленные методы.

Пропаганда — это один из наиболее известных и распространенных методов информационного воздействия. Пропаганда включает использование медиа, социальных сетей, телевидения, радио и других средств массовой информации для распространения однобокой или искаженной информации с целью убеждения аудитории в определенной точке зрения или мнении. Пропаганда может использовать как истинные факты, так и ложную информацию для достижения своих целей.

Ярким примером пропаганды является разработанная и осуществленная вооруженными силами США операция на территории Демократической Республики Вьетнам (1955–1975 гг.).

Сформированное в 1951 году, управление психологической войны США во время войны во Вьетнаме впервые широкомасштабно использовало телевидение. Были разработаны телепрограммы для различной аудитории (гражданская и военная). Были построены студии и 4 передающие станции, каждая из которых вещала по 6 часов в сутки, транслируя пропагандистские передачи. В то же время среди населения Вьетнама были бесплатно распространены телевизионные приемники. В различных общественных местах, таких как школы были установлены телевизоры, а к 1971 году 80 % местного населения могло смотреть телевизор, где основное экранное время занимали американские каналы.

Также применялась сувенирная пропаганда, а именно: с самолетов сбрасывались сигареты, игрушки, медикаменты, продукты питания и т.д. К подаркам в комплект шли листовки с проамериканскими лозунгами и плакатами. Всего в ходе войны на сувенирную пропаганду было потрачено 4 млн долларов.

В ходе военных действий во Вьетнаме, несмотря на поражение американцев, психологические методы ведения войны продемонстрировали свою эффективность. За весь период боевых действий приблизительно 250 тысяч вьетнамцев добровольно перешли на сторону противника [8, с. 16–23].

Однако пропаганда — это не единственный инструмент информационной войны. Дезинформация, как ее неотъемлемая часть, также играла важную роль в мировой истории.

Дезинформация — это целенаправленное распространение ложной или вводящей в заблуждение информации с целью дезориентировать, запутать или обмануть противника. В военных конфликтах дезинформация используется для создания неверного представления о военных намерениях, силах, позициях и действиях, что может привести к стратегическим ошибкам со стороны противника.

Так, во время Второй мировой войны союзниками была разработана операция под кодовым названием «Бодигард». Операция была стратегическим планом дезинформации. Ее цель состояла в том, чтобы ввести в заблуждение немецкое командование относительно времени и места предстоящего вторжения союзников в Западную Европу. Основная цель операции заключалась в том, чтобы скрыть истинные намерения союзников по поводу высадки в Нормандии и заставить немцев распределить свои силы по более широкому фронту.

В ходе операции, путем использования фальшивых радиопередач, двойных агентов, поддельных карт и военных документов, а также имитации военной активности, союзники внушили немецкому командованию, что планируется вторжение на Балканский полуостров, из-за чего немецкое командование не стало перемещать войска из Греции и Югославии на запад, для укрепления границы. В то

же время, союзники создавали фиктивные военные подразделения с использованием надувных танков и деревянных самолетов, чтобы сымитировать подготовку к вторжению в Па-де-Кале, что в свою очередь заставило германское командование удерживать значительные силы в этом районе и пустить меньше таковых на оборону реального места высадки союзников в Нормандии. Данная операция по дезинформации противника позволила союзникам успешно провести операцию «Оверлорд» с меньшими потерями и принять участие в освобождении Западной Европы от фашистской оккупации [9, с. 72–87].

Стоит также отметить, что дезинформация в современном мире используется не только на поле боя. Большое число ложных ново стей и фальшивых сообщений распространяется через интернет и социальные сети с целью манипуляции общественным мнением, дискредитации политических оппонентов, влияния на выборы и даже дестабилизации целых стран.

Современные технологии позволяют создавать высококачественные фальшивки, включая видео и аудиозаписи, что усложняет выявление истинных источников информации. Борьба с дезинформацией стала одной из важнейших задач для правительств, международных организаций и технологических компаний, которые разрабатывают новые методы и инструменты для выявления и предотвращения распространения ложной информации.

В то же время, с развитием технологий, способы информационного поражения также претерпели изменения. Традиционные методы, такие как агентурная сеть, распространение ложной информации через радиоканалы и т.д., ушли на второй план, уступив место кибероперациям.

Кибероперации — это новые формы информационного воздействия в киберпространстве, направленные на сбор информации, воздействие на информационные системы (ИС) или их уничтожение.

Кибероперации стали неотъемлемой частью современной военной и разведывательной деятельности. Они позволяют более эффективно и незаметно манипулировать общественным мнением путем взлома официальных источников информации, разрушать критическую инфраструктуру без непосредственного участия в этом человека и влиять на решения противника путем взлома стратегических устройств и компьютерных сетей, распространять вредоносное программное обеспечение (ПО).

Эффективность кибероперацій заключается в анонимности, экономичности и направленности, кибератаки могут быть проведены из любой точки мира, через прокси-серверы и иные методы маскировки. Кибероперации зачастую требуют меньших финансовых инвестиций, чем традиционные методы, но при этом имеют большую эффективность. Кибератаки тщательно планируются и узнать о том, что таковая готовится, можно только после того, как она произошла.

Примером успешной кибероперации, или, иными словами, кибератаки — является разработанный, предположительно в США, компьютерный червь Stuxnet. Данный вирус был внедрен в иранскую государственную сеть в 2010 году и был направлен на иранскую ядерную промышленность. Вирус внедрялся в центрифуги, предназначенные для обогащения урана, и путем изменения программы работы станка увеличивал скорость вращения центрифуг на непредусмотренные показатели, из-за чего оборудование выходило из строя.

Одной из самых впечатляющих особенностей Stuxnet была его способность скрывать свои действия. Червь подменял данные, передаваемые на операторские консоли, показывая нормальную работу систем, несмотря на их реальное разрушение.

Данное событие считается одной из первых успешных кибероперацій в мире. По оценкам экспертов, оно нанесло ущерб в сотни миллионов долларов и значительно замедлило иранскую ядерную программу.

Внедрение вируса Stuxnet стало поворотным моментом в истории. Его разработчики продемонстрировали возможности кибероружия, как средства достижения стратегических целей без применения традиционных военных методов и открытой агрессии. Это событие в первую очередь подчеркнуло важность кибербезопасности и подтолкнуло государства и частные компании к крупным инвестициям в сферу защиты информации и кибербезопасности [10–13].

Как уже упоминалось, эти методы эффективно работают в комплексе. Их сочетание и одновременное применение на одной территории против одного объекта характеризуется как информационная война. Такие конфликты могут длиться десятилетиями и оказывать глубокое влияние на социальные, политические и экономические процессы в стране и между странами. Целью информационной войны является не только достижение военных целей, но и изменение общественного мнения, формирование стереотипов и управление информационным пространством.

Современные конфликты включают в себя не только физическое противостояние, но и борьбу за информационное превосходство. Это вынуждает государства и частные структуры инвестировать в кибербезопасность, обучение специалистов и разработку новых технологий для защиты от информационных атак.

Информационная война включает комплексную стратегию, где пропаганда, дезинформация и кибероперации действуют взаимодополняюще. Информационные операции оказывают значительное влияние на противника, разрушая его информационные и технические системы, подрывая авторитет правительства и создавая общественное недоверие к официальным источникам. С использованием медиаплатформ и социальных сетей такие операции распространяют фальшивые новости и искаженные факты, усиливая внутренние разногласия и конфликтные настроения в обществе. В сочетании с кибератаками, направленными на критически важную инфраструктуру, эти методы могут парализовать экономику, подорвать национальную безопасность и дестабилизировать политическую ситуацию, что приводит к долгосрочным негативным последствиям для государства.

Примером информационной войны является конфликт на Украине (с 2014 года по наст. вр.), где стороны активно используют медиа, социальные сети и кибертехнологии для формирования общественного мнения и воздействия на критическую инфраструктуру оппонентов.

Так, в 2017 году мир столкнулся с атакой вируса-шифровальщика NotPetya. Хотя организаторов атаки так и не удалось однозначно идентифицировать, основной удар пришелся на украинские государственные и частные предприятия. Этот инцидент привел к параличу банковских систем, государственных учреждений и энергетических компаний. Всего вирус нарушил работу не менее чем 300 украинских предприятий, кроме того, данные были стерты с каждого десятого компьютера на Украине. Среди наиболее пострадавших компаний были: «Укрэнерго» «Запорожьеоблэнерго», «Киевэнерго», «Днепроэнерго», Киевский метрополитен и украинские мобильные операторы «Киевстар», LifeCell и «Укртелеком». Только в США финансовые потери от этой кибератаки оцениваются примерно в 10 миллиардов долларов [14, 15].

В то же время на протяжении всего конфликта велась масштабная пропагандистская кампания, направленная на дискредитацию украинского правительства, усиление паники среди населения. В ходе этой кампании использовались фальшивые аккаунты в социальных сетях, публиковались новости и видеоролики, распространявшие информацию о коррупции в правительстве и неэффективности украинских властей в управлении страной. В результате общественное доверие к правительству значительно снизилось, что усилило внутренние разногласия и на фоне кибератак на критическую инфраструктуру еще сильнее дестабилизировало политическую ситуацию в стране [18–21].

Для проведения успешных информационных операций используется большое число методов. Одним из наиболее опасных инструментов информационного противоборства стали дипфейки — фальсифицированные видео- и аудиозаписи, создаваемые с использованием искусственного интеллекта (ИИ). Эти технологии позволяют создавать крайне реалистичные подделки, которые могут использоваться для дискредитации политических лидеров, распространения ложной информации и провоцирования социальных волнений. Дипфейки своей реалистичностью и легко изменяемыми сюжетами способны подрывать доверие к официальным источникам информации, создавая иллюзию подлинности и правдивости фальсифицированных данных [16, с. 112–119].

Кроме того, информационные кампании в социальных сетях, направленные на распро-

странение ложных новостей и манипуляцию общественным мнением, стали стандартным инструментом в арсенале современных информационных войн. Фальшивые аккаунты и боты активно используются для усиления разногласий внутри обществ, формирования протестов и подрыва доверия к властям. Эти методы в сочетании с традиционной пропагандой и дезинформацией создают многослойную и труднообнаружимую схему манипуляций, способную эффективно влиять на внутренние и внешние политические процессы отдельно взятого государства или политического формирования.

Также активно используются так называемые «Фабрики троллей» — группы людей, организованно создающих и распространяющих комментарии и посты в социальных сетях с целью манипуляции общественным мнением. Эти группы могут быстро реагировать на события и направлять общественное обсуждение в нужное русло, подрывая доверие к оппонентам и формируя необходимую повестку дня [17, 22].

Другой метод — использование поддельных новостных сайтов и платных статей, размещаемых на легитимных ресурсах. Такие сайты и статьи создаются для распространения дезинформации и формирования нужного мнения у широкой аудитории. Эти материалы могут выглядеть как настоящие новости, что делает их выявление и опровержение сложной задачей.

Кроме того, стоит отметить использование манипуляций с алгоритмами поисковых систем и социальных сетей. Например, целенаправленное создание и продвижение контента, который попадает в тренды или на верхние позиции в поисковой выдаче, позволяет дезинформационным кампаниям достигать широкой аудитории. Это может включать в себя не только фальшивые новости, но и искаженную статистику, сфабрикованные исследования и мнения «экспертов», создающих иллюзию легитимности и объективности.

Изучив данную проблему, можно сделать выводы, что в ближайшем будущем информационное противоборство будет только усиливаться, приобретая все более изощренные и технологически продвинутые формы. С развитием ИИ и машинного обучения можно ожидать появления более эффективных и труднообнаружимых методов дезинформации и кибератак. Государства и негосударственные акторы будут все активнее использовать эти технологии для достижения своих целей, включая политическое влияние, экономическое давление и военное преимущество. Информационные войны станут неотъемлемой частью глобальных конфликтов, требуя от государств значительных инвестиций в кибербезопасность, разработку новых технологий защиты информации и подготовку специалистов. В условиях растущей взаимосвязанности мирового сообщества борьба за информационное превосходство будет иметь значительное влияние на международные отношения и стабильность в различных регионах мира.

**Список источников**

1. Макиавелли Н.О. О военном искусстве: пер. с итал. М.: Воениздат, 1939. 181 с.

2. Черняк Е.Б. Химеры старого мира. М.: Молодая гвардия, 1970. 10 с.

3. Крамер С.Н. История начинается в Шумере; под ред. и с предисл. В.В. Струве; пер. Ф.Л. Мендельсона. М.: Наука, 1965. 148 с.

4. Сулейманов Ш.С., Назаров Е.А. Информационные войны: история и современность: уч. пособие. М.: Международный издательский центр «Этносоциум», 2017. 124 с.

5. Сунь Цзы (VI–V вв. до н.э.) Искусство войны / Сунь-Цзы; под ред. Томаса Клири; пер. с англ. Н. Рыбальченко. М.: София, 2008. 223 с.

6. Платон, (427-347 до н. э.). Сочинения : в 3 т.; пер. с древнегреч.; под общ. ред. А. Ф. Лосева и В. Ф. Асмуса. М.: Мысль, 1968–1972.

7. Аристотель. Сочинения в 4-х томах. Том 4. М.: Мысль, 1984.

8. Токов Е., Касюк А. Психологические операции вооруженных сил США в войнах и конфликтах XX века // Зарубежное военное обозрение. 1997. № 6. С. 16–23.

9. Лавренов С.Я., Хмельников В.С. Открытие Второго фронта в Европе. К 75-летию со дня проведения Нормандской операции (6 июня–30 августа 1944 г.) // Научно-аналитический журнал Обозреватель-Observer. 2019. № 6 (353). С. 72–87.

10. Stuxnet: начало // kaspersky daily. URL: https://www.kaspersky.ru/blog/stuxnet-victims-zero/6119/?ysclid=lxmxx1awp7553897625 (дата обращения: 20.06.2024).

11. Вирус Stuxnet может быть нацелен на урановые заводы Symantec // РИА Новости. URL: https://ria.ru/20101116/297125122.html?ysclid=lxmy192cj8375398204 (дата обращения: 20.06.2024).

12. Stuxnet в деталях: «Лаборатория Касперского» публикует подробности атаки на ядерный проект Ирана // kaspersky. URL: https://www.kaspersky.ru/about/press-releases/2014_stuxnet-v-detaliakh?ysclid=lxmy1abmsa71884087 (дата обращения: 20.06.2024).

13. СМИ: вирус Stuxnet подогрел электронную гонку вооружений // Russia Today. URL: https://russian.rt.com/article/11423 (дата обращения: 20.06.2024).

14. Вирус нового поколения: как кибератака NotPetya изменила мир // Газета.ru. URL: https://www.gazeta.ru/tech/2020/06/26/13132537/petya_is_three.shtml?ysclid=lxodteu6nu207308399&updated (дата обращения: 21.06.2024).

15. «Чистой воды манипуляция»: почему Запад обвинил Россию в распространении вируса NotPetya // Russia Today. URL: https://russian.rt.com/world/article/482654-rossiya-ssha-kiberataka-obvineniye (дата обращения: 21.06.2024).

16. Добробаба М.Б. Дипфейки как угроза правам человека // Lex russica. 2022. № 11 (192). С. 112–119.

17. Пригожин назвал себя создателем «фабрики троллей» // РБК. URL: https://www.rbc.ru/technology_and_media/14/02/2023/63ebaac39a7947282a7adc8e?ysclid=lxoqdgm4s1850033771 (дата обращения: 21.06.2024).

18. Селин И.А., Фентисов Д.А. Информация — новое оружие массового поражения // Социально-политические науки. 2022. Т. 12. № 2. С. 15–20.

19. Осавелюк Е.А. Роль средств массовой информации (СМИ) в обеспечении информационной безопасности России на евразийском пространстве // Международное сотрудничество евразийских государств: политика, экономика, право. 2016. № 3. С. 94–104.

20. Шкрабков В.Н. Информационное оружие и информационные войны. М., 2001. 227 с.

21. Кузьмина Е.А. Сетевые информационные войны как фактор угрозы глобальной безопасности // Вестник Саратовской государственной юридической академии. 2017. № 2 (115). С. 221–225.

22. Бурыкин И.А. Информационное сопровождение социальных конфликтов в средствах массовой информации (на примере сирийского конфликта) // Коммуникология: электрон. науч. журн. 2019. Т. 4. URL: http://online.communicology.us/p/archive.html (дата обращения: 20.11.2024).