Информационные войны как феномен постиндустриального (информационного) общества: основные парадигмы

Information wars as a phenomenon of the post-industrial (information) society: the main paradigms

DOI: 10.12737/2587-6295-2025-9-1-25-40
УДК: 32.019.5
Получено: 15.01.2025 Одобрено: 23.02.2025 Опубликовано: 25.03.2025

Сорокин И.О.
Ассистент кафедры политологии, ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», аспирант кафедры политического анализа и социально-психологических процессов ФГБОУ ВО «Российский Экономический Университет имени Г.В. Плеханова", г. Москва
e-mail: IOSorokin@fa.ru

Sorokin I.O.
Assistant at the Department of Political Science at the Financial University under the Government of the Russian Federation, postgraduate student at the Department of Political Analysis and Socio-Psychological Processes at Plekhanov Russian University of Economics, Moscow
e-mail: IOSorokin@fa.ru

Аннотация
Целью настоящей статьи является исследование информационной войны как феномена постиндустриального (информационного) общества в увязке с основными парадигмами, встречающимися в современной науке. Методами исследования стали сравнение, анализ, синтез, классификация, индукция и дедукция. В работе представлены одиннадцать выявленных в научной литературе парадигм изучения информационной войны, которые позволяют обратить более пристальное внимание на различные аспекты столь сложного феномена, а также ознакомиться с трудами авторов, изучающих данное явление. В статье отмечается, что информационное противоборство имеет продолжительную историю, но к настоящему моменту значительно эволюционировало и является феноменом, прежде всего, постиндустриального (информационного) общества. Делается вывод о том, что современная информационная война стала более востребованным и эффективным средством поражения противника нежели было ранее ввиду появления в середине XX в. ядерного оружия, а также произошедшей на рубеже XX—XXI вв. новой «информационной революции», развитию СМК, техник информационно-психологического воздействия и представляет собой не только целенаправленные действия по использованию цифровых средств коммуникации для получения превосходства над противником путем различных манипуляций с информацией и информационными системами, а также защиты собственных информационных систем, но и воздействие на его психоэмоциональное состояние и поведение. Также выявлено, что зачастую в работах по данной тематике из раза в раз повторяются схожие смыслы и тезисы. Теоретическая значимость работы состоит в уточнении и расширении представлений о феномене информационной войны и упорядочении (классификации) имеющихся подходов (парадигм) к ее изучению.
Ключевые слова: информационная война, информационные операции, гибридная война, когнитивная война, ментальная война, психологическая война, кибервойна.

Abstract
The purpose of this article is to study information warfare as a phenomenon of the post-industrial (information) society in conjunction with the main paradigms found in modern science. The research methods are comparison, analysis, synthesis, classification, induction and deduction. The paper presents eleven paradigms of the study of information warfare identified in the scientific literature, which allow us to pay closer attention to a wide range of different aspects of such a complex phenomenon, as well as to familiarize ourselves with authors studying this phenomenon. The article notes that information warfare has a long history, but has evolved significantly to date and is primarily a phenomenon of the post-industrial (information) society. It is concluded that modern information warfare has become a more in—demand and effective means of defeating the enemy than before due to the appearance of nuclear weapons in the middle of the 20th century, as well as the new «information revolution» that took place at the turn of the 20th and 21st centuries, the development of mass media, techniques of information and psychological impact, and represents not only targeted actions to use digital means of communication to gain superiority over the enemy through various manipulations with information and information systems, as well as protecting their own, but also the effect on his psychoemotional state and behavior. It is also revealed that often similar meanings and theses are repeated from time to time in works on this topic. The theoretical significance of the work is to clarify and expand the understanding of the phenomenon of information warfare and to streamline (classify) existing approaches (paradigms) to its study.
Keywords: information warfare, information operations, hybrid warfare, cognitive warfare, mental warfare, psychological warfare, cyberwarfare.

Введение

Современный мир находится в состоянии постоянного информационного противоборства, что делает исследование феномена информационной войны крайне актуальным. В условиях глобальных процессов демократизации и информатизации обострилось понимание того, что средства массовой коммуникации (далее — СМК) оказывают самое непосредственное влияние на публичную политику [25, с. 8], многократно возросла роль общественного мнения [29, с. 107].

Хотя информационное воздействие на противника, возникшее как составная часть вооруженной борьбы для повышения духа своих воинов и ослабления воли врага, велась задолго до появления интернета и насчитывает тысячелетнюю историю [37, с. 6], всемирная сеть вывела существовавшие способы информационного противоборства на качественно иной уровень интенсивности, масштабности и эффективности[1] и привнесла ряд новшеств. В связи с этим изучение различных подходов и парадигм, описывающих данное явление, представляется важной научной задачей.

Основная проблема, рассматриваемая в данной статье, заключается в сложности и многогранности феномена информационной войны, который эволюционировал под влиянием технологических и социальных изменений.

Целью данной работы является анализ и систематизация основных парадигм, встречающихся в современной науке, для более глубокого понимания феномена информационной войны. Для достижения этой цели ставятся следующие задачи:

1. Выявить и проанализировать основные подходы (парадигмы) к изучению информационной войны, существующие в научной литературе.
2. Классифицировать выявленные парадигмы, выделяя их ключевые особенности и различия.
3. Определить место информационной войны в структуре постиндустриального (информационного) общества.

[1] См.: Овчинский В., Ларина Е. Холодная война 2.0. Доклад Изборскому клубу. [Электронный ресурс]. URL: http://dynacon.ru/content/articles/4224/ (дата обращения: 10.02.2025).

4. Обозначить механизмы влияния информационных войн на психоэмоциональное состояние и поведение индивидов.

5. Рассмотреть эволюцию информационного противоборства в контексте современных технологических изменений.

В проведенном исследовании многократно используется ключевая категория — «информационная война», под которой понимается форма противоборства, включающая целенаправленное воздействие на информационные ресурсы, инфраструктуру, общественное мнение и психоэмоциональное состояние противника.

Обзор научной литературы

В статье проанализированы труды ведущих исследователей, посвященные вопросам информационного противоборства. Рассмотрены различные подходы, начиная от первых теорий пропаганды (Лассуэлл, Бернейс), заканчивая современными. Отдельное внимание уделено зарубежным исследованиям, связанным с влиянием информационного воздействия на геополитику (Бжезинский, Най и др.). В ходе проведенного анализа также использованы последние публикации российских и международных научных журналов по рассматриваемой проблематике.

Можно отметить, что текущий этап развития общества характеризуется значительным влиянием информационных технологий на политические, социальные и культурные процессы. Свершившиеся в течение нескольких последних десятилетий изменения, часто называемые «информационной революцией» [4, с. 16], либо ее новым этапом, как характеризуют произошедшие перемены другие авторы [25, с. 7], привели к становлению постиндустриального общества, в котором для приобретения и удержания власти стал особенно важен контроль над информационными технологиями. За прошедшие двадцать лет объемы производства и потребления данных выросли более чем в тысячу раз, радикально повысилась доступность интернета, персональных компьютеров и умных устройств [35].

Известные военные теоретики прошлого не раз отмечали значимость информационной составляющей в войне. Так, Сунь-Цзы, писал, что более эффективно покорить чужое войско, не сражаясь с ним [38, с. 26], А.В. Суворов отмечал глазомер, быстроту и натиск как три ключевых воинских искусства [36]. «Война — есть орудие политики», «война по существу своему это — бой», «бой — это измерение духовных и физических сил», — так писал в трактате «О войне» Карл фон Клаузевиц [16, с. 15, 44]. В подобном ключе высказывались и многие другие военные деятели, ученые и управленцы. Их прозрения актуализировались во второй половине XX в., когда развитие военного потенциала ведущих государств мира (СССР и США) перешагнуло порог создания ядерного оружия, что привело к постепенному вытеснению методов классического (кинетического) вооруженного противоборства более скрытными, завуалированными инструментами воздействия — началась «Холодная война». Не умаляя значимости кинетического оружия, одним из главных «полей битвы» стали культура, история, вера, идеология, менталитет, структуры самоопределения [35].

Помимо противостояния по поводу власти, война как разновидность политического конфликта, обладает еще несколькими специфическими устойчивыми родовыми признаками, а именно: наличие актора-субъекта политики (как правило, государства, либо военно-политического блока, реже — транснациональной корпорации (ТНК), либо частной военной компании (ЧВК)), объекта (к примеру другого государства, ТНК, ЧВК, территорий и (или) имеющихся на них ресурсов вроде полезных ископаемых), цели (нанести поражение противнику (победить) и закрепить результат, например, юридически — в мирном договоре), наступательных и оборонительных действий, носящих системный характер в течение ограниченного времени на конкретных территориях (театре военных действий), использование особых средств (вооружений) [45].

В этой связи необходимо обратить внимание на специфику информационной войны, которая не совсем соответствует данным критериям, поскольку информационное воздействие противников друг на друга в настоящее время полностью не прекращается никогда, в отличие

от более ранних периодов, в связи с чем текущие информационные войны представляют собой перманентное противостояние, но с разной степенью его интенсивности, переходящим из одного этапа в другой (от операции к операции или к группам операций). Помимо этого, при сравнении классической («обычной», кинетической) войны с конфликтами с использованием цифровых технологий можно выделить еще несколько отличий, а именно: в большинстве случаев информационные войны ведутся на чужой территории, они практически бесследны и значительно менее затратны [25, с. 229]; вместе с тем необходимо заметить, что цель информационной войны в общем совпадает с классической, но для ведения активных действий нападающая сторона (агрессор) должна проникнуть в «представления о мире» своего противника, понять алгоритм и уровень его мышления [39, с. 12].

Термин «информационная война» ввел Т. Рона в своем докладе 1976 г., в котором им была отмечена опасность поражения американской экономической и военной информационной инфраструктуры [62]. Впоследствии термин укрепился в лексиконе Минобороны США — сначала для описания радиоэлектронной борьбы (например, в Директиве МО США ТС-3600.1 от 21.12.1992 [64]), а затем и в других документах, например, в Доктрине информационных операций Комитета начальников штабов ВС США 1998 г., в которой были введены понятия оборонительных и наступательных информационных операций [52]. В 2006 г., в одном из полевых уставов (field manual) Министерства обороны США также появляется понятие «Операции в интернете» [50], после чего в 2010 г. возникает Концепция стратегических коммуникаций НАТО [56], в которой информационная война понимается как комплекс мероприятий по целенаправленному коммуникационному воздействию на целевую аудиторию враждебных, союзных и нейтральных государств. Впоследствии развитие концепции информационный войны продолжилось в нормативных правовых актах (НПА) США, НАТО, других государств и военно-политических блоков, однако акцентируем внимание на теории, оставив анализ НПА для отдельной статьи.

Одним из родоначальников осмысления современной информационной войны является Мартин Либики, который в 1995 г. писал, что: «Информационной войны, как отдельного метода ведения войны, не существует. Вместо этого есть семь ее форм: командно-управленческая война, разведывательная война, электронная война, психологическая война, хакерская война, экономико-информационная война и кибервойна» [53].

В свою очередь автором концепции информационного общества зачастую называют испанского социолога — Мануэля Кастельса, который в своих работах «Информационная эпоха: экономика, общество и культура» 1997 г. и «Власть коммуникации» 2009 г. представил анализ взаимосвязи между властью, коммуникацией и сетевым обществом. В них подчеркивается важность сетевой мощи, а также отмечается важнейшая роль средств массовой информации (СМИ) в формировании общественного мнения и оказании влияния. Ученый утверждает, что мы перешли от индустриального общества к сетевому, для которого характерны децентрализованные, самоорганизующиеся сети, ставшие основным средством социальной организации и коммуникации, в связи с чем СМИ теперь являются ключевым местом борьбы за власть между различными группами и отдельными лицами, которые стремятся формировать общественный дискурс и осуществлять медиаполитику. При этом ученый отмечает, что сетевая власть более эффективна, чем традиционные иерархические структуры, поскольку обеспечивает большую гибкость, приспособляемость и инновационность [12, 13].

Вопросы, связанные с анализом информационных войн, либо их ключевых компонентов (в том числе без упоминания самого термина «информационная война», а смежных с ним, например, информационное противоборство, информационные операции, пропаганда, агитация, протестная инженерия, сознание масс, политическая реклама, PR, психолингвистика, кибервойна, кибероперации, кибершпионаж и проч.), рассматриваются также в работах Э. Бернейса, Айви Ли, П. Лазарсфельда, У. Липпмана, Г. Лассуэлла, Ж. Бодрийяра, М. Фуко, Дж. Миршмайера, Г. Лебона, Т. Гарра, Дж. Шарпа, Э. Люттвака,

Дж. Голдстоуна, Дж. Ная мл. и Р. Кохейна, Т. Скочпол, Ш. Айзенштадта, С. Московичи, З. Бжезинского, Г. Киссинджера, С. Манна, С. Анхольта, Э. Тоффлера, И.Н. Панарина, Г.Г. Почепцова, В.В. Кафтана, А.В. Манойло, Л.Л. Штофер, Р.Т. Мухаева, А.Б. Шатилова, С.П. Расторгуева, С.В. Ткаченко, В.В. Цыганова, С.Н. Гриняева и многих других авторов.

Следует заметить, что в различных трудах повторяются схожие тезисы об истоках (природе), функциях, субъектах, объектах, основных инструментах, роли и будущем информационных войн и (или) их компонентов (в том числе, не называя сам термин «информационная война»), что может говорить о сложившемся научном консенсусе, однако, разумеется, есть и различия, в зависимости от того, с каких позиций рассматривалось изучаемое явление. В этой связи представляется целесообразным провести классификацию набора встречающихся в научной литературе парадигм информационной войны.

Феномен информационного противоборства не является статичным — он эволюционировал от примитивных пропагандистских технологий XX в. к многоуровневым стратегическим операциям, использующим возможности цифровых технологий, алгоритмических систем управления информационными потоками, социальных сетей и искусственного интеллекта. Изучение такого сложного явления опирается на концепции из различных наук и научных парадигм, которые обеспечивают рамки для понимания сложной динамики их развития, позволяя сосредоточиться на конкретных ее аспектах.

Методы

В статье используются следующие методы исследования:

1. Анализ — проводится изучение содержания научных трудов по тематике информационных войн, выделяются их ключевые аспекты.
2. Сравнение — автор анализирует различные парадигмы изучения информационных войн, сопоставляя их особенности, отличия и сходства.
3. Синтез — на основе изученных парадигм создается обобщенное представление о феномене информационных войн, систематизируются существующие подходы, формулируются выводы о характере и эволюции информационного противоборства.
4. Классификация — в статье выделены и структурированы одиннадцать парадигм анализа информационных войн.
5. Индукция — автор приходит к общим выводам о закономерностях и особенностях информационных войн, изучая частные примеры.
6. Дедукция — от общих теоретических концепций (парадигм) автор переходит к конкретным примерам, объясняя механизмы информационного воздействия.

Результаты анализа

С точки зрения субъектно-объектной классификации субъекты информационного воздействия можно разделить на следующие основные группы:

1. Производители информации — те, кто создает, генерируют и распространяет информацию. К ним относятся: СМИ и СМК (новостные агентства, издательства, вещательные компании), поставщики информации (базы данных, библиотеки, архивы), создатели контента (авторы, журналисты, блогеры, деятели культуры, иные лидеры общественного мнения (ЛОМы)).
2. Владельцы (правообладатели) и контролеры информации (субъекты, которые обладают правом собственности на информацию и (или) контролируют информационные ресурсы), к ним относятся: правительственные структуры (государственные учреждения, министерства, регулирующие органы), корпорации (компании, организации, учреждения), физические лица (частные коллекционеры, исследователи, эксперты).

Объекты информационной войны также можно разделить на две основные группы:

1. Информационно-технические системы (ЭВМ, в том числе центры обработки данных, сервера; каналы связи, в том числе принимающие и передающие станции, проводные и

беспроводные каналы передачи данных; информационно-аналитические системы (программы) и т.д.).

2. Психика и сознание (мировоззрение) потребителей и пользователей информации (физические и юридические лица, которые получают доступ, извлекают и используют информацию для различных целей), например, граждан (общественность, потребители), профессионалов (эксперты, исследователи, аналитики), сотрудников предприятий (организаций и учреждений, не относящихся к субъектам информационного влияния).

С точки зрения ключевых акцентов информационной войны можно выделить одиннадцать парадигм, содержащихся в трудах российских и зарубежных авторов (рис. 1):

1. Системная
2. Инновационно-синергетическая
3. Эволюционная
4. Философская
5. Психологическая
6. Социокультурная (как разновидность психологического подхода)
7. Коммуникативная (как разновидность психологического подхода)
8. Конфликтологическая (как разновидность психологического подхода)
9. Кибернетическая (техническая)
10. Геополитическая
11. Экономическая

Рис. 1. Основные парадигмы анализа информационной войны в современной науке

Необходимо заметить, что в одних и тех же работах зачастую рассматриваются различные аспекты информационной войны, в связи с чем их можно отнести сразу к нескольким парадигмам (справедливо утверждать о мультипарадигмальности таких исследований).

Наиболее общей является **системная парадигма**, которая рассматривает информационные войны как сложные системы, включающие различные взаимосвязанные компоненты (источники информации, сети и приемники, сознание, подсознание людей, когниции и иные объекты) и подсистемы, взаимодействующие между собой для достижения определенных целей. Теория систем подчеркивает важность понимания связей и циклов обратной связи в этих системах, а также свойств, возникающих в результате их взаимодействий. В работах большого количества авторов присутствует системный подход, однако наиболее отчетливо он выражен в трудах Т. Рона [62], М. Либики [53], С. Манна [63], С.П. Расторгуева [33], В.В. Цыганова [43, с. 40], С.Н. Гриняева [9].

Инновационно-синергетическая парадигма фокусируется на инновационных и синергетических аспектах информационной войны, подчеркивая роль информации в стимулировании инноваций и изменений, создании новых возможностей и угроз. При этом отмечается важность понимания того, каким образом информационные потоки и взаимодействия порождают новые идеи, продукты и услуги, а также как они, в свою очередь, формируют ход конфликтов. К авторам, исследующим роль инноваций и синергии в развитии информационных войн, можно отнести, например, Г.Г. Почепцова [32], С. Манна [63],

Дж. Аркилла и Д. Ронфельдта [47], Т. Рида [61], Дж. Ная мл. [57, 58, 59, 60], М. Либики [53] и др.

Анализ информационных войн в контексте эволюционного развития характерен для **эволюционной парадигмы**, при этом преобразования характера ведения информационной войны, социальных связей, объемов, способов и форм создания и распространения информации рассматриваются как ключевые драйверы адаптации и изменений, что, в свою очередь, определяет выбор стратегии и тактики и общую эволюцию конфликтов. Данный подход также находит отражение в работах многих ученых, но наиболее явно это заметно в трудах Л.Ю. Медовкиной [22], Ш.С. Сулеймановой и Е.А. Назаровой [37], М. Кастельса [12, 13], Э. Тоффлера [40, 41], А. В. Манойло [20], Дж. Аркилла и Д. Ронфельдта [47].

Философская парадигма — изучение информационных войн осуществляется с помощью аналитической философии. Сторонниками данной парадигмы можно назвать В.В. Кафтана [15] и Д.В. Биндаса, рассматривающего в своей диссертационной работе — «Философская парадигма информационной войны и обеспечения медиабезопасности» информационную войну как процесс, направленный на деструктивное воздействие на эпистемологию противника, то есть на систему знаний и представлений, человеческий разум, прежде всего тех, кто принимает ключевые решения в области войны или мира [2].

Психологическая (когнитивная, ментальная, консциентальная) парадигма — одна из наиболее широких и распространенных, фокусируется на психологическом воздействии на гражданское население и военнослужащих, понимании когнитивных процессов, методов влияния и защиты от них.

Человеческое поведение изучается многими науками, в частности, антропологией, психологией, социологией, политологией, психолингвистикой, в значительной степени оно является объектом когнитивной психологии и связано с формированием когниций (знаний), верований, политических установок.

Психологический подход прослеживается в трудах многих авторов. В рамках него можно выделить еще несколько квази-парадигм, а именно: социокультурная, коммуникативная, конфликтологическая. Также к данной парадигме можно отнести такие синонимические наименования войн, выделяемые различными авторами, как мемелогическая война, консциентальная война, ментальная война, когнитивная война, война на дегуманизацию, война на духовную дезориентацию и др.

В «чистом виде» психологическая война анализируется Полом Лайнбарджером, Герхардом Зазворка, Дж. Наем мл., И.Н. Панариным, Д.Ю. Перетолчиным, И. Стечкиным.

Отдельно стоит отметить научные труды Джозефа Ная младшего, предложившего термин «мягкая сила» для обозначения формы политической власти, позволяющей завуалированно добиваться от кого-либо желаемых результатов на основе добровольного участия и симпатии в отличие от жесткой силы, при использовании которой главными инструментами получения господства являются подкуп и принуждение с помощью физического насилия (кинетического оружия) [57, 58]. Впоследствии эта идея получила развитие, и в научный оборот были введены термины «умная сила» («smart power») (способ получения власти, использующий сочетание инструментов жесткой силы и мягкой силы) [59] и «острая сила» («sharp power») (способ получения власти, а также внешнеполитическая деятельность с использованием быстрых («острых») цифровых средств, заключающаяся во вмешательстве во внутренние дела прежде всего «демократических» государств (так называемыми «авторитарными режимами») с целью манипулирования общественным мнением населения и подталкиванием его на подрывные действия в отношении собственных правительств [60].

Психологический подход в информационной войне может включать использование различных методов психологического давления, например, распространение слухов и ложной информации, угроз, дезинформации и иных техник (приемов, методов, инструментов). Перечень инструментария крайне широк и включает в себя методы когнитивной психологии, пропаганды, психолингвистики, PR, маркетинга, имиджелогии, фрейминга и многое другое, а их подробное описание представлено в разнообразных книгах, учебных пособиях,

монографиях и научных статьях, в связи с чем приведем лишь некоторых авторов, в трудах которых приводится анализ данных аспектов: Э. Бернейс [1], Ж. Бодрийяр, Т. Адорно, М. Хоркхаймер, Л. Альтюссер, П. Бурдье, Дж. Най мл. [57, 58, 59, 60], Дж. Овертон[2][26], Т. Рид [61], Г.Г. Почепцов [30, 31, 32], Р.Т. Мухаев [24, 25], А.В. Манойло [19, 20], И.Н. Панарин [28, 29]. Также существует немало работ по тематике цветных революций, в которых, кроме прочего, также анализируются приемы информационно-психологического давления и (или) информационные операции. Наиболее известными трудами по данной тематике являются работы Д. Шарпа [44], Дж. Голдстоуна [7], Т. Гарра [6], Э. Люттвака [18], Т. Скочпол [34], Ш. Эйзенштадта [46], С. Московичи [23], Г.Г. Почепцова [31], А.В. Манойло [19, 20], И.Н. Панарина [28, 29].

Социокультурная парадигма (как разновидность психологического подхода): информационные войны анализируются в контексте социокультурных факторов, например, таких как культурные и языковые особенности, которые могут влиять на эффективность информационных операций. Для закрепления выявленных закономерностей современные эксперты ввели новый термин — «борьба культур», под которым понимают навязывание противнику собственного мировоззрения, подмену национальной идентичности (внедрение антиидей), что может привести не к обогащению собственной культуры, а, наоборот, к ее разрушению [25, с. 229]. К данной парадигме также принадлежит значительное число российских и зарубежных ученых, вот некоторые из них: Р.Т. Мухаев [25], О.С. Иссерс [11], Е.Л. Головлева [8], С.В. Ткаченко [39], Дж. Най мл. [57, 58, 59, 60], Д. Кэри [49].

Коммуникативная парадигма (как разновидность психологического подхода): рассмотрение информационной войны в качестве коммуникативной технологии, изучение характера и способов коммуникативных интеракций, возникающих между субъектами информационного противоборства.

К данному подходу, как и к предыдущим можно отнести значительное число авторов. Так, например, О.В. Красовская анализируя материалы, посвященные геополитическому информационному противостоянию России и Украины, в период с 2013 г. — по настоящее время, дает развернутую характеристику коммуникативной структуре информационной войны, ее субъектного состава, пространства и специфики речевого взаимодействия между оппонентами и приходит к выводу о том, что в условиях информационного противоборства, которое можно рассматривать как процесс формирования коллективной идентичности, происходит активное взаимодействие коммуникаторов, представляющих различные социальные группы. Данный процесс характеризуется высокой интенсивностью обмена информацией и направлен на расширение коммуникационного пространства, преодоление монологических форм общения и интеграцию невербальных элементов в вербальный контекст [17].

Существует и иная позиция, на основании которой: «Информационная война интерпретируется как коммуникативная технология, посредством которой осуществляются разведывательные и политико-психологические действия в отношении противника. Поскольку информация способна формировать у объекта информационного воздействия выгодные субъекту войны когнитивные ориентации, целью информационной войны является достижение информационного превосходства и защита собственного информационного капитала» [45].

На взгляд Л.Л. Штофер, коммуникативный и психологический подходы соединяются в научных работах Г.Г. Почепцова: «Синтезом психологического подхода и коммуникативного направления является концепция Г. Почепцова. Он определяет информационную войну как «коммуникативную технологию по воздействию на массовое сознание с кратковременными и долговременными целями», видя в ней несанкционированную работу в чужом информационном пространстве» [45], при этом Почепцов отдельно отмечает, что

[2] The «Overton Window». Mackinac for public policy — URL: https://www.mackinac.org/OvertonWindow (дата обращения 29.12.2024).

коммуникация в информационном пространстве последовательно влияет на когнитивное и физическое пространства [31, с. 9].

Другие ученые, труды которых можно отнести к данной парадигме: А.Д. Васильев и Ф.Е. Подсохин [5], О.С. Иссерс [11], М. Кастельс [12, 13], М. Маклюэн, Ю. Хабермас, Г. Лассуэлл, П. Лазарсфельд, Т.А. ван Дейк, Н. Коулдри.

Конфликтологическая парадигма (как разновидность психологического подхода) трактует информационную войну как политическое и военное противостояние, конфликт международного и (или) внутригосударственного уровня, при этом акцент делается на рассмотрении феномена с точки зрения конфликтологии. Среди авторов, изучающих проблематику информационного противоборства с данной точки зрения, можно выделить следующих: А.В. Брега [3], М.Ю. Зеленков [10], Д. Б. Фролов [42], Л. И. Никовская [27].

Кибернетическая парадигма (технический подход) базируется на анализе архитектуры кибератак и методов кибершпионажа, разработке микроэлектроники, радиоэлектронных средств воздействия и противодействия им, работе с каналами связи, криптографией, применении методов кибернетики, теории управления, теории систем, технологий информационной безопасности, хакерских атак, кибершпионажа и других технических и кибернетических аспектах.

Основная цель информационной кампании в данном случае — разрушить информационную систему противоборствующей стороны, либо нарушить ее работоспособность, препятствовать получению, обработке и использованию информации, либо способствовать ее искажению, фрагментации, перехвату и прочим негативным явлениям, что в итоге должно привести к поражению противника в краткосрочной, среднесрочной или долгосрочной перспективе. Средствами информационно-технического давления являются в том числе кибератаки (взломы, кражи данных с использованием компьютерных средств), радиоэлектронное воздействие, физическое воздействие на средства связи и каналы коммуникации и др.

К представителям данной парадигмы можно отнести основоположника термина «информационная война» — Т. Рона [62], создателя теории «управляемого хаоса» С. Манна [46], видных российских ученых, одного из основоположников отечественной научной школы информационного противоборства, С.П. Расторгуева [33], член-корреспондента Академии военных наук С.И. Макаренко, австралийского специалиста по коммуникациям К. Галлоуэя, выдвинувшего концепцию кибер-прикосновения («кибер-PR», «киберосязание», динамическое коммуникационное прикосновение) [51], британского профессора Дэвида Бетца [48], Энтони Х. и Джастина Г. Кордесмана [54], М. Либики [53], Д. Аркилла и Д. Ронфельдта [47], Д. Деннинг [55], С. А. Гриняева [9] и других.

Сторонниками **геополитической парадигмы** при рассмотрении сущности информационной войны акцент делается на использовании информационных технологий в решении задач внешней политики и, в первую очередь, достижении гуманитарной, а не военной победы для реализации политического влияния и контроля за определенными территориями (достижении геополитических целей) [42]. К авторам, рассматривающим информационную войну в качестве инструмента решения геополитических задач, в целом можно отнести многих ученых, однако наиболее явно это прослеживаются в трудах И.Н. Панарина, Д.Б. Фролова, З. Бжезинского, Г. Киссинджера, Э. Люттвака, М. Либики, А.В. Манойло, Г.Г. Почепцова, А.Г. Дугина, К.В. Сивкова, С.В. Ткаченко, И.А. Михальченко. Особенностью данного подхода, как и системного, является его обширность, в связи с чем работы, в которых он представлен, зачастую включают в себя и другие парадигмы.

Наконец, в научной литературе достаточно широко распространен подход, который рассматривает информационное противоборство через призму экономических процессов, интересов и последствий — **экономическая парадигма**. Так, например, в работе «Манипуляция сознанием» С.Г. Кара-Мурза анализирует механизмы воздействия на общественное сознание с целью достижения экономических и политических целей [14]; В.В. Цыганов является автором книги «Информационные войны в бизнесе и политике: Теория

и методология» [43]; в публикациях «Третья волна» (1980 г.) и «Метаморфозы власти» (1990 г.) американский социолог, один из авторов концепции постиндустриального общества, Э. Тоффлер анализирует переход к информационному обществу и роль информации как ресурса, в том числе экономического [40, 41]; М. Кастельс в монографии «Информационная эпоха: экономика, общество и культура» подробно рассматривает, как информационные технологии трансформируют экономику (главы о сетевой экономике и глобализации) [12]; Дж. Най в своих трудах также рассуждает, как информация и коммуникации используются для достижения экономических и политических целей [57, 58, 59, 60]; подобный подход прослеживается в исследованиях и других ученых.

Выводы

Таким образом, проведенный анализ показал, что в постиндустриальном (информационном) обществе, где основным ресурсом стали информация и знания, информационная война занимает одно из центральных мест в структуре социальных, политических и экономических процессов. Современная информационная война прошла долгий процесс эволюции и стала значительно более востребованным и эффективным средством поражения противника нежели чем было ранее в силу многих причин, прежде всего — ввиду появления в середине XX в. ядерного оружия, последовавшей на рубеже XX—XXI вв. новой «информационной революции», колоссальному рывку СМК и повышению доступности средств коммуникации, развитию техник информационно-психологического воздействия, и в настоящее время представляет собой крайне широкое явление, включающее не только целенаправленные действия по использованию цифровых средств коммуникации для получения превосходства над противником путем различных манипуляций с информацией (в том числе причинения ущерба, кражи и пр.) и информационными системами, а также защиты собственных информационных систем, но и воздействие на его общественное мнение, психоэмоциональное состояние и поведение.

В настоящее время научная литература изобилует работами по изучению широкого спектра вопросов информационной войны, были выявлены одиннадцать парадигм ее анализа, при этом отсутствует единство мнений на ее сущность. Различные подходы позволяют рассматривать информационное противоборство с разных точек зрения, но их границы часто размыты. Вместе с тем, эти парадигмы не являются взаимоисключающими, и всеобъемлющее понимание информационных войн, вероятно, требует интеграции идей с разных точек зрения. Признавая сильные стороны и ограничения каждой парадигмы, исследователи и практики, в том числе с опорой на данную статью, могут разработать более структурированные и эффективные подходы к их анализу, акцентируя внимание на общих тенденциях и на конкретных аспектах.

Также необходимо заметить, что, зачастую, в научных работах повторяются схожие тезисы и смыслы. С одной стороны, это может быть не только недостатком, но и признаком сложившегося в науке консенсуса и устойчивых дискурсов, с другой — в определенном смысле усложняет процесс научного творчества ввиду необходимости изучать практически идентичные тексты. Также в современном мире ключевую роль играет работа с большими данными, что ставит вопрос о значительном устаревании работ с опорой на чрезвычайно малое их количество (единичные примеры, в лучшем случае — десятки, крайне редко — сотни), которые возводятся в правило и могут не обеспечивать достаточно емкого и всеобъемлющего анализа исследуемой проблемы в условиях все возрастающих требований.

Тем не менее, автором были выявлены существующие парадигмы исследования информационных войн в научной литературе, сформулированы их основные характеристики, представители, сходства и различия, обозначены механизмы влияния, проведена их классификация, определено место информационного противоборства в структуре постиндустриального (информационного) общества, кратко представлена эволюция данного явления в контексте технологических и социальных изменений, что является теоретической значимостью работы.

По мере увеличения числа случаев проявления информационной агрессии и защиты от нее, а также последующего научного анализа данных явлений будет накапливаться еще больший материал для формирования новых концепций и парадигм, осмысления ключевых технологий информационной войны. Дальнейшие исследования могут быть направлены на изучение специфики информационных войн в условиях искусственного интеллекта и больших данных.

Литература

1. Бернейс Э. Пропаганда / Пер. с англ. И. Ющенко. - М.: Hippo Publishing, 2010. - 176 с.
2. Биндас Д.В. Философская парадигма информационной войны и обеспечения медиабезопасности: диссертация ... кандидата философских наук: 5.7.8. - М.: Московский государственный институт международных отношений, 2023. - 186 с.
3. Брега А.В. Управление политическим конфликтом // Гуманитарные науки. Вестник Финансового университета. - 2014. - № 1 (13). - С. 33-37.
4. Василенко И. Политология: базовый курс. - 6-е изд., перераб. и доп. - М.: Издательство «Э», 2016. - 528 с.
5. Васильев А.Д., Подсохин Ф.Е. Информационная война: лингвистический аспект // Политическая лингвистика. - 2016. - № 2. – С. 10-16.
6. Гарр Т.Р. Почему люди бунтуют. - СПб.: Питер, 2005. - 461 с.
7. Голдстоун Д. Революции. Очень краткое введение / Пер. с англ. А. Яковлева. - М.: Изд-во Института Гайдара, 2017. - 200 с.
8. Головлева Е.Л. Основы межкультурной коммуникации. - Ростов-на-Дону: Феникс, 2008. - 222 с.
9. Гриняев С.Н. Поле битвы - киберпространство: теория, приемы, средства, методы и средства ведения информационной войны. - Минск: Харвест, 2004. - 448 с.
10. Зеленков М.Ю. Социальная конфликтология (базовый курс). - М.: Юридический институт МИИТа, 2011. - 272 с.
11. Иссерс О.С. Речевое воздействие: учеб. пособие для студентов, обучающихся по специальности «Связи с общественностью». - М.: Флинта: Наука, 2009. - 224 с.
12. Кастельс М. Информационная эпоха: экономика, общество и культура / Пер. с англ. под науч. ред. О.И. Шкаратана. - М.: ГУ ВШЭ, 2000. - 608 с.
13. Кастельс М. Власть коммуникации: учеб. пособие / Пер. с англ. Н.М. Тылевич; под науч. ред. А.И. Черных. - М.: Изд. дом Высшей школы экономики, 2016. - 564 с.
14. Кара-Мурза С.Г. Манипуляция сознанием [Электронный ресурс]. - М.: Алгоритм, 2017. - 528 с.
15. Кафтан В.В. Гуманитарный фактор современной информационной войны // Гуманитарные науки. Вестник Финансового университета. - 2017. - № 7 (1). - С. 27-31.
16. Клаузевиц К. О войне. - М.: Госвоениздат, 1934. - 448 с. / Clausewitz K. Vom Krieg. 1832/34.
17. Красовская О.В. Информационная война как коммуникативный феномен // Политическая лингвистика. - 2016. - № 4. - С. 123-130.
18. Люттвак Э. Государственный переворот: Практическое пособие / Пер. с англ. - М.: Русский Фонд Содействия Образованию и Науке, 2012. - 326 с.
19. Манойло А.В. Гибридные войны и цветные революции в мировой политике // Право и политика. - 2015. - № 7. - С. 918-929.
20. Манойло А.В. Информационные операции современной гибридной войны: учебное пособие. - М.: Горячая линия - Телеком, 2023. - 490 с.
21. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. - СПб.: Наукоемкие технологии, 2017. - 546 с.
22. Медовкина Л.Ю. Эволюция информационных войн от древности к современности // Известия ТулГУ. Гуманитарные науки. - 2017. - № 3. – С. 15-23.
23. Московичи С. Век толп. Исторический трактат по психологии масс / Пер. с фр. - М.: Центр психологии и психотерапии, 1998. - 480 с.

24. Мухаев Р.Т. Геополитика: учебник для студентов вузов. - 2-е изд., перераб. и доп. - М.: ЮНИТИ-ДАНА, 2017. - 839 с.
25. Мухаев Р.Т. Медиаполитика: учебник. - М.: ИНФРА-М, 2024. - 401 с.
26. Никишин В.Д. Вредоносная информация в интернет-медиа: «окно Овертона» и взаимосвязь деструктивных сетевых течений // Lex Russica. - 2022. - № 11 (192). – С. 131-148.
27. Озеров В.В., Никовская Л.И. Информационная война в зеркале теории конфликта // Социально-политические исследования. - 2022. - № 4 (17). – С. 34-47.
28. Панарин И.Н. Первая мировая информационная война. Развал СССР. - СПб.: Питер, 2010. - 256 с.
29. Панарин И.Н. Гибридная война и Ялта-2. - М.: Горячая линия - Телеком, 2022. - 452 с.
30. Почепцов Г.Г. Информационные войны. - М.: Рефл-бук, Ваклер, 2000. - 576 с.
31. Почепцов Г.Г. Революция.com. Основы протестной инженерии. - М.: Европа, 2005. - 532 с.
32. Почепцов Г.Г. Информационные войны. Новый инструмент политики. - М.: Алгоритм, 2015. - 254 с.
33. Расторгуев С.П. Информационная война. - М.: Радио и связь, 1999. - 416 с.
34. Скочпол Т. Государства и социальные революции: сравнительный анализ Франции, России и Китая / Пер. с англ. С. Моисеев; науч. ред. перевода Д. Карасев. - М.: Изд-во Института Гайдара, 2017. - 552 с.
35. Сорокин И.О. Роль СМИ и информационных технологий в гибридной войне // Актуальные и перспективные научные исследования. - 2024. - № 9. - С. 248-259.
36. Суворов А.В. Наука побеждать. - М.: Издательство АСТ, 2019. - 320 с.
37. Сулейманова Ш.С., Назарова Е.А. Информационные войны: история и современность: Учебное пособие. - М.: Международный издательский центр «Этносоциум», 2017. - 124 с.
38. Сунь-Цзы. Трактат о военном искусстве. - М.: Военное издательство Министерства обороны СССР, 1955. - 123 с.
39. Ткаченко С.В. Информационная война против России. - СПб.: Питер, 2011. - 224 с.
40. Тоффлер Э. Третья волна. - М.: ООО «Фирма «Издательство АСТ», 1999. - 784 с.
41. Тоффлер Э. Метаморфозы власти / Пер. с англ. - М.: ООО «Издательство АСТ», 2003. - 669 с.
42. Фролов Д.Б. Информационное противоборство в сфере геополитических отношений: диссертация … доктора политических наук: 10.01.10 - М.: Рос. акад. гос. службы при Президенте РФ, 2006. - 426 с.
43. Цыганов В.В., Бухарин С.Н. Информационные войны в бизнесе и политике: Теория и методология. - М.: Академический Проект, 2007. - 336 с.
44. Шарп Д. От диктатуры к демократии: Стратегия и тактика освобождения / Пер. с англ. Н. Козловской. - М.: Новое издательство, 2005. - 84 с.
45. Штофер Л.Л. Информационная война как радикальная форма политической борьбы // Гуманитарий Юга России. - 2018. - Том 7. - № 4. - С. 158-174.
46. Эйзенштадт Ш. Революция и преобразование обществ. Сравнительное изучение цивилизаций / Пер. с англ. А.В. Гордона; под ред. Б.С. Ерасова. - М.: Аспект Пресс, 1999. - 416 с.
47. Arquilla J., Ronfeldt D. (Eds.). Networks and Netwars: The Future of Terror, Crime, and Militancy. - Санта-Моника: RAND Corporation, 2001. - 372 p.
48. Betz D. Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power. - London: C Hurst & Co Publishers Ltd, 2015. - 261 p.
49. Carey J.W. Communication as culture: Essays on media and society. - Psychology Press, 1992. - 241 p.
50. FMI 2-22.9. Open-Source Intelligence, December 2006. - URL: https://info.publicintelligence.net/fmi2-22-9.pdf (дата обращения: 24.01.2025).
51. Galloway C. Cyber-PR and «Dynamic touch» // Public relations review. - 2005. - № 31 (4). - pp. 572-577.

52. Joint Doctrine for Information Operations (JP 3-13). - 1998. - URL: https://irp.fas.org/doddir/dod/jp3_13.pdf (дата обращения: 24.01.2025).
53. Libicki M.C. What is Information Warfare? - Washington: National Defense University, 1995. - 110 p.
54. Cordesman A., Cordesman J. Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland. - Bloomsbury Publishing, 2001. - 189 p.
55. Denning D. Information warfare and security. - ACM Press, 1999. - 522 p.
56. Military concept for NATO strategic communications. - 2010. - URL: https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf (дата обращения: 24.01.2025).
57. Nye J. Bound to Lead: The Changing Nature of American Power. - New York: Basic Books, 1990. - 307 p.
58. Nye J. Soft power: The Means to success in world politics. - New York: Public Affairs, 2004. - 191 p.
59. Nye J. Smart power and the war on terror // Asia-Pacific Review. - 2008. - № 15 (1). - pp. 1-8. - DOI: 10.1080/13439000802134092.
60. Nye J. How Sharp Power Threatens Soft Power. Foreign Affairs, 2018, https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power. (дата обращения 17 февраля 2025).
61. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. - Farrar, Straus and Giroux, 2020 - 512 p.
62. Rona T.P. Weapon Systems and Information War (Boeing, 1976). - URL: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf (дата обращения: 23.01.2025).
63. Steven R. Mann. Chaos Theory and Strategic Thought (1992). - URL: https://apps.dtic.mil/sti/pdfs/ADA528321.pdf (дата обращения: 24.01.2024).
64. TS-3600.1. Information Warfare (1992). - URL: https://archive.org/details/14F0492Doc01DirectiveTS3600.1/mode/2up (дата обращения: 23.01.2024).

References

1. Bernays E. Propaganda [Propaganda]. Moscow, Hippo Publishing Publ., 2010, 176 p. (In Russian).
2. Bindas D.V. Filosofskaya paradigma informatsionnoy voyny i obespecheniya mediabezopasnosti [Philosophical Paradigm of Information Warfare and Media Security]. Moscow, MGIMO Publ., 2023, 186 p. (In Russian).
3. Brega A.V. Upravlenie politicheskim konfliktom [Management of Political Conflict]. Gumanitarnye nauki. Vestnik Finansovogo universiteta [Humanitarian Sciences. Bulletin of the Financial University], 2014, I. 1 (13), pp. 33-37. (In Russian).
4. Vasilenko I. Politologiya: bazovyy kurs [Political Science: Basic Course]. 6th ed., revised and expanded. Moscow, E Publ., 2016, 528 p. (In Russian).
5. Vasiliev A.D., Podsokhin F.E. Informatsionnaya voyna: lingvisticheskiy aspekt [Information Warfare: Linguistic Aspect]. Politicheskaya lingvistika [Political Linguistics], 2016, I. 2, pp. 10-16. Available at: https://cyberleninka.ru/article/n/informatsionnaya-voyna-lingvisticheskiy-aspekt (Accessed: 10.02.2025). (In Russian).
6. Garr T.R. Pochemu lyudi buntuyut [Why Men Rebel]. St. Petersburg, Piter Publ., 2005, 461 p. (In Russian).
7. Goldstone D. Revolyutsii. Ochen' kratkoe vvedenie [Revolutions: A Very Short Introduction]. Moscow, Gaidar Institute Publ., 2017, 200 p. (In Russian).
8. Golovleva E.L. Osnovy mezhkul'turnoy kommunikatsii [Fundamentals of Intercultural Communication]. Rostov-on-Don, Feniks Publ., 2008, 222 p. (In Russian).

9. Grinyaev S.N. Pole bitvy – kiberprostranstvo: teoriya, priyomy, sredstva, metody i sredstva vedeniya informatsionnoy voyny [Battlefield – Cyberspace: Theory, Techniques, Tools, Methods and Means of Information Warfare]. Minsk, Kharvest Publ., 2004, 448 p. (In Russian).
10. Zelenkov M.Yu. Sotsial'naya konfliktologiya (bazovyy kurs) [Social Conflictology (Basic Course)]. Moscow, Yuridicheskiy institut MIITa Publ., 2011, 272 p. (In Russian).
11. Issers O.S. Rechevoe vozdeystvie [Speech Influence]. Moscow, Flinta: Nauka Publ., 2009, 224 p. (In Russian).
12. Castells M. Informatsionnaya epokha: ekonomika, obshchestvo i kul'tura [The Information Age: Economy, Society and Culture]. Moscow, GU VShE Publ., 2000, 608 p. (In Russian).
13. Castells M. Vlast' kommunikatsii [The Power of Communication]. Moscow, Izdatel'skiy dom Vysshey shkoly ekonomiki Publ., 2016, 564 p. (In Russian).
14. Kara-Murza S.G. Manipulyatsiya soznaniem [Manipulation of Consciousness]. Moscow, Algoritm Publ., 2017, 528 p. (In Russian).
15. Kaftan V.V. Gumanitarnyy faktor sovremennoy informatsionnoy voyny [Humanitarian Factor of Modern Information Warfare]. Gumanitarnye nauki. Vestnik Finansovogo universiteta [Humanitarian Sciences. Bulletin of the Financial University], 2017, I. 7 (1), pp. 27-31. (In Russian).
16. Clausewitz K. O voyne [On War]. Moscow, Gosvoenizdat Publ., 1934, 448 p. (In Russian). / Clausewitz K. Vom Krieg. 1832/34.
17. Krasovskaya O.V. Informatsionnaya voyna kak kommunikativnyy fenomen [Information Warfare as a Communicative Phenomenon]. Politicheskaya lingvistika [Political Linguistics], 2016, I. 4, pp. 123-130. (In Russian).
18. Luttwak E. Gosudarstvennyy perevorot: Prakticheskoye posobiye [Coup d'État: A Practical Handbook]. Moscow, Russkiy Fond Sodeystviya Obrazovaniyu i Nauke Publ., 2012, 326 p. (In Russian).
19. Manoylo A.V. Gibridnyye voyny i tsvetnyye revolyutsii v mirovoy politike [Hybrid Wars and Color Revolutions in World Politics]. Pravo i politika [Law and Politics], 2015, I. 7, pp. 918-929. (In Russian).
20. Manoylo A.V. Informatsionnyye operatsii sovremennoy gibridnoy voyny [Information Operations of Modern Hybrid Warfare]. Moscow, Goryachaya liniya – Telekom Publ., 2023, 490 p. (In Russian).
21. Makarenko S.I. Informatsionnoye protivoborstvo i radioelektronnaya bor'ba v setetsentricheskikh voynakh nachala XXI veka [Information Warfare and Electronic Warfare in Network-Centric Wars of the Early 21st Century]. St. Petersburg, Naukoemkiye tekhnologii Publ., 2017, 546 p. (In Russian).
22. Medovkina L.Yu. Evolyutsiya informatsionnykh voyn ot drevnosti k sovremennosti [Evolution of Information Warfare from Antiquity to the Present]. Izvestiya TulGU. Gumanitarnyye nauki [Izvestiya Tula State University. Humanities], 2017, I. 3, pp. 15-23 (In Russian).
23. Moscovici S. Vek tolp [The Age of the Crowd]. Moscow, Tsentr psikhologii i psikhoterapii Publ., 1998, 480 p. (In Russian).
24. Mukhaev R.T. Geopolitika [Geopolitics]. Moscow, YUNITI-DANA Publ., 2017, 839 p. Available at: https://znanium.com/catalog/product/1028710 (Accessed: 14.12.2024). (In Russian).
25. Mukhaev R.T. Mediapolitika [Media Policy]. Moscow, INFRA-M Publ., 2024, 401 p. Available at: https://znanium.ru/catalog/product/2117168 (Accessed: 24.12.2024). (In Russian).
26. Nikishin V.D. Vredonosnaya informatsiya v internet-media: «okno Overtona» i vzaimosvyaz destruktivnykh setevykh techeniy [Harmful Information in Internet Media: The Overton Window and the Interconnection of Destructive Network Trends]. Lex Russica, 2022, I. 11 (192), pp. 131-148 (In Russian).
27. Ozerov V.V., Nikovskaya L.I. Informatsionnaya voyna v zerkale teorii konflikta [Information Warfare in the Mirror of Conflict Theory]. Sotsial'no-politicheskiye issledovaniya [Socio-Political Studies], 2022, I. 4 (17), pp. 34-47 (In Russian).
28. Panarin I.N. Pervaya mirovaya informatsionnaya voyna. Razval SSSR [The First World Information War. The Collapse of the USSR]. St. Petersburg, Piter Publ., 2010, 256 p. (In Russian).

29. Panarin I.N. Gibridnaya voyna i Yalta-2 [Hybrid War and Yalta-2]. Moscow, Goryachaya liniya - Telekom Publ., 2022, 452 p. (In Russian).
30. Pocheptsov G.G. Informatsionnye voyny [Information Wars]. Moscow, Refl-buk, Vakler Publ., 2000, 576 p. (In Russian).
31. Pocheptsov G.G. Revolyutsiya.com. Osnovy protestnoy inzhenerii [Revolution.com. Basics of Protest Engineering]. Moscow, Evropa Publ., 2005, 532 p. (In Russian).
32. Pocheptsov G.G. Informatsionnye voyny. Novyy instrument politiki [Information Wars. A New Tool of Politics]. Moscow, Algoritm Publ., 2015, 254 p. (In Russian).
33. Rastorguev S.P. Informatsionnaya voyna [Information Warfare]. Moscow, Radio i svyaz Publ., 1999, 416 p. (In Russian).
34. Skocpol T. Gosudarstva i sotsial'nyye revolyutsii [States and Social Revolutions]. Moscow, Gaidar Institute Publ., 2017, 552 p. (In Russian).
35. Sorokin I.O. Rol SMI i informatsionnykh tekhnologiy v gibridnoy voyne [The role of media and information technologies in hybrid warfare]. Aktualnye i perspektivnye nauchnye issledovaniya [Current and Prospective Scientific Research]. 2024, I. 9, pp. 248-259. (In Russian).
36. Suvorov A.V. Nauka pobezhdat [The Science of Victory]. Moscow, AST Publ., 2019, 320 p. (In Russian).
37. Suleymanova Sh.S., Nazarova E.A. Informatsionnye voyny: istoriya i sovremennost [Information Wars: History and Modernity]. Moscow, Mezhdunarodnyy izdatelskiy tsentr «Etnosotsium» Publ., 2017, 124 p. (In Russian).
38. Sun Tzu. Traktat o voennom iskusstve [The Art of War]. Moscow, Voennoe izdatelstvo Ministerstva oborony SSSR Publ., 1955, 123 p. (In Russian).
39. Tkachenko S.V. Informatsionnaya voyna protiv Rossii [Information War Against Russia]. St. Petersburg, Piter Publ., 2011, 224 p. (In Russian).
40. Toffler E. Tretya volna [The Third Wave]. Moscow, AST Publ., 1999, 784 p. (In Russian).
41. Toffler E. Metamorfozy vlasti [Metamorphoses of Power]. Moscow, AST Publ., 2003, 669 p. (In Russian).
42. Frolov D.B. Informatsionnoye protivoborstvo v sfere geopoliticheskikh otnosheniy [Information Warfare in the Sphere of Geopolitical Relations]. Moscow, Russian Academy of Public Administration under the President of the Russian Federation, 2006, 426 p. (In Russian).
43. Tsyganov V.V., Bukharin S.N. Informatsionnye voyny v biznese i politike: Teoriya i metodologiya [Information Wars in Business and Politics: Theory and Methodology]. Moscow, Akademicheskiy Proekt Publ., 2007, 336 p. (In Russian).
44. Sharp D. Ot diktatury k demokratii [From Dictatorship to Democracy]. Moscow, Novoye izdatel'stvo Publ., 2005, 84 p. (In Russian).
45. Shtofer L.L. Informatsionnaya voyna kak radikalnaya forma politicheskoy borby [Information war as a radical form of political struggle]. Gumanitariy Yuga Rossii [Humanitarian of the South of Russia]. 2018, V. 7, I. 4, pp. 158-174. (In Russian).
46. Eisenstadt S. Revolyutsiya i preobrazovaniye obshchestv [Revolution and the Transformation of Societies]. Moscow, Aspekt Press Publ., 1999, 416 p. (In Russian).
47. Arquilla J., Ronfeldt D. (Eds.). Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, RAND Corporation Publ., 2001, 372 p. Available at: http://www.rand.org/pubs/monograph_reports/MR1382/index.html (Accessed: 10.01.2025).
48. Betz D. Carnage and Connectivity: Landmarks in the Decline of Conventional Military Power. London, C Hurst & Co Publishers Ltd Publ., 2015, 261 p.
49. Carey J.W. Communication as culture: Essays on media and society. Psychology Press, 1992, 241 p.
50. FMI 2-22.9. Open Source Intelligence. Department of the Army, 2006, 161 p. Available at: https://info.publicintelligence.net/fmi2-22-9.pdf (Accessed: 24.01.2025).
51. Galloway C. Cyber-PR and «Dynamic touch». Public Relations Review. 2005, V. 31, I. 4, pp. 572-577.

52. JP 3-13. Joint Doctrine for Information Operations. Federation of American Scientists, 1998, 89 p. Available at: https://irp.fas.org/doddir/dod/jp3_13.pdf (Accessed: 24.01.2025).
53. Libicki M.C. What is Information Warfare? Washington, National Defense University Publ., 1995, 110 p.
54. Cordesman A., Cordesman J. Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland. Bloomsbury Publishing, 2001, 189 p.
55. Denning D. Information Warfare and Security. ACM Press, 1999, 522 p.
56. Military concept for NATO strategic communications. NATO 2010, 15 p. Available at: https://info.publicintelligence.net/NATO-STRATCOM-Concept.pdf (Accessed: 24.01.2025).
57. Nye J. Bound to Lead: The Changing Nature of American Power. - New York: Basic Books, 1990. - 307 p.
58. Nye J. Soft Power: The Means to Success in World Politics. New York, Public Affairs Publ., 2004, 191 p.
59. Nye J. Smart power and the war on terror // Asia-Pacific Review. - 2008. - № 15 (1). - pp. 1-8. - DOI: 10.1080/13439000802134092.
60. Nye J. How Sharp Power Threatens Soft Power. Foreign Affairs, 2018, https://www.foreignaffairs.com/articles/china/2018-01-24/how-sharp-power-threatens-soft-power. (Accessed: 17.02.2025).
61. Rid T. Active Measures: The Secret History of Disinformation and Political Warfare. Farrar, Straus and Giroux Publ., 2020, 512 p.
62. Rona T.P. Weapon Systems and Information War. Boeing, 1976, 86 p. Available at: https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Science_and_Technology/09-F-0070-Weapon-Systems-and-Information-War.pdf (Accessed: 23.01.2025).
63. Mann S.R. Chaos Theory and Strategic Thought. Defense Technical Information Center 1992, 16 p. Available at: https://apps.dtic.mil/sti/pdfs/ADA528321.pdf (Accessed: 24.01.2024).
64. TS-3600.1 Information Warfare. Internet archive, 1992, 4 p. Available at: https://archive.org/details/14F0492Doc01DirectiveTS3600.1/mode/2up (Accessed: 23.01.2024).