МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М.В. ЛОМОНОСОВА
ФАКУЛЬТЕТ ГЛОБАЛЬНЫХ ПРОЦЕССОВ

На правах рукописи

Лю Ци

Особенности современных информационных войн в контексте глобальных социальных трансформаций

Научная специальность: 5.5.4. Международные отношения,
глобальные и региональные исследования»

Диссертация
на соискание ученой степени
кандидата политических наук

Научный руководитель:
доктор социологических наук,
профессор В.В. Кочетков

Москва – 2026

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность исследования. Информационная война (information war) – противоборство сторон посредством распространения специально подготовленной информации и противодействия аналогичному внешнему воздействию на себя. Согласно Большой российской энциклопедии, это также «противоборство между двумя государствами или группами государств в информационном пространстве в целях нанесения ущерба государственным информационным системам, процессам и ресурсам, критически важным и другим объектам» [1]. Информационная война как явление непреложно сопровождает межнациональную, межстрановую, межблоковую и межцивилизационную конкуренцию на протяжении всей истории человечества.

В эпоху цифровизации резко увеличились возможности для ведения информационных войн, а развитие цифровых технологий и инфраструктуры значительно повысило зависимость противоборствующих сторон от информационно-коммуникационных технологий (ИКТ) и, следовательно, их уязвимость. Процесс цифровизации стал основным катализатором глобальных социальных трансформаций современности.

В последние десятилетия ни один конфликт не обходится без значительной информационной составляющей, что обуславливает гибридный характер современных конфликтов в целом.

Актуально и целесообразно выделить новые и ключевые свойства информационной войны в современную эпоху и пути минимизации ее негативных эффектов, а также успешного противостояния с противниками с использованием ее инструментов.

Современная цифровая эра предоставила принципиально новые технологические возможности для активизации информационных конфликтов. Технологии информационных войн, включая целенаправленное

[1] Информационная война/ Большая российская энциклопедия. URL:https://bigenc.ru/c/informatsionnaia-voina-2b7815 (дата обращения: 1.04.2025)

распространение дезинформации через социальные сети и другие интернет-ресурсы, а также использование технологий для создания фальшивых видео и аудиозаписей, применяются для манипуляций общественным мнением, что позволяет достигать политических целей вплоть до смены власти в государствах. Данные технологии стали важным инструментом как государственной, так и негосударственной политики, и могут достигать цели без использования экономического или военного давления. Однако эти же технологии могут использоваться для борьбы с дезинформацией. Например, машинное обучение может помочь в распознавании и фильтрации фейковой информации, а криптография обеспечивает безопасность передачи информации.

Социо-гуманитарные технологии также играют ключевую роль в информационных войнах, причем как для атакующей стороны, так и для обороняющейся, так как они базируются на данных и исследованиях политологии, социальных наук, психологии, лингвистики и нейрофизиологии. Психологические исследования позволяют понять, как люди реагируют на определенные виды информации, что может быть использовано для борьбы с дезинформацией. Социологические исследования помогают определить важные темы для общества и то, как поведение людей в интернете влияет на их мнение и действия.

Цифровая трансформация и сближение наук и технологий тесно связаны с глобальными трансформациями, которые ускорились в новом тысячелетии. Они изменяют структуру международных отношений, расширяют сферы конфликта и конкуренции. В результате информационные войны становятся все более разнообразными и важными в современном мире. Сложность информационных войн и их инструментария, а также разнообразие практик их использования требуют уточнения и систематизации стратегий по борьбе с ними в целях национальной безопасности.

Степень научной разработанности проблемы. В основе исследований информационной составляющей международных отношений лежат труды Г. Алмонда, Р. Арона, З. Бжезинского, И.М. Валлерстайна, А. Вендта, Дж. Денниса, Л. Гарта, Д. Истона, Г. Моргентау, Дж. Ная, Ю. Хабермаса, С. Хантингтона, Т. Хофа, В.И. Аникина, Е.П. Бажанова, А.Д. Богатурова, А.Г. Володина, Л.Е. Гришаевой, А.А. Громыко, А.Г. Дугина, С.С. Жильцова, А.Г. Задохина, Т.А. Закаурцевой, О.П. Иванова, О.Г. Карповича, Т.В. Кашириной, И.В. Кондакова, М.А. Кукарцевой, М.М. Лебедевой, А.В. Мальгина, М.М. Мчедловой, М.А. Неймарка, Е.Г. Пономаревой, Г.А. Рудова, Г.М. Сидоровой, И.В. Сурмы, А.В. Торкунова, К.А. Феофанова, П.А. Цыганкова, Т.А. Шаклеиной, В.В. Штоля, А.Д. Шутова, и др.[2] К настоящему

[2] Аникин В.И. О некоторых практических аспектах философии информационной цивилизации в международных отношениях // Человечество на границе тысячелетий: диалог цивилизаций: сборник материалов научно-практической конференции, Киев. 2003. С. 43; Аникин В.И., Моисеев А.В., Сурма И.В., Семенова О.В. Современные подходы в принятии внешнеполитических решений в Российской Федерации. М.: Русайс, 2021; Аникин В.И., Сурма И.В. Новые подходы к обеспечению национальной безопасности России // Россия и современный мир. М.: Канон+, 2016. С. 9-28; Бажанов Е.П., Бажанова Н.Е. Мир и война. М.: Восток-Запад, 2011, 335 с.; Бажанов Е.П., Бажанова Н.Е. Диалог и столкновение цивилизаций. М.: Весь мир, 2013; Бажанов Е.П., Бажанова Н.Е. Международные отношения в XXI веке. М.: «Восток-Запад», 2011; Бажанов Е.П. Россия между Западом и Востоком // Современный мир и геополитика. М.: Канон+, 2015. С. 9-47; Богатуров А.Д., Аверков В.В. История международных отношений 1945-2017. М.: Аспект Пресс, 2017; Богатуров А.Д. «Украинский вызов» и альтернативы внешней политики России // Научно-образовательный форум по международным отношениям. 2014. Т. 12. № 39. С. 6-16.; Володин А.Г. Становление полицентрического мироустройства как продолжение геополитических процессов XX века // Контуры глобальных трансформаций: политика, экономика, право. 2019. Т. 12. № 4. С. 6–31; Гришаева Л.Е. Устав ООН и новое мироустройство // Вестник РУДН. Серия: политология. 2015. Т.15. № 4. С. 92-102; Громыко А.А. Дилеммы Европейского оборонного союза // Контуры глобальных трансформаций: политика, экономика, право. 2019. Т. 12. № 2. С. 6–28; Громыко А.А. Глобальный мир: риски и возможности // Современная Европа. 2018. № 1. С. 137-147; Дугин А.Г. Концептуальные подходы к понятию «цивилизация» // Вестник московского университета. Сер. 18: Социология и политология. 2013. № 1. С. 33-41.; Жильцов С.С. Истоки украинского национализма // Вестник РУДН. Сер. Политические науки. 2014. № 4. С. 21-36.; Жильцов С.С. Технологии и механизмы борьбы за власть на Украине // Россия и современный мир. М.: Канон+, 2016. С. 451-470; Задохин А.Г., Чиджиев Б. Геополитика симбиоза «периферия-центр» и перспективы многополярного мира // Мировая политика. 2016. № 1 (13). С. 55-63; Гаврилова С.М., Закаурцева Т.А. Италия: опыт автономий как пример национально-государственного устройства // Вестник Дипломатической академии МИД России. Россия и Мир. 2017. № 2 (12). С. 71-80; Иванов О.П. Россия и НАТО: новая парадигма отношений // Россия и современный мир, М.: Канон+, 2016. С. 44-59; Иванов О.П. Россия и НАТО: точка невозврата // Обозреватель-Observer. 2015. № 1. С. 5-16; Карпович О.Г. Украинский кризис в контексте противостояния России и Запада // Вестник российской нации. 2016. № 6 52). С. 197-205; Карпович О.Г. Роль США в украинском кризисе (2013–2014-е гг.) // Международные отношения. 2016. № 2. С. 179-188; Аватков В.А., Каширина Т.В. Тенденции развития современных международных отношений // Обозреватель-Observer. 2017. № 11 (334). С. 5-15; Кондаков И.В., Соколов К.Б., Хренов Н.А. Цивилизационная идентичность в переходную эпоху: культурологический, социологический и искусствоведческий аспекты. М.: ПрогрессТрадиция, 2011; Кукарцева М.А. Политический нарратив – инструмент «формирования себя» в мировой политике // Обозреватель-Observer. 2013. № 4 (279). С. 100-109; Лебедева М.М., Кузнецов Д.А. Трансрегионализм – новый феномен мировой политики // Полис. Политические исследования. 2019. № 5. С. 71-84; Современные международные отношения: учебник / под ред. Торкунова А.В., Мальгина А.В. М.: Аспект-Пресс, 2012; Мчедлова М.М. Модернизация: политическая реинтерпретация концептуальных оснований и российский цивилизационный контекст // Россия реформирующаяся. 2013. № 12. С. 80-110; Неймарк М.А. «Мягкая сила» в мировой политике. Уточнение

время только в российской базе научной литературы РИНЦ – около 5 тыс. публикаций, непосредственно посвященных тематике информационных войн (подробно: п. 3.1). В последние годы изучение информационных войн приобрело особую актуальность в связи с началом Специальной войной операции России на Украине и активизацией борьбы объединений развивающихся стран во главе с Китаем и Россией за новый. Более справедливый миропорядок. Написанные в последние годы работы А.А. Алаудинова, А.В. и Д.В. Бакулиных, Гавра Д.П., Л.А. Гаврилова, Р.И. С.Г. Галагановой, С.Г Зарипова, М.Р. Егоровой, О.И. Калинина, Д.Ю. Кургиновой, В.А. Лукушина, А.В. Манойло, А.Н. Чумакова, О.В. Ярмака[3] и др. авторов посвящены новым аспектам разворачивания большой

проблемного поля. Часть 1. // Обозреватель-Observer. 2016. № 1 (312). С. 31-42; Неймарк М.А. «Умная сила»: к перспективам в мировой политике. Часть 2. // Обозреватель-Observer. 2016. № 2 (312). С. 67-77; Пономарева Е.Г., Рудов Г.А. «Цветные революции»: природа, символы, технологии // ОбозревательObserver. 2012. № 3 (266). С. 36-48; Пономарева Е.Г., Рудов Г.А. «Принцип домино»: мировая политика на рубеже веков. М.: Канон+, 2016; Пономарева Е.Г. Вывихнутый век. Кто его вправит? М.: Книжный мир, 2016; Феофанов К. А. Цивилизационная теория модернизации. М.: Издательские решения, 2016; Шаклеина Т. А. Лидерство и современный мировой порядок // Международная жизнь. 2015. Т. 13. № 43. С. 6-19; Штоль В.В. Холодная война как элемент системы противостояния Запада и России // Обозреватель-Observer. 2016. №10 (321). С. 1-29; Шутов А.Д. Теория и практика современной мировой политики // Вестник Дипломатической академии МИД России. Россия и мир. 2018. № 1 (15). С. 153-159; Цыганков П.А. Системный подход в теории международных отношений // Вестник МГУ. Сер.12: Политические науки. 2013. № 5. С. 3-25; Арон Р. Опиум интеллектуалов // Логос. 2005. № 6. С. 182-205.; Бжезинский З. Великая шахматная доска: господство Америки и его геостратегические императивы. М.: Международные отношения, 1999; Валлерстайн И. Есть ли будущее у капитализма?; пер. с англ. М.: Ин-т Гайдара, 2015; Wendt A. Social Theory of International Politics. Cambridge: Cambridge University Press. 1999;

[3] Алаудинов А.А., Манойло А.В. Когнитивная и ментальная составляющие современной гибридной войны// Вопросы политологии. 2024. Т. 14. № 2 (102). С. 583-591; Бирюков С.В., Чирун С.Н., Андреев А.В. Информационно-пропагандистские стратегии и технологии украинской элиты в информационной войне с Россией// PolitBook. 2023. № 2. С. 66-86; Гавра Д.П. Информационное противоборство: современное понимание, характеристики, подходы к междисциплинарному познанию// Российская школа связей с общественностью. 2023. № 29. С. 10-26; Гаврилов Л.А., Зарипов Р.И. Язык массовой коммуникации и информационная война// Москва, 2023; Галаганова С.Г. Лингвистическое программирование в информационной войне// Вестник Академии военных наук. 2024. № 1 (86). С. 43-46; Егорова М.Р. Информационная война как угроза национальной безопасности страны в современном мире на примере конфликтов XXI века// Евразийский Союз: вопросы международных отношений. 2023. Т. 12. № 7 (53). С. 991-999; Калинин О.И., Приходько М.В. Информационная война: коммуникативный, дискурсивный, когнитивный и культурно-идеологический аспекты// Военно-филологический журнал. 2023. № 1. С. 23-36; Кургинова Д.Ю. К вопросу о том, что такое русофобия// Каспийский регион: политика, экономика, культура. 2024. № 1 (78). С. 104-110; Лукушин В.А. Внешнее информационное давление на российскую молодежь как инструмент глобального противоборства// Общественные науки и современность. 2023. № 3. С. 68-82; Манойло А.В. "Киев за три дня" и "новая искренность Хёрша" как пример "управления ожиданиями" в операциях информационной войны// Российский социально-гуманитарный журнал. 2023. № 3; Чумаков А.Н. Актуальный инструментарий информационного противоборства в "холодной", "горячей" и "гибридной" войне// Наука. Общество. Оборона. 2023. Т. 11. № 2 (35). С. 19; Ярмак О.В., Бакулин А.В., Бакулин Д.В. Феномен сетецентризма в условиях современного когнитивного противостояния: на примере анализа херсонского кейса// Вестник Института социологии. 2023. Т. 14. № 2. С. 114-135.

информационной войны между Россией (и шире – Глобальным Югом) и коллективным Западом в том числе, в «гибридном» и когнитивном форматах.

Смене доминирующих держав и порядков и понятию баланса сил посвящены многие классические исследования представителей академической науки, таких, как П. Кеннеди, Дж. Арриги, Дж. Моделски и У.Томпсон, И. Валлерстайн, Дж. Мершаймер, С. Хантингтон, Ф. Закария, Д. Мюррей, Д. Браун, Т. Пол, Дж. Вирц, М. Фортманн, Р. Литтл, Д. Нексон, Н. Спайкман, М. Андерсен, У. Вольфорт, Т. Мюллер, М. Альберт[4].

Глобальные трансформации, задающие социально-политический контекст, в котором разворачиваются информационные войны, рассматриваются в работе с позиций мир-системного подхода, развиваемого в трудах таких ученых, как Ф. Бродель, И. Валлерстайн. Э. Геллнер, Дж. Арриги и Б. Силвер, И. Дьяконофф, У.МакНил, А.Г.Франк, Б.Гиллс, Дж. Моделски, У. Томпсон, Т. Девезас, К. Чейз-Данн, Р. Денемарк, П.В. Турчин, Б. Родриг, В.А. Садовничий, А.А. Акаев, И.В. Ильин, Л.Е.Гринин, А.В. Коротаев, А.Д. Урсул, С.Ю. Малков, Ю.В. Зинькина[5].

---

[4] Andersen M.S., Wohlforth W.C. Balance of power: a key concept in historical perspective. In: de Carvalho B., Costa Lopez J., Leira H. (eds). Routledge handbook of historical international relations. London: Routledge, 2021. P. 289-301. Arrighi G. The long twentieth century: money, power, and the origins of our times. London: Verso, 1994. 400 p. Kennedy P. The rise and fall of great powers: economic change and military conflict from 1500 to 2000. New York, NY: Random House, 1987. 677 p. Little R. The balance of power in international relations: metaphors, myths and models. Cambridge: Cambridge university press, 2007. 317 p. Mearsheimer J.J. The tragedy of great power politics. New York: W.W. Norton, 2001. 555 p. Modelski G., Thompson W.R. Leading sectors and world powers: the coevolution of global politics and economics. Columbia, SC: University of South Carolina press, 1996. 263 p. Müller T., Albert M. Whose balance? A constructivist approach to balance of power politics // European journal of international security. 2021. Vol. 6, No 1. P. 109-128. Murray D., Brown D. (eds). Multipolarity in the 21st century: a new world order. New York: Routledge, 2012. 224 p. Nexon D.H. The balance of power in the balance // World Politics. 2009. Vol. 61, No 2. P. 330-359. Paul T.V., Wirtz J.J., Fortmann M. Balance of power: theory and practice in the 21st century. Stanford, CA: Stanford University Press, 2004. 384 p. Spykman N.J. America's strategy in world politics: the United States and the balance of power. London: Routledge, 2017. 525 p. Zhang F. Reconceiving the balance of power: a review essay //Review of international studies. 2011. Vol. 37, No 2. P. 641-651. Валлерстайн И. Анализ мировых систем и ситуация в современном мире. СПб.: Университетская книга, 2001. 416 с. Закария Ф. Постамериканский мир будущего. М.: Европа, 2009. 280 с. Хантингтон С. Столкновение цивилизаций. М.; СПб.: АСТ, 2003. 603 с.

[5] Akaev A. A., Sadovnichiy V. A. A closed dynamic model to describe and calculate the Kondratiev long wave of economic development // Herald of the Russian Academy of Sciences. 2016. Vol. 86, No 5. P. 371–383. Akaev A., Sadovnichy V., Korotayev A. On the dynamics of the world demographic transition and financial-economic crises forecasts // The European Physical Journal Special Topics. 2012. Vol. 205, No 1. P. 355–373. Akaev A., Korotayev A., Issaev L., Zinkina J. Technological development and protest waves: Arab spring as a trigger of the global phase transition? // Technological Forecasting and Social Change. 2017. Vol. 116. P. 316–321. Arrighi G., Silver B. J. Chaos and governance in the modern world system. University of Minnesota Press, 1999. Braudel F. Capitalism and material life, 1400–1800. Harper and Row, 1973. Braudel F. Civilization and capitalism, 15th – 18th century.

Для понимания технологической сути информационных войн с социогуманитарной точки зрения ключевыми являются работы Р.Ф. Абдеева, В.И. Аникина, М.Г. Анохина, В.А. Боришполец, Е.Г. Баранова, А.Г. Караяни, В.Е. Лепского, А.В. Манойло, А.П. Назаретяна, Д.В. Ольшанского, В.С. Степина, Э.Г. Соловьева, И.В. Сурмы, И.Н. Панарина, Г.Г. Почепцова, А.Я.

Harper and Row, 1982. Chase-Dunn C., Anderson E. (Eds.). The historical evolution of world-systems. Cham: Springer, 2005. Chase-Dunn C., Hall T. D. Rise and demise: Comparing world-systems. Westview Press, 1997. Chase-Dunn C., Lerro B. Social change: Globalization from the Stone Age to the present. London: Routledge, 2016. Chase-Dunn C., Niemeyer R., Alvarez A., Inoue H., Love J. Cycles of rise and fall, upsweeps and collapses: Changes in the scale of settlements and polities since the Bronze Age. In L. Grinin, P. Herrmann, A. Korotayev, & A. Tausch (Eds.), History and mathematics: Processes and models of global dynamics. Volgograd: Uchitel, 2010. P. 64–91. Denemark R. A., Friedman J., Gills B. K., Modelski G. World system history: The social science of long-term change. London: Routledge, 2000. Diakonoff I. The paths of history. Cambridge: Cambridge University Press, 1999. Frank A. G., Gills B. K. (Eds.). The world system: Five hundred years, or five thousand. London: Routledge, 1993. Gellner E. Plough, sword and book. The structure of human history. Chicago: University of Chicago Press, 1988. Gills B. K., Thompson W. (Eds.). Globalization and global history. London: Routledge, 2012. Grinin L. Macrohistory and globalization. Volgograd: Uchitel, 2012. Grinin L. On revolutionary waves since the 16th century. In J. A. Goldstone, L. Grinin, & A. Korotayev (Eds.), Handbook of revolutions in the 21st century: The new waves of revolutions, and the causes and effects of disruptive political change. Cham: Springer, 2022. P. 389–411. Гринин Л. Е., Гринин А. Л. От рубил до нанороботов. Мир на пути к эпохе самоуправляемых систем: История технологий и описание их будущего. ООО «Издательство "Учитель"», 2015. Grinin L., Grinin A. The cybernetic revolution and the forthcoming epoch of selfregulating systems. Volgograd: Uchitel, 2016. Grinin L., Grinin A. Historical materialism: Does the concept have a future? // Social Evolution & History. 2023. Vol. 22. No 1. P. 143–178. Grinin L., Korotayev A. Social macroevolution. Genesis and transformations of the world system. Moscow: Librocom/URSS, 2009. Grinin L., Korotayev A. Great divergence and great convergence. A global perspective. Cham: Springer, 2015. Grinin L., Korotayev A. Origins of globalization in the framework of the Afroeurasian world-system history. In T. D. Hall (Ed.) Comparing globalizations. Historical and worldsystems approaches. Cham: Springer, 2018. P. 37–70. Ilyin I., Ursul A. Globalistics: New investigative trends in science // Globalistics and Globalization Studies. 2012. Vol. 1. P. 107–118. McNeill W. H. The pursuit of power: Technology, armed force, and society since AD 1000. Chicago: University of Chicago Press, 2013. Malkov S., Davydova O. Modernization as a global process: The experience of mathematical modeling // Computer Research and Modeling. 2021. Vol. 13, No 4. P. 859–873. Modelski G., Thompson W. R. Leading sectors and world powers: The coevolution of global politics and economics. University of South Carolina Press, 1996. Modelski G., Devezas T., Thompson W. R. (Eds.). Globalization as evolutionary process: Modeling global change. London: Routledge, 2007. Korotayev A. World religions and social evolution of the old world Oikumene civilizations: A cross-cultural perspective. Edwin Mellen Press, 2004. Korotayev A. Compact mathematical models of world system development, and how they can help us to clarify our understanding of globalization processes. In G. Modelski, T. Devezas, & W. R. Thompson (Eds.) Globalization as evolutionary process: Modeling global change. London: Routledge, 2008. P. 133–160. Korotayev A. The 21st century singularity in the big history perspective. A re-analysis. In A. Korotayev & D. LePoire (Eds.) The 21st century singularity and global futures. A big history perspective (pp.). Cham: Springer, 2020. P. 19–75. Korotayev A., Malkov S. Mathematical models of the world-system development. In S. Babones & C. Chase-Dunn (Eds.) Routledge handbook of world-systems analysis. Routledge, 2012. P. 158–161. Korotayev A., Malkov A., Khaltourina D. Introduction to social macrodynamics: Compact macromodels of the World System growth. Moscow: KomKniga/URSS, 2006. Rodrigue B. H. Disaster's offspring: Catastrophe, narrative, and survival in global history // Journal of Globalization Studies. 2021. Vol. 12, No 1. P. 159–171. Turchin P. Historical dynamics: Why states rise and fall (2nd ed.). Princeton, NJ: Princeton University Press, 2018. Wallerstein I. The modern world-system I: Capitalist agriculture and the origins of the European world-economy in the sixteenth century. Vol. 1. University of California Press, 2011. Wallerstein I. World-systems analysis: An introduction. Duke University Press, 2020. Wallerstein, I. 1974. The Modern World-System: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century. NY: Academic. 410 p. Wallerstein I. 1979. The Capitalist World-Economy. Cambridge: Cambridge University Press. 305 p. Wallerstein I. 1980. The Modern World-System II. Mercantilism and the Consolidation of the European World Economy, 1600-1750. NY: Academic. 370 p. Zinkina J., Christian D., Grinin L., Ilyin I., Andreev A., Aleshkovski I., Shulgin S., Korotayev A. A big history of globalization: The emergence of a global world system. Cham: Springer, 2019.

Фариной, Т. Адорно, Д. Белла, Ф. Зимбардо, М. Кастельса, А. Маслоу, К.Р. Санстейна, Э. Тоффлера, Дж. Шарпа и др.[6]

Таким образом, многие аспекты информационных войн к настоящему времени изучены достаточно глубоко. Однако ввиду быстрого развития информационных технологий и изменений политической ситуации в мире, эта проблема продолжает оставаться актуальной и требует дальнейшего изучения и разработки эффективных инструментов противодействия. Решение данного вопроса невозможно без изучения социально-технологических основ влияния на противостоящие и конкурирующие общества, что, в свою очередь, должно рассматриваться в контексте изучения глобальных трансформаций. Данные трансформации, происходящие в обществе (глобальные социальные трансформации) в значительной степени вызваны процессами технологического и цифрового развития последних десятилетий, однако, также происходят в плоскости ценностных, демографических, политических и иных социальных, и даже социо-природных изменений. Тема глобальных социальных трансформаций поднималась и раскрывалась в работах ученых МГУ И.В. Ильина, Ю.Н.

[6] Аникин В.И., Абдеев Р.Ф., Сурма И.В. Философские аспекты информационной цивилизации и современные проблемы управления в ракурсе глобальной безопасности // Вопросы безопасности. 2017. № 2. С. 44-54; Баранов Е.Г. Информационно-психологическое воздействие: сущность и психологическое содержание // Национальный психологический журнал. 2017. № 1 (25). С. 25-31; Баришполец В.А. Информационно-психологическая безопасность: основные положения // Информационные технологии. 2013. №5. С. 62-107; Лепский В.Е. Технологии управления в информационных войнах (часть 1: от классической к постнеклассической рациональности) // Информационные войны. 2016. № 2 (38). С. 57-64; Лепский В.Е. Информационно-психологическая безопасность субъектов дипломатической деятельности. М.: Научная книга, 2003; Манойло А.В. Государственная информационная политика в особых условиях: монография. М.: МИФИ, 2003; Караяни А.Г., Зинченко Ю.П. Информационно-психологическое противоборство в войне: история, методология, практика. М.: МГУ, 2007; Назаретян А.П. Психология стихийного массового поведения. Лекции. М.: ПЕР СЭ, 2001; Ольшанский Д.В. Политическая психология. Екатеринбург: Деловая книга, 2001; Степин В.С. Эпоха цивилизационных перемен и диалог культур. М.: ИНИОН РАН, 2009; Панарин И.Н. СМИ, пропаганда и информационные войны. М.: Поколение, 2012; Почепцов Г.Г. Информационно-психологическая война. М.: СИНТЕГ, 2000; Фарина А.Я. Анализ современных форм, методов и приемов информационного воздействия по каналам СМИ // Вестник МГЛУ. Серия: Исторические науки. 2010. Вып. 2 (581). С. 247-266; Кастельс М. Информационная эпоха: экономика, общество и культура; пер. с англ. под науч. ред. Шкаратана О.И. М.: ГУВШЭ, 2000; Shwab K. The Fourth Industrial Revolution // International Affairs. 2016; Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. Москва: Прогресс, 1986. С. 330-342; Зимбардо Ф., Ляйппе М. Социальное влияние. СПБ: «ПИТЕР», 2001; Maslow A. H. Motivation and Personality. New York: Harpaer & Row, 1954; Хьелл Л., Зиглер Д. Теории личности. Основные положения, исследования и применение. 3-е изд. СПб.: Питер, 2008; Hjelle L., Ziegler D. Personality Theories: Basic Assumptions, Research, and Applications, 1992; Sunstein C. R. The Law of Group Polarization // J. of Political Philosophy. 2002. Vol. 10. № 2. Pp. 175-195; Шарп Дж. От диктатуры к демократии. Концептуальные основы освобождения; пер. Козловской Н.М.: Новое издательство, 2012.

Саямова[7], Н.Л. Смакотиной[8], А.Т. Гаспаришвили[9], В.В. Кочеткова[10], а также представителей других вузов и научных центров – А.М. Старостина[11], Н.Г. Дехановой и Ю.А. Холоденко[12], Т.И. Грабельных[13] и др. ученых.

Таким образом, вопрос об оптимизации системы мер противодействия информационным войнам целесообразно рассматривать прежде всего с учетом передовых воззрений на процессы глобальной трансформации и их национальные и региональные проекции.

В связи с вышеизложенным, **целью исследования** является выявление особенностей ведения информационных войн в условиях глобальных социальных трансформаций, а также наиболее перспективных форм и методов противодействия связанным с ними угрозам национальной безопасности.

Задачи:

1) разработать авторскую классификацию информационных войн современности на основе анализа теоретических подходов к их изучению;
2) выявить общие особенности информационных войн современности, возникшие в ходе реализации ключевых глобальных социальных трансформаций;

---

[7] Саямов Ю.Н. Глобальные социальные трансформации и современный мир// Alma Mater (Вестник высшей школы). 2021. № 2. С. 66-71.

[8] Смакотина Н.Л. Глобальные социальные трансформации в контексте демографических изменений и урбанизации. Acta Biomedica Scientifica. 2022;7(3):47-56. https://doi.org/10.29413/ABS.2022-7.3.6

[9] Смакотина Н.Л., Саямов Ю.Н., Гаспаришвили А.Т., Егоренкова М.А. Управление социальными трансформациями в контексте глобальных процессов и проблем: предварительные результаты исследования// В книге: I Российско-Иранский социологический форум. Сборник тезисов докладов участников форума. Москва, 2020. С. 489-499.

[10] Кочетков В. В. Глобализация в образовании: информационная война и "промывание мозгов" или доступ к мировым знаниям и благам цивилизации? // Вестник Московского университета. Серия 18: Социология и политология. — М.: Издательство Московского государственного университета, 2005. — № 1. — С. 144—159.

[11] Старостин А.М. Глобальные социальные трансформации в координатах концепции социальных инноваций// В сборнике: Глобалистика-2020: Глобальные проблемы и будущее человечества. Сборник статей Международного научного конгресса. Москва, 2020. С. 215-219.

[12] Деханова Н.Г., Холоденко Ю.А. Приоритеты социальной политики России в условиях глобальных социальных изменений// Социодинамика. 2024. № 3. С. 76-87.

[13] Грабельных Т.И. Историческое самосознание, интеллектуальный капитал и глобальные социальные трансформации как макросистемные показатели изменения социального мира// В сборнике: Интеллектуальный капитал в XXI веке. Сборник научных трудов. Иркутск, 2019. С. 15-18.

3) определить современные особенности ведения информационных войн и противостояния им у США, России и КНР как ведущих в военно-политическом отношении мировых держав;
4) выявить основные перспективы развития информационных войн с точки зрения их интенсивности и характера;
5) разработать рекомендации по повышению эффективности ведения информационных войн, а также укреплению информационной безопасности и эффективному противодействию дезинформации и манипуляциям общественным сознанием в контексте современных глобальных социальных трансформаций.

Объект исследования – современные информационные войны между государствами, их блоками, с участием негосударственных структур, в том числе, террористических группировок.

Предмет – особенности информационных войн, возникшие и проявившиеся в результате глобальных социальных трансформаций современности.

Хронологические рамки охватывают временной отрезок с конца двадцатого столетия по настоящее время. На это время приходится период развития интернета и, как следствие, расширение возможности распространения дезинформации в онлайн-среде, а также активное использование социальных сетей и мессенджеров для распространения дезинформации и манипуляции общественным мнением.

Нормативно-эмпирическая база исследования включает в себя следующие источники:

– международные правовые нормы, регулирующие информационные войны, такие как Женевская конвенция, Конвенция ООН по борьбе с киберпреступностью и другие;

– стратегические документы изучаемых стран в области национальной безопасности, информационной и кибер-безопасности;

– теоретические концепции, описывающие природу и механизмы информационных войн, такие как концепция информационной безопасности, теория информационной войны и другие.

Научная новизна исследования заключается в выявлении основных характеристик информационных войн в условиях глобальных социальных трансформаций и состоит в следующем:

1) разработана авторская классификация информационных войн, учитывающая как психологические, так и технологические аспекты их направленности в современном мире;

2) выявлены ключевые общие особенности информационных войн в условиях реализации основных направлений глобальных социальных трансформаций;

3) определены особенности стратегий ведущих в военно-политическом отношении стран мира в современном информационном противоборстве;

4) выявлены основные перспективы развития информационных войн в ближайшие десятилетия;

5) разработаны рекомендации по повышению эффективности ведения информационных войн, включая вопросы информационной безопасности и эффективного противодействия дезинформации и манипуляциям общественным сознанием.

Теоретико-методологическая основа исследования представляют теория глобального эволюционизма, развитая в работах А.Д. Урсула и И.В. Ильина, концепция мягкой силы, получившая отечественное осмысление и развитие в трудах О.Г. Леоновой, система взглядов на социальные трансформации современности, сформированная в работах Г.В. Осипова, И.В. Ильина, Н.Л. Смакотиной, Ю.Н. Саямова и других авторов.

Для изучения комплексного влияния процессов цифровизации на сферу внешней политики ведущих в геополитическом отношении стран мира и международной политики в области глобального и регионального развития применялись, во-первых, общенаучные методы анализа и синтеза и

политико-описательный метод для систематизации фактов; во-вторых, элементы системного анализа и институционального подхода; в-третьих, сравнительный анализ, в-четвертых, метод классификации, в-пятых, методы контент-анализа и библиометрии.

Автор исходит из рассмотрения глобального управления как «комплекса формальных и неформальных институтов, механизмов, отношений и процессов» – в соответствии с теорией, изложенной в начале нынешнего века Т. Вайссом и Р. Такуром. При этом наиболее справедливым подходом к глобальному управлению, соответствующему целям устойчивого развития, будет максимальный учет национальных интересов всех стран мира, без однополярной гегемонии и избыточности национальных барьеров. Процессы и явления, связанные с развитием информационных войн рассматриваются автором на основе мир-системного подхода, развиваемого в трудах таких ученых, как Ф. Бродель, И. Валлерстайн. Э. Геллнер, Дж. Арриги и Б. Силвер, И. Дьяконофф, У.МакНил, А.Г.Франк, Б.Гиллс, Дж. Моделски, У. Томпсон, Т. Девезас, К. Чейз-Данн, Р. Денемарк, П.В. Турчин, Б. Родриг, В.А. Садовничий, А.А. Акаев, И.В. Ильин, Л.Е. Гринин, А.В. Коротаев и др.

Теоретическая и практическая значимость. Изучение социо-гуманитарных технологий в контексте информационной войны имеет как теоретическую, так и практическую значимость.

Теоретическая значимость данного исследования заключается в формировании новой классификации информационных войн, структурирующей многообразие их определений и учитывающей современные теоретические концепции их изучения, кроме того, рассмотрение информационных войн в контексте глобальных социальных трансформаций формирует концептуально новых подход к ним как к естественному глобальному явлению, соответствующему всем основным движениям социальных процессов.

Практическая значимость этого исследования проявляется в возможности разработки и применения более эффективных стратегий по противодействию дезинформации, манипуляциям и фейковым новостям. Более того, понимание социо-гуманитарных технологий позволяет эффективно мобилизовать информационные ресурсы для распространения достоверной информации среди населения.

Положения, выносимые на защиту:

1. Многообразие современной терминологии информационных войн, а также их частая «мимикрия» под социо-культурный обмен стран и цивилизаций и иные проявления позитивной мягкой силы заставляют предложить уточняющую их классификацию. Информационные войны целесообразно разделять по направленности на информационно-психологические, то есть направленные на сознание человека и информационно-технологические, направленные на информационную инфраструктуру. Первые включают: 1) военную пропаганду, 2) информационно-экстремистские или террористические действия, 3) информационно-мировоззренческие войны (включающие, в свою очередь: а) социо-культурные войны, б) «войны памяти» или войны исторических нарративов, в) информационно-политические войны); 4) информационно-экономические войны, ведущиеся против хозяйствующих субъектов или экономического потенциала в целом стран-конкурентов; 5) информационно-экологические войны, направленные на дискредитацию природного потенциала. Круг ключевых технологий, используемых для подготовки и ведения информационных войн, определяется прежде всего глобальным технологическим прогрессом в цифровизации и расширяющимся доступом широких слоев населения разных стран к информационной среде.

2. Становление во второй половине XX века информационного, а в XXI веке – цифрового общества, что является ключевой глобальной трансформацией современности, цифровизация промышленности и управления, а также научные достижения в области психологии и

социологии создали условия для появления как новых объектов для информационных атак (цифровая инфраструктура экономики и, особенно, промышленности, финансов, госуправления, социальные сети, базы личных данных и т.д.), так и для технологизации информационно-психологического воздействия вплоть для использования технологий искусственного интеллекта для пропаганды или создания ложных нарративов. При этом круг объектов направленности информационно-психологических войн практически не изменился со времен Второй мировой войны и даже с более раннего периода активизации противостояния России с европейскими странами в XIX веке. В то же время с усилением значимости экологической составляющей жизни человечества, новыми трендами декарбонизации и экологизации появилась новая сфера информационного воздействия – осознание природно-экологической защищенности и комфорта населения противоборствующих и конкурирующих стран.

3. К концу 2024 года США и их союзники достигли пика интенсивности информационных войн с Россией, Китаем и другими государствами, которые идеологически противостоят западным странам. США, Россия и Китай, будучи крупнейшими военно-политическими акторами, следуют различным стратегиям в ведении информационных войн, основывающимся на их идеолого-мировоззренческой базе и технологических возможностях. Данные стратегии можно определить следующим образом: 1) Наступательно-гегемонистская стратегия США, исходящая из стремления к глобальному доминированию; 2) Оборонительно-технологическая стратегия Китая, исходящая из принципа не навязывания другим странам своих нарративов, наличия возможностей для защиты внутреннего киберпространства и концентрации на информационно-технологических аспектах военного противостояния; 3) Оборонительно-наступательная стратегия современной России, связанная, прежде всего, со стремлением защитить внутреннее информационное пространство, а также продвигать нарративы и контр-нарративы во всем мире, используя прежде всего

цифровые площадки. Начавшийся в 2025 году позитивный диалог российского руководства с администрацией США пока не имеет стабильности, необходимой для стратегической смены ситуации. Руководство Китая строго контролирует информационное пространство в стране с помощью цензуры, блокировки новостных сайтов и социальных сетей. Эти меры ограничивают доступ к нежелательной информации, что делает Китай более защищенным от информационных атак со стороны Запада. В то же время, и России, и Китаю, в условиях консолидации Глобального Большинства, не хватает наступательных информационно-психологических действий для повышения успешности своего лидерства в борьбе за новый, более справедливый миропорядок. Вместе с тем, США и коллективный Запад также подвержены информационно-психологическим и информационно-технологическим атакам ввиду как развитости и открытости своего киберпространства, так и его идеолого-мировоззренческого кризиса. Ввиду этого, секьюритизация и суверенизация киберпространства, повышение уровня цензуры и контроля охватывает как Россию, Китай и ряд других стран Глобального Большинства, так и страны коллективного Запада, особенно Европейского Союза.

4. В контексте глобальных социальных трансформаций, связанных в том числе с естественным социально-политическим процессом реконфигурации Мир-Системы и сопровождающимся в его ходе глобальным геополитическим обострением и усилением значимости идеолого-мировоззренческой составляющей информационного противоборства, не приходится ожидать ослабевания интенсивности развязываемых Западом информационных войн в ближайшие 10-20 лет. Усиление идеолого-мировоззренческого аспекта информационных войн находит отражение в интенсивности соответствующих научных публикаций. В целом потенциальные угрозы национальной безопасности, связанные с внешним информационно-психологическим воздействием, могут стать критическими только в случае наличия серьезных факторов, способствующих социально-

экономической и/или социально-политической нестабильности в целевых странах, подвергшихся таким атакам. Важно отметить, что ни Россия, ни Китай не имеют фундаментальных оснований для такой внутренней дестабилизации. Однако следует учитывать, что угрозы, связанные с разрушительными атаками в цифровой и технологической сфере, создают для России все больше рисков в области обеспечения безопасности критической инфраструктуры.

5. Перспективным для России и Китая направлением информационных войн является наступательный вектор идеолого-мировоззренческой войны, реализуемой путем формирования и продвижения нарративов справедливого мироустройства и партнерства цивилизаций как для интеллектуально-элитной, так и массовой аудитории коллективного Запада. Вместе с тем, данное направление представляется наиболее наукоемким в информационно-психологической сфере, поскольку связано не столько с социо-техническими вопросами формирования самих нарративов, сколько с научным обеспечением их идеологической основы.

Наиболее перспективными и эффективными способами борьбы с угрозами, связанными с информационными войнами, и обеспечения национальной безопасности, являются:

– повышение критического мышления и медиа-грамотности среди населения, чтобы люди могли легче выявлять фейки, дезинформацию и пропаганду;

– регулирование использования информационных технологий и социальных медиа с целью предотвращения распространения ложной информации и негативного воздействия на общественное мнение;

– разработка и применение систем фильтрации контента, анализа данных и алгоритмов искусственного интеллекта;

– сотрудничество между правительством, научным сообществом и предприятиями для разработки и внедрения комплексных стратегий по защите от информационных войн;

– обучение и подготовка специалистов в области информационной безопасности и киберзащиты;

– ключевым элементом противодействия информационным войнам будет разработка и принятие международных норм регулирования конкуренции между странами в информационном пространстве.

Апробация результатов работы. По теме диссертационного исследования опубликовано 5 статей в журналах, входящих в перечень ВАК, в том числе 4 статьи – в рецензируемых научных изданиях, рекомендованных для защиты в диссертационном совете МГУ имени М.В.Ломоносова по специальности и отрасли наук.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ИНФОРМАЦИОННЫХ ВОЙН

1.1. Сущность и специфика информационных войн

Становление информационного общества усложнило понятие «информационная война» отражающего явление, известное с глубокой древности. Информация стала играть роль движителя экономики, а не просто набором сведений для управления. В этой связи требуется очертить понятие информационной войны, как и ряд других, связанных с ней понятий.

Информационная война — «противоборство сторон посредством распространения специально подготовленной информации и противодействия аналогичному внешнему воздействию на себя, она направлена на достижение политических, экономических, военных или иных целей стратегического уровня» [14] . В информационной войне могут участвовать как созданные властями структуры, так и отдельные сообщества, группы и лица. Как правило, методами информационной войны являются вброс дезинформации или представление информации в выгодном для себя ключе[15].

Кибервойна — новое понятие, возникшее в конце прошлого столетия в связи с активным развитием интернета и цифровых технологий. Это - противоборство и противостояние в кибернетическом пространстве (киберпространстве), в том числе компьютерное противостояние в интернете, одна из разновидностей информационной войны. Кибервойна направлена на дестабилизацию компьютерных систем и доступа к интернету государственных учреждений, финансовых и деловых центров, а также на создание беспорядка и хаоса в жизни стран и государств, которые

[14] Информационная война// Большая российская энциклопедия https://bigenc.ru/c/informatsionnaia-voina-2b7815 (дата обращения: 1.09.2025).
[15] Информационная война// Социология: Энциклопедия / Сост. А.А. Грицанов, В.Л. Абушенко, Г.М. Евелькин, Г.Н. Соколова, О.В. Терещенко., 2003 г. URL: https://web.archive.org/web/20140326164153/http://voluntary.ru/dictionary/568/word/informacionaja-voina (дата обращения: 1.09.2025).

полагаются на интернет в повседневной жизни.

Таким образом, информационная война более широкое понятие, а кибервойна — один из видов информационной войны, связанный с использованием информационных технологий.

«Гуманитарной» составляющей информационной войны является воздействие на психологию противника. Психологическая война — «это деятельность (как правило) специальных органов одного государства или связанных с ним организаций, оказывающих психологическое воздействие на гражданское население и (или) на военнослужащих другого государства ради достижения своих политических и военных целей»[16]. Психологическая война направлена зачастую не только на противника, но и на мобилизацию и оптимизацию моральных и психологических сил нации и вооружённых сил в интересах решения военных задач. В ее рамках также решаются задачи защиты населения своей страны и её вооружённых сил от разлагающего информационно-психологического влияния противника. Но основной целью является психологическое воздействие на войска и население противника в целях их дезориентации, деморализации и дезорганизации, влияние на взгляды, настроения, поведение дружественных и нейтральных аудиторий (стран, социальных групп, вооружённых формирований) в направлении, благоприятном для достижения победы над противником.

Таким образом, информационная война охватывает средства воздействия (механизмы передачи, способы доставки, формы обработки и сохранения), а психологическая война — содержание, цели и задачи воздействия на массовое сознание. Вместе с тем, информационная война – как правило общее, единое понятие, объединяющее все виды противоборства с использованием информации или направленной на информационное обеспечение противника, кибервойна – война в киберпространстве, в основном ведущаяся технологическими методами, а война психологическая –

[16] Лукин Е.В. Психологические основы информационной войны// Центр стратегических оценок и прогнозов. URL:https://csef.ru/ru/oborona-i-bezopasnost/265/psihologicheskie-osnovy-informacczionnoj-vojny-3725 (дата обращения: 1.09.2025).

социогуманитарная составляющая информационной войны, ее содержание (гуманитарную составляющую информационной войны часто называют также «информационно-психологической войной»).

В условиях расширения возможностей и технологического развития, а также достижений социогуманитарной науки, воздействие на психику приобретает масштабное влияние на мировоззрение и на поведение войск и населения стран противника. С конца XX века на Западе (в США, у военных) возник термин «когнитивная война», который пока не прижился в академическом сообществе, но активно используется в политических документах. Когнитивная война может охватывать множество областей, включая традиционную пропагандистскую войну, психологическую войну, идеологическую войну (войну исторических нарративов) и правовую войну (войну правовых определений и оценок). То есть понятие когнитивной войны может быть включено непосредственно как более общее по отношению к понятию «психологическая война», но входящую в понятие «информационная война».

Наконец, в последние годы информационная война включается в качестве направления в понятие «гибридной войны» - термин появился в начале XXI века и используется как ведение противоборства комплексными, всеми известными способами, часто без непосредственных боевых действий между противниками, но посредством использования вооруженных прокси-сил, социально-политической дестабилизации внутри страны противника, финансово-экономических санкций, диверсий и собственно информационного воздействия.

Явление информационной войны в истории человечества не ново; российские исследователи А. Д. Васильев и Ф. Е. Подсохин пишут в этой связи: «античные авторы во всех красках описывали агитационные кампании, деморализующие и таким образом ослабляющие противника, либо наоборот — поднимающие боевой дух соотечественников»[17].

[17] Васильев А. Д. Информационная война: лингвистический аспект / А. Д. Васильев, Ф. Е. Подсохин //

Первое наиболее яркое проявления информационной войны было отмечено в ходе Ливонской войны и несколько ранее, когда молодое Российское царство отказалось следовать в фарватере западной цивилизации в качестве ее «окраинного вассала». Наступившая эпоха книгопечатания породила процесс создания мифов о России для мобилизации европейского сообщества на борьбу с ней. Формы и методы тогдашней войны полностью воспроизводятся в настоящее время. Ярким этапом развития информационной войны стали ее проявления в преддверии и в ходе Крымской войны (1853-1856), когда в отношении действий российских войск западными СМИ распространялись слухи о якобы жестоком обращении со сдающимися в плен, пленными, убийствах парламентеров и т.д. Германией и союзниками велась информационная война против России в годы Первой мировой войны[18], и, конечно же, Второй мировой (Великой Отечественной) войны.

Однако, сам термин возник относительно недавно, в эпоху «информационного взрыва», совпавшую с разгаром Холодной войны. В 1968 году М. Маклюэн (исследователь СМИ из Канады) отметил, что «Третья мировая война — это партизанская информационная война, где нет различия между военными и гражданскими»[19].

Полномасштабно информационная война Запада против Китая разворачивается активно лишь в последние десятилетия.

Существует несколько версий того, где и когда впервые был употреблен термин «информационная война». Часто его авторство приписывается американскому ученому Томасу Роне, употребившему этот термин в 1976 году в своем отчете для компании «Boeing» по заказу Министерства обороны США. Однако есть мнение, что этот термин стал употребляться намного раньше, в именно в 1951 году, и был изначально

Политическая лингвистика. — 2016. — № 2 (56). — С. 10-16.

[18] Качмазова З.Н. Информационно-психологические войны: из истории возникновения и развития методов их ведения// Научная мысль Кавказа. 2012. № 3 (71). С. 140-142.

[19] McLuhan M. War and Peace in the Global Village 1968 https://www.amazon.com/exec/obidos/ASIN/B000NPDT7S/ref=nosim/globalguerril-20 (Дата обращения 1.09.2025)

предложен политиком Джорджем Кеннаном и Джоном фон Нейманом для обозначения одного из видов пропагандистской деятельности[20].

На момент, когда Рона писал свой доклад, сети Интернет еще не существовало, и даже ее предшественница ARPANET находилась еще в начале своего развития, однако Рона предвидел ключевую роль информационной инфраструктуры стран в военных кампаниях будущего – ее стремительно возраставшая роль в экономике стран делала ее привлекательным объектом для совершения атак противниками той или иной страны (в первую очередь, он вел речь о возможных атаках на таковую инфраструктуру в США со стороны СССР – напомним, это происходило в период существования биполярной системы).

И, хотя Рона вел речь только об одном направлении информационных войн, связанном именно с разрушением такой инфраструктуры, он смог предусмотреть фундаментальное отличие информационных войн будущего от войн «традиционных» – это своего рода «необъявленные» войны, которые могут иметь место как в военное, так и в «формально мирное» время. В отличие от «традиционных» военных кампаний, информационные войны в своем начале не сопровождаются объявлением военных действий, и могут не иметь ни четко выраженного начала, ни завершения.

В целом можно считать правильными обе эти версии, с тем лишь различием, что информационные войны, о которых вели речь Кеннан и фон Нейман, велись в пространстве масс-медиа, Рона же подразумевал ведение таких кампаний в киберпространстве.

В мировой науке еще не выработано общепринятого определения информационных войн. Прежде всего, отметим, что мы следуем за А.В. Манойло, убедительно показавшим, что термины «информационное противоборство» и «информационная война» являются полными синонимами, возникшими в научном обороте из-за многозначности перевода

[20] Fredericks Brian E. Information Warfare at the Crossroads. Joint Force Quarterly, 1997. Pp. 97-103.

американского термина «information warfare»[21]. Соответственно, в настоящей работе мы употребляем эти термины как взаимозаменяемые.

Как отмечает М.Ю. Лаврентьева: «Понятие «информационная война» сконцентрировало в себе целый ряд явлений из сферы массовых коммуникаций и в течение XX века называлось различными терминами, такими как дезинформация, пропаганда, контрпропаганда, спецпропаганда, психологическая война, психологические операции» [22] . О.Г. Леонова рассматривает информационное противоборство как часть кибервойн[23].

Эксперты американского аналитического центра RAND Corporation (объявлен нежелательным на территории России), тесно связанного с военной отраслью США, определяли информационную войну как «процесс защиты собственных источников информации о поле боя и, в то же время, стремление отвергать, ухудшать, искажать или уничтожать источники информации противника о поле боя»; в этом определении информационная война включала шесть сфер, таких, как «оперативная безопасность, электронная война (EW), психологические операции (PSYOP), введение в заблуждение, физические атаки на информационные процессы и информационные атаки на информационные процессы»[24].

Отдельные элементы этих сфер применялись на поле боя задолго до того, как термин «информационные войны» стал активно употребляться. В.М. Грызлов и А.Б. Перцев выделяют четыре этапа развития информационного противоборства; их последовательная смена была обусловлена появлением новых коммуникационных технологий и/или связанных с ними изобретений. Так, первый этап, вербальный или «устный»,

---

[21] Манойло А.В. К вопросу о содержании понятия «информационная война». В: Современная Россия и мир: альтернативы развития (Информационные войны в международных отношениях): сборник научных статей/под ред. Ю.Г. Чернышова. — Барнаул : Изд-во Алт. ун-та, 2012. 244 с. С. 18-19.

[22] Лаврентьева М. Ю. Особенности технологий и методов информационно-психологических войн СССР с Великобританией и США в период 1939–1953 гг. Автореф. … кандидата филологических наук. М., 2020. – 26 с. С. 3

[23] Леонова О.Г. Кибервойна и противоборство в цифровом информационном пространстве. Информационное общество. 2018;(2):43–46.

[24] Nichiporuk, B. (2002). US Military opportunities: Information-warfare concepts of operation. In: Z. Khalilzad & J. Shapiro (eds). *Strategic appraisal: United States air and space power in the 21st century*. Rand Corporation, 2002. Pp. 187-219. P. 188.

уступил второму, связанному с появлением бумаги. Третий этап постепенно развертывался с появлением технических новшеств (таких, как печать, а затем массовая печать, появление печатных СМИ) и уже в XX столетии уступил место четвертому, связанному с появлением телекоммуникационных технологий[25].

К примеру, исследователи Я.С. Шатило и В.Н. Черкасов первыми информационными войнами считают мифы, так как войска каждого завоевателя следовали за рассказами об их жесткости, это достаточно сильно подрывало моральных дух противника[26].

В.В. Орехов показывает, как недоучет влияния СМИ на информационное поле стал причиной важных просчетов в политике Николая I по противостоянию европейским политическим идеям и антироссийской информации из западных стран [27] (то есть, по сути, информационной кампании стран Запада против России).

Первые психологические операции включали в себя разбрасывание с самолетов пропагандистских листовок, направленных на подрыв морального духа вражеских сил. Первыми современными примерами введения в заблуждение можно считать, к примеру, имитацию радиопереговоров между несуществующими подразделениями. М.В. Лаврентьева пишет об использовании методов и инструментария информационно-психологических войн в противостоянии СССР и США в период Холодной войны с самого ее начала [28] . Этот пример можно рассматривать как первую масштабную информационную войну, которая велась без объявления «традиционной» войны и не сопровождалась боевыми действиями как таковыми.

Ранние информационные атаки на информационные процессы

---

[25] Грызлов В.М., Перцев А.Б. Информационное противоборство. История и современность. Вестник Академии военных наук. 2015;(2):124–128.

[26] Шатило, Я.С., Черкасов, В.Н. Информационные войны // Информационная безопасность регионов. - 2009. - №2 (5).

[27] Орехов, В. В. (2021). " Партизанская тактика" информационной войны. Часть II: Информационная безопасность в эпоху Николая I. *Ученые записки Крымского федерального университета имени ВИ Вернадского. Филологические науки*, *7*(3), 131-167.

[28] Лаврентьева М. Ю. Особенности технологий и методов информационно-психологических войн СССР с Великобританией и США в период 1939–1953 гг. Автореф. … кандидата филологических наук. М., 2020. – 26 с.

зачастую имели форму компьютерных вирусов. Однако по мере распространения «кибернетической революции» и цифровизации всех сфер жизни общества информационные атаки приобретают все более угрожающий масштаб, поскольку способны привести к коллапсу не только военных систем противника, но и широкого спектра технологий гражданского применения и жизнедеятельности населения страны-противника в целом[29].

Коллектив авторов из РУДН полагает, что термин «информационная война» пришел на смену термину «пропаганда» в последней четверти XX века с появлением новых инструментов информационного противостояния и стремительным развитием глобального информационного пространства в целом. По их мнению, инструментарий пропаганды начал применяться в невиданном до того масштабе в ходе Первой мировой войны, что дает основания полагать, что это была первая «традиционная» война, сопровождавшаяся массированной информационной кампанией[30].

Это ставит вопрос о соотношении терминов «пропаганда» и «информационная война», различие между которыми отмечают В.В. Барабаш и Е.А. Котеленец: «пропаганда ведется всегда, а информационная война – только в определенные периоды, как правило, либо предшествующие, либо совпадающие с обычной, гибридной или «холодной» войной. В пропаганде упор делается на позитивные образы Своего, а в информационной войне – на негативные образы Чужого. Таким образом, информационная война – это наиболее концентрированные пропагандистские кампании, направленные на создание образа врага и на то, чтобы убедить собственное население в справедливости того дела, за которое борется правительство, в необходимости отстаивать определенные ценности и стремиться к достижению определенных целей. В этих кампаниях некоторая часть информации фальсифицируется, а та информация, которая соответствует истине, подвергается препарированию и манипуляциям, чтобы подчинить ее

[29] Кафтан, В. В., & Погорелый, А. П. (2023). Роль идеологии в современной информационной войне. *Гуманитарные науки. Вестник Финансового университета*, *13*(6), 46-53.
[30] Барабаш, В. В., Котеленец, Е. А., & Лаврентьева, М. Ю. (2019). Информационная война: к генезису термина. *Знак: проблемное поле медиаобразования*, (3 (33)), 76-89.

целям информационной войны»[31].

Можно сказать, что информационные войны в их современном понимании появились одновременно с формированием глобального информационного поля, появление и расширение которого было напрямую связано с развитием коммуникационных технологий различных поколений и появлением масс-медиа.

Первой такой технологией стало появление радио; после завершения Второй мировой войны и активизации противостояния СССР и США последние учредили особый орган внешнеполитической пропаганды – Информационное Агентство Соединенных Штатов Америки (*United States Information Agency*). Оно просуществовало с 1953 по 1999 годы. В его структуру входили радиостанции «Голос Америки», «Свобода» и «Свободная Европа», являвшиеся на то время одними из главных инструментов ведения информационной войны[32]. Они вещали на русском (и других языках), имея своей целью, в частности, создание положительного образа США у советской аудитории (и аудитории других стран социалистического блока).

Однако подлинный «расцвет» методов ведения информационных войн приходится на современную эпоху развития информационного общества и непосредственно связан с бурным развитием информационных технологий и цифровизацией всех сфер общественной жизни населения стран мира. Информационные технологии, пронизывающие все сферы развития человечества, изменили и методы создания боевой мощи. Это предоставило, с одной стороны, несравненные возможности для развития вооруженных сил, с другой – серьезные вызовы для их эффективности.

В современном научном пространстве – как российском, так и мировом – существуют различные определения информационных войн. Так, В.И. Добреньков определяет информационные войны через их цель,

[31] Барабаш, В. В., & Котеленец, Е. А. (2016). Информационные войны и медийное пространство: теоретические аспекты новейших изменений. *Известия высших учебных заведений. Поволжский регион. Гуманитарные науки*, (3 (39)), 150-158. С. 152.
[32] Кугушева, А. (2016). От информационных войн к поведенческим. *Информационные войны*, (1), 11-22.

состоящую «не в физическом уничтожении живой силы противника, а в подрыве целей, взглядов и мировоззрения населения, в разрушении социума»[33].

К этому определению близки И.В. Гончарова с коллегами – они отмечают, что информационные войны ведутся в культурном поле, их целью является трансформация сознания политического оппонента. Эти войны направлены на ценностные ориентиры, традиции, историческую и культурную идентичность И.В. Гончарова с коллегами также определяют информационные войны через их принципиальное отличие от «традиционных» войн – оно состоит в том, что информационные войны «ведутся в культурном поле, а их целью является трансформация сознания политического оппонента, который может не подозревать, что находится в эпицентре «ведения боевых действий». Объектами подобных войн являются ценностные ориентиры, традиции, историческая и культурная идентичность той или иной страны»[34].

С.Н. Бухарин, А.Г. Глушков, И.Д. Ермолаев определяют информационную войну следующим образом: «Специальная форма ведения боевых действий, характеризующаяся применением средств информационного воздействия для дезорганизации систем управления, воздействия на элементы вооружения, включая информационные технологии и информационные ресурсы враждебных государств и защиты от аналогичных воздействий соответствующих элементов собственной информационной структуры»[35].

Согласно А.В. Соловьеву, информационная война «всегда подразумевает владение ключевой информацией, способной изменить статус-кво в свою пользу, что, безусловно, требует от субъектов

---

[33] Добреньков, В. И. (2013). Система и стратегии национальной безопасности России в XXI в. *Вестник Московского университета. Серия 18. Социология и политология*, (4), 5-36.

[34] Гончарова, И. В., Ницевич, В. Ф., & Судоргин, О. А. (2024). Информационная война как инструмент политического противостояния в современном многополярном мире. *Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление*, *11*(1), 19-31. С. 21.

[35] Бухарин С.Н., Глушков А.Г., Ермолаев И.Д. Информационное противоборство. Кн. 2. М.: Полиори, 2004. С. 471.

информационного противоборства наличия адекватной соответствующей доктрины, постоянного совершенствования материально-технической базы, наличия высококвалифицированных специалистов, а также высокого уровня мобилизации всего общества»[36].

Современная информационная война тесно связана с войной технологической. Понятия и явления информационной и технологической войн в сфере ИКТ соединяются в термина «кибервойна» или «война в киберпространстве».

Вместе с тем, в российской практике их принято разделять: информационная война – это дезинформация в любом виде и форме, технологическая война в сфере ИКТ (кибератаки, атаки на критическую информационную инфраструктуру и тд)

Имеется необходимость понятийного уточнения в связи с усилением технологической составляющей.

Своего рода «интегральным» определением, затрагивающим и информационно-технологические аспекты информационных войн, и их ценностно-мировоззренческие аспекты, можно считать определение, данное Российской Федерацией в предложениях по разработке международных принципов предотвращения информационных войн, внесенных в Организацию Объединенных Наций в начале XXI века. Это определение информационной войны как «противоборства между государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным структурам, подрыва политической и социальной систем другого государства, а также массированной обработки населения и дестабилизации общества»[37].

Сходное определение выработано странами ШОС и закреплено в соответствующей документации еще в 2009 году: «Информационная война – противоборство между двумя или более государствами в информационном

[36] Соловьёв, А. В. (2010). Информационная война: понятие, содержание, проспектива. *Пространство и время*, (2), 75-81. С. 81.
[37] Цит. По: Алексеев, А. П. (2017). Общество в условиях информационной войны: вопрос интеллектуального суверенитета. *Философия и общество*, (2 (83)), 18-27. С. 21.

пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны»[38].

Выработка единого определения информационных войн осложняется высоким уровнем политизированности данного термина и тем, что контекст его использования или отказа от его использования определяется не столько спецификой характеризуемого им явления, но и политическими соображениями. Так, США в своих официальных документах, относящихся к военной сфере, вовсе отказались от употребления термина «информационная война», заменив его более «нейтральным» понятием «информационные операции», скрадывающим масштаб разрушений, которые могут нанести такие войны[39].

Такие операции бывший командующий ВМС США Стюарт Грин подразделил на пять категорий: 1) радиоэлектронная борьба (Electronic Warfare, EW); 2) психологические операции (Psychological Operations, PSYOP); 3) операции в компьютерных сетях (Computer Network Operations, CNO); 4) мероприятия по оперативной маскировке и введению противника в заблуждение (Military Deceptions, MILDEC); 5) мероприятия по обеспечению оперативной безопасности (Operations Security, OPSEC) [40] . Как верно подмечает А. Смирнов, эта категоризация в явном виде демонстрирует сочетание психологических и технических направлений, которое присуще информационным войнам[41].

Эту категоризацию целесообразно сопоставить с категоризацией,

---

[38] «Соглашение между правительствами государств—членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года». — «Бюллетень международных договоров». 2012. № 1. С. 13—21.

[39] Смирнов А. Информационно-психологическая война //Свободная мысль. – 2013. – №. 6. – С. 81-96.

[40] Green S. Cognitive Warfare. The Augean Stables. Joint Military Intelligence College. July 2008 [Электронный ресурс]. URL: www.theaugeanstables.com/wp-content/uploads/2014/04/Green-Cognitive-Warfare. pdf (дата обращения: 29.10.2022).

[41] Смирнов А. Информационно-психологическая война //Свободная мысль. – 2013. – №. 6. – С. 81-96. С. 83.

предложенной западным исследователем информационных войн М. Либики[42].

Первая категория – радиоэлектронная борьба – присутствует в классификации Либики; хотя он называет ее «электронной», суть данного направления остается неизменной – выведение из строя соответствующей техники противника (в особенности техники, обеспечивающей связь). Н.Р. Красовская и А.А. Гуляев отмечают, что с этим направлением можно объединить такое направление, как кибервойна, поскольку в определении Либики оно практически синонимично электронной борьбе[43]. На наш взгляд, сюда целесообразно также отнести хакерское воздействие, выделенное Либики в отдельный пункт – оно является скорее одним из инструментов электронной борьбы, чем отдельным направлением.

Второе направление – психологические операции – также присутствует в классификации Либики, его главной особенностью является воздействие на массовое мирное население, а не только (и не столько) на комбатантов. На наш взгляд, с этим направлением можно объединить экономико-информационное направление в классификации Либики, которое Либики трактует как информационную блокаду. Действительно, для эффективного осуществления информационного воздействия на массы населения необходимо сделать источник такого воздействия безальтернативным, т.е. уничтожить плюрализм мнений в информационной среде и отрезать населению доступ к источникам информации, предлагающим альтернативные точки зрения.

Наконец, сетевые операции могут быть сопоставлены с командно-управленческим и разведывательным направлениями в классификации Либики, поскольку они направлены на выявление уязвимых мест в информационных сетях противника и подавление или искажение потоков информации, проходящей по этим сетям.

---

[42] Libicki, M. (1995), What is information warfare? Washington: GPG, 280 p.

[43] Красовская Н. Р., Гуляев А. А. К вопросу классификации информационных войн //Социология науки и технологий. – 2019. – Т. 10. – №. 2. – С. 44-55.

Что касается масштабов информационных войн, обратимся к трехуровневой классификации, предложенной В.И. Кандаловым и Д.А. Карташовой. Они относят к собственно информационным войнам только события самого верхнего, стратегического уровня (могут сопровождать «традиционную» войну или предшествовать ей). Выделяется также оперативный уровень (к нему относятся отдельные информационные кампании) и тактический уровень (отдельные информационные акции в медиа)[44].

Приведем еще несколько классификаций информационных войн по различным основаниям. Одно из, казалось бы, «простых» разделений информационных войн основано на категоризации их в наступательные и оборонительные (по аналогии с «традиционными» войнами). Однако в действительности определить, должна ли та или иная информационная война относиться к наступательным или оборонительным для данного государства, бывает очень сложно, поскольку ведение кампаний в информационном пространстве отнюдь не всегда сопровождается формальным объявлением войны, поэтому определить момент ее начала (и, соответственно, определить сторону, начавшую войну) бывает крайне затруднительно.

Современные информационные войны тесно переплетены с некоторыми другими современными видами военных кампаний, также ориентированными на психику и восприятие и рассчитанными не только (и даже не столько) на боевые силы противника, сколько на его гражданское население. Одним из таких видов являются, к примеру, когнитивные войны. Как и информационные войны, они основаны на нефизических методах ведения войны. Ю. П. Сурмин и Н. В. Туленков, к примеру, выделяют четыре вида информационных войн по предмету конфликта: психологические (направлены на психику масс населения), коммуникационные (нацелены на коммуникационные системы противника), собственно информационную войну (за обладание информацией) и ценностно-мировоззренческую войну

[44] Кандалов, В. И., & Карташова, Д. А. (2023). Особенности реализации современных военных информационно-коммуникативных операций. *Социально-гуманитарные знания*, (9), 69-72.

(направлена на ценности населения), хотя в научном пространстве остается крайне дискуссионным вопрос, являются ли эти войны видами информационных войн или же отдельными видами противостояния[45].

Н.Р.К. Мехтиева предлагает критерий «видимости» (транспарентности) как основу для классификации информационных войн. По этому критерию они могут быть разделены на явные (открытые), главными непосредственными агентами которых национальные, региональные или глобальные масс-медиа, новостные корпорации, а также закрытые (латентные), способные принимать форму, к примеру, хакерских атак. Промежуточным (или гибридным) вариантом являются сетевые войны[46].

В целом для правильного позиционирования роли и места информационных войн в современном мире необходимо их рассматривать как неотъемлемый элемент более широкой категории «гибридных» войн. Эта категория также не имеет четкого сущностного определения и зачастую определяется по совокупности признаков – так, выдающийся российский политолог П.А. Цыганков отмечает, что для «гибридных» войн, по мнению ряда экспертов, характерны «во-первых, многообразие типов акторов, эволюционирующих в рамках гетерогенной системы и движимых многообразием мотивов с преобладанием экономических и культурных интересов; во-вторых, переменчивая конфигурация сражений, дающая преимущество то одной, то другой воюющей стороне; в-третьих, отказ противников от диалога и/или повторяющийся провал переговоров; наконец, в-четвертых, слабость и/или отсутствие интеграционных институтов»[47].

Другие эксперты, как отмечает Цыганков, определяют «гибридные» войны через их черты сходства и различия с «асимметричными» конфликтами и «традиционными» войнами: «как и в асимметричном вооруженном конфликте, в гибридной войне невозможно зафиксировать дату

---

[45] Сурмин Ю. П., Туленков Н. В. Теория социальных технологий: учебное пособие. Киев: МАУП, 2004. 605 с.

[46] Мехтиева, Н. Р. К. (2017). Информационные войны как" цифровой" аспект глобализации. *Век глобализации*, (3 (23)), 77-89.

[47] Цыганков, П. А. (2015). “Гибридная война”: политический дискурс и международная практика. *Вестник Московского университета. Серия 18. Социология и политология*, (4), 253-258.

начала и окончания, различить фронт и тыл, выявить статус бойца. Как и в нерегулярной войне, в гибридной трудно разделить вооруженные действия, угрозы, переговоры, четко разграничиваемые в классическом понимании войны. Не менее сложно идентифицировать носителя главной угрозы: являются ли таковыми террорист (террористическое формирование), враждебная идеология, акт вооруженного насилия, экономическое преступление. … Утрачивается момент окончательного "разгрома врага"»[48].

Д.А. Егорченков и Н.С. Данюк также обращают внимание именно на момент отсутствия «окончательной» победы – по их мнению, в «гибридных» войнах «ставка делается на тотальное изматывание противника, слом его способности противостоять организованному внешнему давлению, которое сочетается с «взломом» государства изнутри («5-я и 6-я колонны», деструктивные политические технологии «цветных революций», использование экстремистских и террористических формирований), что в конечном счете должно привести к антиконституционной «смене режима». Затем следует потеря государством своего суверенитета, установление над страной внешнего управления и, как следствие, разграбление ее ресурсной базы»[49].

В контексте нашего исследования следует обратить внимание на технологии информационной войны, активно применяемые в ходе «гибридных» войн: благодаря этим технологиям «война ведется одновременно во многих областях, на разных уровнях и в условиях непрерывного цикла: 7 дней в неделю, 24 часа в сутки. Особенно это относится к сфере информации, которая приобрела первостепенную важность в информационную эпоху, наступившую после окончания холодной войны. Главные сражения гибридной войны происходят в различных секторах этой сферы – от кибербразведки и использования

[48] Там же.

[49] Егорченков, Д. А., & Данюк, Н. С. (2018). Теоретико-идеологические подходы к исследованию феномена" гибридных войн" и" гибридных угроз": взгляд из России. *Вестник Московского университета. Серия 12. Политические науки*, (1), 26-48.

искусственного интеллекта до пропаганды и фейковых новостей»[50]. По мнению Цыганкова, «одной из особенностей «гибридной войны» являются широкие возможности современных информационных технологий, которые становятся средством намеренного искажения информации, распространения заведомо ложных сведений, вбросов сфабрикованных «фактов» (так называемых фейков), а также использование самых грязных социальных технологий, фальсификация истории. Проявляется многогранная направленность феномена в том, что …“гибридная война” втягивает в антагонизм все население и охватывает все сферы общественной жизни: политику, экономику, социальное развитие, культуру»[51].». Исследователь объясняет «гибридный» характер многих из новейших вооруженных конфликтов заинтересованностью американских политических элит в сохранении своего доминирования в глобальной политике.

Роль человеческого фактора в нетрадиционных конфликтах 21 века стала еще более важной в связи с драматическими изменениями, произошедшими в последние годы в средствах массовой информации, технологиях и культуре. Это век круглосуточного освещения новостей, когда люди могут отслеживать действия правительств и военных с бешеной скоростью с помощью смартфонов, кабельного телевидения и социальных сетей. Люди больше связаны друг с другом, но их внимание перегружено чередой отвлекающих факторов. Еще более тревожным является то, что общественность легко вводится в заблуждение дезинформацией.

Для военного и политического руководства, участвующего в нетрадиционной войне, эти факторы создают новые проблемы. В конце XX – начале XXI веков обязательным и главным атрибутом победы является завоевание превосходства в информационно-психологической сфере.[52] Это

---

[50] Тренин Д. Смягчение конфликта в условиях гибридной войны // Московский центр Карнеги. 2018. 25 янв. URL: http://carnegie.ru/2018/01/25/ru-pub-75296

[51] Цыганков П.А. «Гибридные войны»: понятие, интерпретации и реальность // «Гибридные войны» в хаотизирующемся мире XXI века / Под ред. П.А. Цыганкова. М.: Издательство Московского университета, 2015. С. 21.

[52] Грызлов В.М., Перцев А.Б. Информационное противоборство. История и современность. Вестник Академии военных наук. 2015;(2):124–128.

означает, что победа в нетрадиционной войне требует долгосрочного развертывания, начиная с "нулевой фазы", задолго до начала вооруженного насилия. Взаимодействие на этой "нулевой фазе" является эффективным, поскольку оно направлено на использование невоенных средств для формирования оперативной обстановки и работы по предотвращению насилия с самого начала. И поскольку одним из инструментов нетрадиционной войны являются средства мягкой силы, такие как дипломатия, экономическая помощь и пропаганда, требуется от руководства терпение и настойчивость. Мягкая сила не обеспечивает немедленных явных признаков победы, и общественность может считать такие мягкие меры несостоятельными или излишними.

Теоретики давно признали решающее значение человеческого фактора в войне. В частности, военные стратеги Карл фон Клаузевиц и китайский военный мыслитель Сунь-Цзы уделяли особое внимание поддержке населения и моральному аспекту войны. Они считали, что моральный дух и легитимность военной кампании зависят от интересов и пожеланий ее сторонников, которые поддерживают ее, голосуют за нее и страдают ради нее. Поэтому лидеру следует уделять внимание как своему собственному народу, так и народу противника, проявляя "любовь, справедливость и честность" по отношению к своим гражданам, а одновременно психологически ослабляя вражеское население, постепенно истощая его физические и психологические ресурсы. "Человеческий фактор" представляет собой третий элемент "Троицы" Клаузевица и, возможно, играет наиболее важную роль в контексте нетрадиционной войны. Изматывание воли населения может нанести противнику больший ущерб, чем захват территории или нанесение физических повреждений.

Информационная война представляет собой борьбу за захват и удержание контроля над информацией. Если рассматривать информационную войну как часть «традиционной» войны, то есть как попытку воюющих сторон захватить инициативу на поле боя, контролируя

поток информации и разведывательные данные, то можно смело утверждать, что она появилась задолго до появления соответствующего термина и сопровождает практически всю историю человечества – как и собственно «традиционные» войны.

В рамках информационной войны блокируется информационный поток противника, создается ложная информация для оказания воздействия и ослабления способностей командования и управления противника. Одновременно с этим принимаются меры для защиты собственных систем командования и управления от подобных атак со стороны противника.

Уточняя имеющиеся определения, можно подчеркнуть, что целью информационной войны является население страны-противника или отдельные группы в составе этого населения (враждебно, дружественно или нейтрально настроенные), на ценностные установки и убеждения которых осуществляется информационное воздействие с целью достижения такого их поведения, которое выгодно атакующей стороне.

Итак, информационные войны представляют серьезный вызов для всех, кто работает с информацией. Борьба с этим явлением требует сложных технических решений, организационных мер и согласованной работы участников этого процесса. При этом формирование и влияние этих вызовов реализуется в условиях больших вызовов и изменений в обществе.

Профессор МГУ Н. Л. Смакотина выделяла следующие ключевые процессы глобальных социальных трансформаций: ослабление социальных структур; повышение субъективности социальных субъектов; преобразования и кризис «институтов современности»; рост неопределенности и нестабильности; социальная и культурная диверсификация; ослабление социальных границ. В качестве основных причин таких трансформаций профессор Н.Л. Смакотина называет: развитие современной медицины; снижение рождаемости; процессы урбанизации; миграционные процессами; урбанизацию сельского пространства с точки

зрения демографических и культурных моделей[53]. Профессор МГУ В.В. Кочетков указывает, что процессы активной неолиберальной глобализации в конце 1990-х – начале 2000-х годов, приводя к унификации образования, усилили использование этого института для ведения информационных войн на территории геополитических противников коллективного Запада[54]. При этом В.В. Кочетков отмечает, что одним из наилучших способов противостояния информационным войнам является практика проведения успешных международных событий, способствующих укреплению имиджа государства[55]. По мнению профессора И.В. Ильина, важнейшими факторами которых являются:1) Эпоха цифровизации, активная фаза которой началась примерно с начала нового тысячелетия (когда объем информации, хранимой в цифровом виде, превысил объем аналоговой информации – 2002 год – определение И.В. Ильина) является ключевым процессом, обеспечивающим генеральную социальную трансформацию глобального уровня – формирования «цифровой цивилизации» (определение акад. Г.В. Осипова). Цифровизация в социальном плане порождает: 1) формирование виртуальных сообществ; 2) уязвимость людей, обществ, стран перед цифровыми атаками. 2) Обострение внутристрановых социальных противоречий (рост протестной политической активности, начиная с 2000-х годов). 3) Осознание человечеством единства проблемного поля в рамках единой глобальной ресурсно-энерго-экологической проблемы (глобальное потепление, «пределы роста» и т.д.). 4) Глобальное геополитическое обострение: «восхождение» Глобального Большинства (экономическое, политическое, военное), обострение глобальной геополитической конкуренции (за ресурсы, территории), стремление коллективного Запада к сохранению глобальной гегемонии, рост числа и остроты вооруженных

[53] Смакотина Н.Л. Глобальные социальные трансформации в контексте демографических изменений и урбанизации. Acta Biomedica Scientifica. 2022;7(3):47-56. https://doi.org/10.29413/ABS.2022-7.3.6

[54] Кочетков В. В. Глобализация в образовании: информационная война и "промывание мозгов" или доступ к мировым знаниям и благам цивилизации? // Вестник Московского университета. Серия 18: Социология и политология. — М.: Издательство Московского государственного университета, 2005. — № 1. — С. 144—159.

[55] Кочетков В.В. Роль чемпионата мира по футболу 2018 г. в формировании имиджа России // Социологические исследования, 2020, № 7, С. 82-92.

конфликтов и гибридных войн с ключевой информационной составляющей. 5) Старение населения, охватившее развитые и охватывающее развивающиеся страны, ведущее к усилению распространения консервативных ценностей, замедлению технологического и экономического роста, укреплению стагнационных тенденций в развитии общества[56].

Многообразие современной терминологии информационных войн, а также их частую «мимикрию» под социокультурный обмен стран и цивилизаций и иные проявления позитивной мягкой силы заставляют предложить уточняющую их классификацию.

Информационные войны целесообразно разделять по направленности на информационно-психологические, то есть направленные на сознание человека и информационно-технологические, направленные на информационную инфраструктуру.

Первые включают 1) военную пропаганду, 2) информационно-экстремистские или террористические действия, 3) информационно-мировоззренческие войны, (включающие, в свою очередь, а) социокультурные войны, б) «войны памяти» или войны исторических нарративов, в) информационно-политические войны); 4) информационно-экономические войны, ведущиеся против хозяйствующих субъектов или экономического потенциала в целом стран-конкурентов; 5) информационно-экологические войны, направленные на дискредитацию природного потенциала. Круг ключевых технологий, используемых для подготовки и ведения информационных войн, определяется прежде всего глобальным технологическим прогрессом в цифровизации и расширяющимся доступом широких слоев населения разных стран к информационной среде (рис. 1.1)

[56] Ильин И. В. Глобальные проблемы цифровой трансформации общества// Социальные науки и образование в условиях становления электронно- цифровой цивилизации / Научно-практическая конференция. – М.; СПб.: Нестор- История, 2020. — 152 с. С. 18-32/

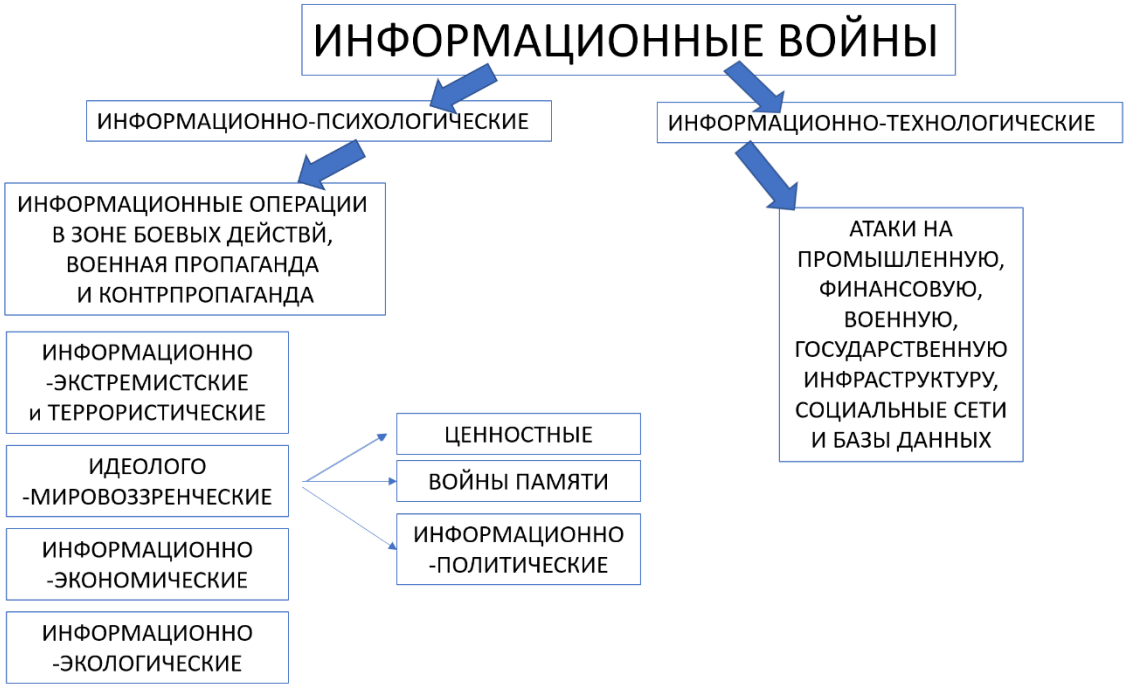

Рисунок 1.1. – Классификация современных информационных войн по направленности воздействия.

Составлено автором на основе теоретических подходов к изучению информационных войн.

В этой связи важно уточнить, происходит ли критические изменения сути, содержания и смысла информационных войн в условиях глобальных социальных трансформаций.

1.2. Информационные войны в киберпространстве

Как было отмечено в предыдущем параграфе, информационные войны определяются различным образом, и потому зачастую не существует четкого разделения между этим понятием и смежными понятиями – к примеру, таким, как кибервойны. В настоящей работе мы следуем подходу Л.В. Мониной, которая считает информационно-психологические и информационно-коммуникативные (кибервойны) двумя видами информационных войн [57] . В настоящем параграфе будут рассмотрены сходства и различия этих двух видов.

Представляется, что два вида информационных войн, выделенные Л.В. Мониной, во многом перекликаются с подходом О.Г. Леоновой. Хотя, в отличие от подхода Мониной, профессор Леонова полагает не кибервойну как вид информационной войны, а, напротив, информационное противоборство как вид кибервойн, их подходы имеют важное сходство – профессор Леонова разделяет технологии кибервойн на «жесткие», которые «имеют целью разрушение сетей управления инфраструктурой страны, что может привести к фактически уничтожению государства», и мягкие, «проявляющиеся как информационное противоборство в цифровом информационном пространстве»[58].

Представляется целесообразным последовать подходу А.А. Смирнова – проведя обзор значительного числа научных работ по данной теме, он пришел к выводу, что «большинство отечественных исследователей выделяет два основных направления (или вида) [информационных войн]: информационно-техническое, объектами воздействия которого являются информационно-технические системы (системы связи и управления,

[57] Монина Л. В. Проблема обеспечения информационной безопасности России. В: Современная Россия и мир: альтернативы развития (Информационные войны в международных отношениях): сборник научных статей/под ред. Ю.Г. Чернышова. — Барнаул : Изд-во Алт. ун-та, 2012. 244 с. С. 29-34. С. 29.

[58] ЛЕОНОВА, О. Г. (2018). Кибервойна и противоборство в цифровом информационном пространстве. *Информационное общество*, (2), 43-48.

компьютерные и телекоммуникационные системы, радиоэлектронные средства и т. д.), и информационно-психологическое, для которого в качестве таковых выступают информационно-психологические объекты (психика человека и общественное сознание)»[59].

Остановимся подробнее на понятии кибервойн. Одно из ранних определений кибератак было предложено ФБР США, которое в 1995 году предложило рассматривать кибератаки как преднамеренную, политически мотивированную атаку против информации, компьютерных систем, компьютерных программ и баз данных в виде насильственного вторжения со стороны международных групп или секретных агентов[60].

Однако очевидно, что с момента выработки этого определения кибератаки и кибервойны в целом значительно усложнились и приобрели массу новых форм и видов. В этом свете заслуживает внимания определение П.И. Антоновича, который полагает, что кибервойна – это «систематическая борьба в кибернетическом пространстве между государствами (группами государств), политическими группами, экстремистскими и террористическими и т.п. группировками, проводимая в форме атакующих и защитных действий. Основными целями как нападения, так и защиты в кибервойне являются информационные ресурсы, свойства которых с точки зрения безопасности (целостность, доступность и конфиденциальность) могут быть нарушены»[61]. Очевидно, что здесь речь идет о «жестких» кибервойнах (в терминологии О.Г. Леоновой) и информационно-коммуникативных войнах (в рамках подхода Л.В. Мониной).

Заслуживает внимания подход К.А. Панцерева и Р.С. Выходца, которые подчеркивают, что «концепция кибервойны концентрируется на теоретическом осмыслении использования компьютеров и сети Интернет для нанесения ущерба противнику, а также выработке механизмов защиты от

---

[59] Смирнов А. Информационно-психологическая война //Свободная мысль. – 2013. – №. 6. – С. 81-96. С. 83.
[60] Капто, А. С. (2013). Кибервойна: генезис и доктринальные очертания. *Вестник Российской академии наук*, *83*(7), 616-616.
[61] АНТОНОВИЧ, П. И. (2011). О современном понимании термина" кибервойна". *Вестник Академии военных наук*, (2), 89-96. С. 94.

угроз в киберпространстве и противодействия кибератакам, которые включают в себя финансовые преступления и шпионаж против человека, организаций и государства (киберпреступность), действия негосударственных акторов, направленные на взлом компьютерных систем критически важных объектов, государственных органов, транспорта и т. д. (кибертерроризм), использование киберпространства против вооруженных сил противника, инфраструктуры и гражданского населения (кибервойна)» [62].

Обратимся также к определению кибервойн, данному выдающимся российским политологом, профессором А.С. Капто. Он также полагает кибервойну составной частью информационной войны и отмечает, что «кибервойна не существует вне традиционной, хотя конкретные кибероперации могут проводиться (и ныне проводятся во многих регионах планеты) вне войны как таковой. Кибервойна представляет собой угрозы атак и со стороны отдельных хакеров, и со стороны террористических групп и государств. Она предполагает нарушение деятельности или полный вывод из строя систем управления государством и вооружёнными силами за счёт воздействия на компьютерные сети, в результате чего государственные и военные институты могут оказаться полностью парализованными и неспособными к организации сопротивления агрессору» [63]. Очевидно, что здесь также речь идет о «жестких» кибервойнах (в терминологии О.Г. Леоновой) и информационно-коммуникативных войнах, т.е. направленных на разрушение информационно-коммуникационных систем противника (в рамках подхода Л.В. Мониной).

В чем заключается отличие «жестких» кибервойн от «традиционных» войн? Нам представляется, что можно выделить несколько принципиальных черт:

– Кибератака осуществляется не на физические объекты, а на их системы управления, базы данных и другие нефизические объекты. Тем не

[62] Выходец Р. С., Панцерев К. А. Сравнительный анализ современных концепций информационного противоборства. Евразийская интеграция: экономика, право, политика. 2022; 16 (4): 139–148. С. 142.
[63] Капто А. С. (2013). Кибервойна: генезис и доктринальные очертания. *Вестник Российской академии наук, 83*(7), 616-616.

менее, хотя кибератака производится в информационном пространстве, вызванные ею разрушения могут быть вполне очевидны в физическом мире и выводить из строя физически существующие объекты. Однако не все кибератаки таковы – их целью может быть не выведение из строя объектов критической инфраструктуры (таких, как электростанции и сети электроэнергетики), но и, к примеру, «слив» конфиденциальных и/или секретных данных в открытый доступ в сеть Интернет, шпионаж (в том числе промышленный) и т.д. Такое разнообразие затрудняет создание четкого определения кибератаки – и, соответственно, существенно усложняет введение этого понятия в правовое поле и выработку политики, направленной на борьбу с кибератаками. Наиболее сложны в этом плане кибератаки, имеющие целью «расшатывание социально-экономических и политических устоев общества; дестабилизацию, а впоследствии и трансформацию социально-экономической и политической системы страны-мишени»[64], т.е. кибератаки, соединяющие в себе «жесткие» и «мягкие» технологии.

– Кибервойна необязательно сопровождает «традиционную» войну или даже вооруженный конфликт; она может предшествовать им, происходить параллельно с ними, или даже «замещать» традиционные боевые действия. При этом начало кибервойны не сопровождается формальным объявлением войны и не имеет иных важных признаков начала и/или завершения «традиционной» войны; не происходит вторжения живой силы атакующего государства на территорию противника и т.д. Из этого проистекает фундаментально важное отличие, подмеченное А.С. Капто – «в ответ на кибератаку или киберконфликт, осуществлённые какой-то страной без начала боевых действий, невозможно применение пятой статьи Вашингтонского договора НАТО о коллективной безопасности. Другими

[64] Леонова, О. Г. (2018). Кибервойна и противоборство в цифровом информационном пространстве. *Информационное общество*, (2), 43-48.

словами, в отсутствии реальных боевых действий кибервойна не может быть классифицирована в качестве таковой»[65].

– Кибератаки, киберконфликты и даже полномасштабные кибервойны обходятся атакующим государствам значительно дешевле, чем традиционные боевые действия, поскольку не требуют масштабной мобилизации человеческих, технических и иных ресурсов, организации снабжения и т.д. Более того, источник кибератак зачастую сложно или вовсе невозможно определить.

– Кибератаки происходят в режиме реального времени и потому позволяют атакующему государству более оперативно реагировать на изменение политической ситуации, какие-либо действия, предпринимаемые противником, и т.д. Вкупе с относительно невысокой стоимостью организации таких атак это зачастую делает их очень эффективными.

Все эти факторы в общей сложности обусловили появление нового направления выстраивания национальной безопасности, а именно обеспечения кибербезопасности – то есть выстраивания системы защиты национальных интересов в киберпространстве (которая, по Капто, включает не только оборонные, но и наступательные технологии). В Национальной военной стратегии США от 2004 года киберпространство было объявлено «областью» конфликта наряду с воздушным, наземным, морским и космическим пространствами – при этом признание киберпространства в качестве такой области на практике означало начало его активного освоения Штатами с целью доминирования в этом пространстве.

Действительно, хотя кибератаки существуют с момента появления Интернета, на начальных стадиях его развития большинство из них были инициированы отдельными лицами и хакерскими группами, в основном ради демонстрации навыков, кражи информации или вымогательства денег, и редко имели политические мотивы.

---

[65] Капто, А. С. (2013). Кибервойна: генезис и доктринальные очертания. *Вестник Российской академии наук, 83*(7), 616-616.

Однако с развитием Интернета и становлением его в качестве неотъемлемой части жизни человека он превратился в многоуровневое и многомерное сложное пространство, в котором люди общаются и действуют. Следовательно, сложные международные отношения, присутствующие в реальном мире, неизбежно отражаются в киберпространстве. Война, оставаясь постоянной и непреодолимой проблемой для человечества, начинает проявлять себя и в киберпространстве.

Частота и интенсивность кибервойн продолжают расти, и в новостях появляются отчеты о многочисленных транснациональных кибератаках. Однако они представляют лишь верхушку айсберга. Существует множество неофициальных атак, о которых не сообщается. По мере роста их числа, кибервойны также приобретают новые черты, связанные с целенаправленностью и эффективностью атак.

На данный момент невозможно оценить масштаб всемирных киберсил, однако методы атак и разрушительные возможности, которые они продемонстрировали, не уступают традиционной военной мощи. В прошлом кибератаки были направлены преимущественно на сетевую инфраструктуру с целью парализовать сетевые соединения противника.

Однако сейчас кибератаки начинают нацеливаться как на военные, так и на гражданские объекты в реальном мире. Потенциальными целями кибервойны становятся такие объекты национальной инфраструктуры, как электросети, водопроводные системы, транспортные сети, нефтегазовые сети и сети финансовых терминалов. Нападения на электросети, например, могут привести к значительным экономическим убыткам, оцениваемым в сотни миллионов долларов при незначительных затратах для атакующей стороны. Представимы сценарии, включающие нарушение работы сетей финансовых терминалов, вызывающие социальную панику, а также атаки на транспортные и нефтегазовые сети, которые могут привести к жертвам и материальным убыткам.

По мере того, как государства становятся доминирующими акторами в киберпространстве, кибератаки перестают быть атаками хакеров-одиночек и все больше превращаются в настоящие войны, связанные с политической повесткой дня.

В связи с этим в последние годы многие страны ускорили развитие кибервойск и включили понятие кибербезопасности в свои концепции и стратегии национальной безопасности. Например, в течение 2019 года ВВС США сформировали еще одно совершенно новое боевое подразделение – 16-е ВВС. Как специализированное подразделение, ориентированное на кибервойну, 16-е ВВС является единственным оперативным подразделением ВВС США для глобального разведывательного наблюдения, киберразведки и ведения радиоэлектронной борьбы.

В 2018 году, по указанию президента Трампа, киберкомандование США было повышено до уровня совместного боевого командования первого уровня. В его распоряжении находятся 133 подразделения кибермиссии с общей численностью 6,2 тыс. человек.

В последней редакции Стратегии национальной безопасности Российской Федерации руководство страны также признало, что в условиях текущей геополитической турбулентности «космическое и информационное пространства активно осваиваются как новые сферы ведения военных действий» [66] и обозначило развитие безопасного информационного пространства и защиту российского общества от деструктивного информационно-психологического воздействия в качестве одного из стратегических национальных приоритетов.

В документе также уделяется внимание необходимости обеспечения международной информационной безопасности. Однако значимость киберугроз в этом документе, на наш взгляд, существенно занижена и не вполне осознается ее масштаб. Это можно отметить и в отношении Доктрины

[66] Указ Президента Российской Федерации от 02.07.2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации». П. 17. URL: http://www.kremlin.ru/acts/bank/47046/page/1 (дата обращения 31.10.2024).

информационной безопасности РФ, принятой в 2016 году – понятие киберугроз и кибервойн там отсутствовало вовсе, присутствовал лишь термин «угроза информационной безопасности Российской Федерации», определяемый как «совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере»[67].

Среди документов, уделяющих внимание проблеме кибербезопасности как одной из центральных, можно в первую очередь назвать Федеральный закон от 26.07.2017 N 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации», в соответствии со Ст. 5 которого была создана Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации[68]. Действие системы распространяется на объекты критической инфраструктуры и дипломатические представительства РФ за рубежом.

Создание данной системы, безусловно, является большим шагом вперед в вопросе обеспечения кибербезопасности России, однако она охватывает лишь ограниченное число объектов (хотя и безусловно важных), и не распространяется на другие важные объекты (к примеру, банки). Между тем, с распространением информатизации и цифровизации, перечень категорий объектов, способных подвергнуться кибератакам с серьезными отрицательными последствиями, постоянно возрастает.

Часть этих задач решает Национальный координационный центр по компьютерным инцидентам, утвержденный приказом директора ФСБ России в 2018 году. Основной задачей специалистов центра является обнаружение компьютерных атак на промышленную, военную, продовольственную, энергетическую и банковскую сферы РФ. Однако К.В. Найденкова и В.В.

---

[67] Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения 31.10.2024).

[68] Федеральный закон от 26.07.2017 N 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации»

Чугунов справедливо отмечают, что «основной проблемой России в применяемых методах защиты является отсутствие уникальности», поскольку организации подобного функционала «давно существуют во многих странах, при этом они охватывают безопасность не только объектов КИИ, но и частичной доли коммерческих предприятий» [69].

Появление государств в роли главных участников в кибервойне также привело к дальнейшему увеличению уровня киберборьбы на практике. Таким образом, кибервойна перестала быть скрытой операцией и стала мощным инструментом в противостоянии между странами. В таких условиях многие страны и правительства уже не уклоняются от кибервойн, а признают существование «кибервойск» и разрабатывают дополнительные стратегические рекомендации.

Ресурсы, которые правительства могут мобилизовать и использовать для ведения кибервойны, намного больше, чем у частного сектора. Силы кибервойск быстро формируются, и их возможности как в наступлении, так и в обороне, весьма существенны. На конкурсе DEF CON 2019, семь хакеров, нанятых Пентагоном, смогли взломать внутренние системы F-15, главного истребителя США, всего за два дня.

С ростом разрушительной силы кибервойны начала формироваться концепция киберсдерживания как эффективного дополнения к традиционному сдерживанию. Белый дом представил Конгрессу доклад о политике киберсдерживания еще в 2015 году; особое внимание в документе уделялось федеральному (национальному) уровню, что означает готовность правительства США мобилизовать все национальные ресурсы, включая дипломатические, разведывательные, военные, экономические и прочие, для успешной реализации стратегии киберсдерживания.

Действия, предпринимаемые Соединенными Штатами против России, Ирана и других стран в последние годы, в основном соответствуют

[69] Найденкова, К. В., & Чугунов, В. В. (2022). Институциональные аспекты обеспечения кибербезопасности в РФ и за рубежом. In *Финансовая безопасность. Современное состояние и перспективы развития* (pp. 240-252). Материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ. Том 1. Москва: НИЯУ МИФИ, 2022. С. 241-242.

вышеупомянутым идеям. Это включает в себя отказ от чрезмерных дипломатических контактов с враждебными странами, максимально возможное избегание традиционных военных действий и использование кибердударов в качестве основного метода наступления, а также всестороннее применение стратегий «отмены» и «наказания». Демонстрируя свои возможности в кибервойне, Соединенные Штаты стремятся добиться подчинения своей воле со стороны противников.

В последние годы лавинообразно нарастают риски для России, связанные с кибератаками и киберугрозами от недружественных государств. Особенно заметной эта тенденция стала в 2022 году число кибератак на государственные и частные информационные системы России выросло в 7 раз по сравнению с 2021 годом. Основными их объектами были сайты госорганов (22%), системы, содержащие персональные данные (16%) и СМИ (15%)[70].

К.В. Найденкова и В.В. Чугунов, изучавшие мотивы таких атак, показывают, что распределение мотивов изменилось и появился новый мотив – кибервойна, «суть которой заключается в атаке на объекты критических инфраструктур (КИИ) с целью воздействия на системы обеспечения жизнедеятельности государства, а также в атаке на компьютерное оборудование гражданского и военного назначения с целью вывода его из строя» [71] . Однако вспышки кибератак случались и в период, предшествовавший началу СВО – например, большое количество кибератак было зафиксировано в начале 2021 года, их мишенью стали российские учреждения, участвовавшие в разработке и производстве вакцин от COVID-19.

К.В. Найденкова и В.В. Чугунов обращают также внимание на важную тенденцию в сфере финансирования Россией развития своей

[70] Количество кибератак на сервисы и структуры России в 2022 году выросло в семь раз// ТАСС. 21 марта 2023 года. URL: https://tass.ru/ekonomika/17327093 (дата обращения: 1.09.2025).

[71] Найденкова, К. В., & Чугунов, В. В. (2022). Институциональные аспекты обеспечения кибербезопасности в РФ и за рубежом. In *Финансовая безопасность. Современное состояние и перспективы развития* (pp. 240-252). Материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ. Том 1. Москва: НИЯУ МИФИ, 2022. С. 241-242.

кибербезопасности. С одной стороны, это финансирование продемонстрировало колоссальный рост – в 1,5 раза за 2019 – 2021 гг. С другой стороны, даже при таком росте объем бюджетных средств, выделяемых на цели, связанные с кибербезопасностью, существенно уступает в абсолютном исчислении таковым расходам в США.

В условиях информационного противостояния двух государств, когда Россия вынуждена давать адекватный ответ на беспрестанные попытки США подавить РФ в глобальном информационном поле, такое отставание может сыграть критически важную негативную роль в обеспечении кибербезопасности и разработке требуемых для этого технологий, а также обеспечении сферы кибербезопасности высококвалифицированными патриотичными кадрами.

Важный шаг в этом направлении был сделан в 2022 году, когда Президент России В.В. Путин подписал указ, вводящий сразу несколько серьезных мер поддержки ИТ-компаний (существенное снижение ставки налогообложения) и ИТ-специалистов (льготная ипотека, отсрочка от армии). Представляется, что эти меры помогли снизить долю ИТ-специалистов, желающих эмигрировать из России и продолжать трудовую деятельность и строить карьеру в других странах, в том числе недружественных к России.

Представляется, что в поисках нетиповых решений по обеспечению кибербезопасности в высшей степени целесообразно обратиться к опыту Китая, путь которого в этой области действительно уникален. Во-первых, кибербезопасность является приоритетом высочайшего уровня, то есть вопросы ее достижения и сохранения регулируются непосредственно на уровне Коммунистической Партии Китая, которая и осуществляет регулирование этой сферы через соответствующие органы в своем составе.

Главным, центральным элементом этой системы, получившей название «Золотой щит», является существенное ограничение числа компьютеров и других электронных устройств, имеющих доступ к ресурсам сети Интернет, находящимся за пределами собственно китайского сегмента

Интернета – а устройства, имеющие такой доступ, тщательно контролируются специалистами по кибербезопасности.

Это резко ограничивает число устройств, которые могут подвергнуться зарубежным кибератакам. Международные каналы связи и интернет-провайдеров связывает система серверов, автоматически оценивающая всю информацию согласно установкам от руководства страны. Система фильтрации контента играет ключевую роль в интернет-пространстве Китая[72].

Количество устройств, подключенных к Интернету, является огромным. Самораспространяющиеся компьютерные черви представляют собой серьезную угрозу с конца 1990-х и начала 2000-х годов, часто заражая сетевые компьютеры в больших масштабах. Их способность представлять опасность объясняется двумя факторами: отсутствием защиты на компьютерах и тем, что компьютеры напрямую подключены к Интернету, через который они могут свободно взаимодействовать.

Исходя из прошлого опыта, распространение устройств "Интернет вещей" (IoT) сегодня вызывает серьезную тревогу. Несмотря на то, что устройства IoT могут включать в себя дверные звонки, термостаты, холодильники, телевизоры и камеры безопасности, очень немногие из них оснащены программным обеспечением для обнаружения и защиты от киберугроз. Исследование 2020 года показало, что 98% из 1,2 миллиона опрошенных IoT-устройств используют незашифрованный сетевой трафик, 83% устройств для медицинской визуализации работают на неподдерживаемом программном обеспечении, а 57% подвержены атакам средней или высокой степени уязвимости.

Однако следует отметить, что это исследование было проведено спустя четыре года после инцидента с ботнетом Mirai, который подчеркнул уязвимость IoT-устройств. В то время вирусы получили доступ к сотням

[72] Найденкова, К. В., & Чугунов, В. В. (2022). Институциональные аспекты обеспечения кибербезопасности в РФ и за рубежом. In *Финансовая безопасность. Современное состояние и перспективы развития* (pp. 240-252). Материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ. Том 1. Москва: НИЯУ МИФИ, 2022.

тысяч IoT-устройств по всему миру и использовали их для проведения кибератак. Поэтому, несмотря на определенный опыт в этой области, вызывает тревогу факт, что в плане повышения безопасности IoT-устройств было предпринято сравнительно немного мер.

Устройства "Интернет вещей" (IoT) используются не только в гражданских, но и в военных кибероперациях. Связанные с ними уязвимости могут особенно усилить уязвимость глобальных организаций. В то время как риск причинения вреда гражданскому населению часто можно регулировать путем нацеливания на конкретные устройства IoT, обратное верно для кибероперацій, которые направлены на уязвимые устройства без дополнительной фильтрации. Поэтому странам важно оценивать значительные риски, связанные с кибероперациями, использующими IoT-устройства, поскольку их потенциальное воздействие на медицинские учреждения, критическую инфраструктуру, образовательные учреждения и другие чувствительные сети часто трудно обнаружить.

Кроме того, мы свидетельствуем некоторым тревожным изменениям в кибероперациях. Два крупных киберинцидента, произошедших за последний год, включают в себя нарушение цепочки поставок в компании SolarWinds и нарушение работы сервера Microsoft Exchange в марте 2021 года. Хотя эти два инцидента не включают в себя вооруженные конфликты, они подчеркивают новую тенденцию: кибероперации проводятся на уровне, который не вызывает вооруженных конфликтов и, следовательно, не подпадают под защиту, предоставляемую гражданским лицам в соответствии с международным гуманитарным правом.

Предотвращение вреда гражданскому населению в ходе военных кибероперацій во время вооруженных конфликтов представляет собой значительный шаг в направлении признания сложности этой проблемы. Этот отчет способствует дальнейшему развитию и интерпретации норм и правовых правил для предотвращения ущерба, причиненного гражданскому населению в ходе военных кибероперацій.

Благодаря 5G, кибервойна, несомненно, становится еще более угрожающей. Несмотря на удобства, которые «Интернет вещей» приносит в жизнь людей, он также означает, что любая вещь, имеющая выход в глобальную сеть, может стать мишенью для кибератак. Критически важные инфраструктуры, такие как системы управления промышленными процессами, сети транспорта и интеллектуальные электросети, столкнутся с еще более серьезными угрозами в области кибербезопасности. Рост числа сетевых узлов затрудняет защиту всех аспектов сети; высокая пропускная способность и низкая задержка позволяют злоумышленникам быстрее достигать своих целей. В связи с революционной технологией искусственного интеллекта можно ожидать коренных изменений в способах ведения кибервойны и функционирования интернета. Искусственный интеллект способен находить уязвимости гораздо более эффективно, чем человек.

Более того, искусственный интеллект может быть использован для создания оружия. Технологии искусственного интеллекта могут революционизировать военное дело, например, путем применения беспилотных летательных аппаратов, беспилотных подводных лодок и крылатых ракет, оснащенных ИИ. Эти технологии обеспечат более высокую точность и разрушительную мощность, и могут вызвать революцию в военном деле. Можно предположить, что будущая кибервойна будет характеризоваться как "сетецентрическая война", в основе которой будут лежать сети искусственного интеллекта. Они будут способствовать принятию оптимальных военных решений, планированию боевых операций и прогнозированию ситуации на поле боя. Следовательно, в будущем военная мощь страны будет в значительной мере зависеть от её киберпотенциала, и киберпотенциал может сильно зависеть от её технологической мощи в области искусственного интеллекта.

Наиболее распространенным видом атак в киберпространстве являются так называемые DDOS-атаки, интенсивность которых в отношении структур

внутри разных стран мира определенно зависит от их размера и значимости. Так, в 2024 году наибольшее число атак приходилось на структуры в США, Китае и Индии – в крупнейших экономках мира (если рассматривать уровень ВВП по ППС), доля США в общем объеме атак составила 14,3%, при этом в ходе выборов президента этой страны в ноябре 2024 года произошло трехкратное увеличение их интенсивности по сравнению с остальными месяцами. Китая также выросла на 2% с 2023 года и составила 12,8%, Индии – на 1% - до 10,2%. 4,5 и 6е место заняли, соответственно Великобритания (9,8%, годовой рост на 1,6%), Франция (9,2%, рост на 0,8%) и Германия (8,4%, рост на 1,6%), эти увеличения также связывают с выборными процедурами. Интересно при этом, что на 7м месте – небольшой по населению (6,8%, рост за год почти в 2 раза), являющийся восточно-азиатским экономическим «хабом». Россия в данном списке была только на 8м месте (7,3% атак, в 2023 году – на 7м, но рост за год – почти двукратный). Финансовый (22% от всех атак) и государственный сектор (19%) киберпространства стали наиболее атакуемыми в последние годы, вместе с тем, впервые в числе наиболее атакуемых сфер в 2024 году оказались промышленность и логистика (7 и 5% всех инцидентов, соответственно)[73].

Таким образом, очевидно, что помимо политической составляющей к кибератаках значительную роль играет конкурентная борьба, осуществляемая не в военно-политической, а, скорее, в экономической плоскости, а также – криминальными структурами.

[73]DDoS-атаки в мире и России: отчёт StormWall за 2024 год// URL: https://stormwall.pro/resources/blog/ddos-2024-godovoj-otchet (дата обращения: 1.08.2025).

1.3. Информационно-психологические войны

Близко к информационным войнам находится понятие психологических войн. К примеру, в определении информационной войны, данном Г.Г. Почепцовым, как «коммуникативной технологии по воздействию на массовое сознание с долговременными и кратковременными целями»[74] эта близость особенно заметна. Сам Почепцов отмечает: «Целями такого воздействия на массовое сознание является внесение изменений в когнитивную структуру с тем, чтобы получить соответствующие изменения в поведенческой структуре. Практически то же самое делает психотерапия, только на уровне индивидуального сознания»[75].

Информационно-психологические войны по самой сути своей являются предметом междисциплинарных исследований; они имеют не только политические, но и психологические, лингвистические, правовые, социальные и другие особенности. Это становится заметно при сопоставлении различных определений данного явления.

Так, по определению, данному учеными-лингвистами А.П. Сковородниковым и Г.А. Копниной, «Информационно-психологическая война — это противоборство сторон, которое возникает из-за конфликта интересов и осуществляется путем намеренного, прежде всего речевого, воздействия на сознание противника (народа, коллектива или отдельной личности) для его когнитивного подавления и/или подчинения, а также посредством использования мер информационно-психологической защиты от такого воздействия»[76].

И.В. Сергеев, характеризуя информационно-психологические войны с правовой точки зрения, фокусируется на «фактическом отсутствии международных и национальных правовых норм и социальных механизмов, препятствующих обострению конфликтов и регулирующих степень их

---

[74] Почепцов, Г. Г. Информационные войны / Г. Г. Почепцов // -М. ; Киев : Рефл-бук Ваклер, 2000. – 574 с.
[75] Там же.
[76] Сковородников А. П., Копнина Г. А. Лингвистика информационно-психологической войны: к обоснованию и определению понятия // Политическая лингвистика. – 2016. – №. 1. – С. 42-50.

социальной опасности» [77] . Как уже отмечалось выше, определить хронологически точки начала и окончания кибервойн бывает крайне сложно из-за характера действий, состоящих из отдельных кибератак.

Для информационно-психологических войн решение этой задачи становится и вовсе фактически невозможным, поскольку таким войнам присуща «скрытность и маскировка под другие социальные процессы» [78], и точно определить, в какой степени изменения сознания и поведения населения являются объективным процессом, а в какой – результатом скрытого манипулирования и влияния извне, крайне затруднительно.

А.В. Манойло определяет информационно-психологические войны через их задачи, к которым причисляет следующие: «трансформация структуры национальных экономических, политических, социально-культурных, информационно-психологических пространств участников международных отношений в соответствии с собственными принципами формирования информационно-политической картины мира; достижение военно-политического превосходства и безусловного лидерства в сфере международных отношений; достижение целей национальной экономической, идеологической, культурной, информационно-психологической экспансии; обеспечение благоприятных условий для перехода собственной национальной системы социально-политических отношений на новый, более высокоразвитый и высокотехнологичный этап эволюционного развития»[79].

Однако представляется, что определение Манойло верно лишь для информационных войн, ведущихся в современном обществе и во многом связано с современными реалиями на глобальной политической арене. Между тем, информационно-психологические войны имеют значительно более глубокую историю, поскольку попытки психологического воздействия

---

[77] Сергеев И. В. Информационно-психологическая война как форма эскалации межгосударственных конфликтов // Информационные войны. – 2015. – №. 2. – С. 38-41. С. 39.

[78] Сергеев И. В. Информационно-психологическая война как форма эскалации межгосударственных конфликтов // Информационные войны. – 2015. – №. 2. – С. 38-41. С. 39.

[79] Манойло, А. В. К вопросу о содержании понятия «информационная война». *Дневник АШПИ*, 2012, (28), 17-24. С. 19-20

на противника, запугивания его имели место даже в самых ранних человеческих обществах.

Великий древнекитайский философ Сунь Цзы причислял к методам такого воздействия «разложение всего позитивного, что имеется у противника, дискредитацию лидеров противника, разжигание в стане противника конфликтов, особенно между молодёжью и старшим поколением, создание помех в работе правительства, подрыв системы снабжения, обесценивание системы ценностей противника» [80].

Переход информационно-психологических войн на новый этап развития произошел, как нам представляется, в начале XX века и был связан с появлением новых технологических возможностей оказания психологического влияния на противника; многие из этих возможностей были опробованы в ходе Первой мировой войны.

Действительно, понятие «психологическая война» впервые использовал британский историк Дж. Фуллер в 1920 году при анализе психологических аспектов Первой мировой войны. Во время Второй мировой войны психологическая война «использовалась в качестве вспомогательного оружия современной войны и полезной составной частью реализации стратегии», своего рода элемент ведения традиционной войны «нелетальными средствами» [81] . После окончания Второй мировой войны информационно-психологическая война «превратилась в инструмент упреждения, подготовки условий для традиционной войны» [82].

В современном мире распространились именно информационно-психологические войны, т.е. психологические войны, в которых активно задействуется инструментарий современных информационных технологий. По замечанию А.В. Кириченко, «использование современных достижений в области информационных технологий средств массовой коммуникации, в разработке современных манипулятивных технологий превратило

[80]Сунь Цзы. Искусство войны. М.: АСТ. 2023. 195 с.
[81] Лайнбарджер П. Психологическая война. – М., Воениздат, 1962. С. 335.
[82] Кириченко А. В. Информационно-психологические войны: современные тенденции и технологические возможности //Акмеология. – 2015. – №. 4 (56). – С. 209-214.

информационно-психологические войны в инструмент формирования нового миропорядка».

Перечислим лишь некоторые из таких инструментов, которые можно выявить из анализа ключевых научных работ по данной тематике:

- использование «фейков», в том числе «фейковых» новостей;
- использование технологий искусственного интеллекта для создания заведомо ложных визуальных изображений с целью дискредитации противника;
- использование комментаторов-«троллей» для массового комментирования сообщений и/или постов в социальных сетях, посвященных тем или иным событиям (явлениям), в определенном ключе, целью которого является создание определенного отношения к описываемым событиям (явлениям) у остальных читателей и комментаторов;
- «демонизация» лидеров страны-противника и ключевых лиц, принимающих решения;
- фальсификация истории;
- тщательные чистки информационного пространства от информационных ресурсов и контента противника с одновременным активным распространением собственных;
- технологии «управляемого хаоса».

Объектом применения всех этих инструментов является общественное сознание и мировоззрение населения противоборствующей стороны, стратегической целью – разрушение ее культуры как основы ценностных установок населения [83] . Для достижения этой стратегической цели использование данного инструментария имеет вполне определенные тактические задачи, заключающиеся в обострении внутренних (национальных, религиозных, этнических и т.д.) противоречий между

[83] Крылова И. А. Информационно-психологические войны как фактор дезинтеграционных процессов в современном мире //Большая Евразия: развитие, безопасность, сотрудничество. – 2021. – №. 4-1. – С. 106-110.

отдельными группами в составе населения противоборствующей стороны, «стравливании» этих групп между собой. Для этого применяются, в том числе, и многочисленные инструменты «мягкой силы», разрушительное действие которой в раздробленном, разрозненном обществе, раздираемом внутренними противоречиями, оказывается намного сильнее и эффективнее, нежели в обществе сплоченном[84].

Информационные технологии играют ключевую роль в применении таких инструментов не только потому, что позволяют генерировать и распространять «фейки» – эти технологии восходят еще к пропагандистским листовкам начала века. Ключевое отличие современных технологий в том, что они позволяют собирать персональные данные и колоссальный массив данных о предпочтениях отдельных индивидов в составе населения противника, что чрезвычайно важно для эффективного «таргетирования» всех перечисленных выше инструментов. Как совершенно корректно отмечает Р.С. Выходец, ключевым принципом когнитивной войны «выступает так называемый «взлом личности», суть которого состоит в использовании современных информационных и когнитивных технологий для глубокого понимания человеческой психики, особенностей восприятия информации и достаточно точного прогнозирования поведения человека, что открывает широкие возможности для манипуляции сознанием, действиями людей в беспрецедентных и сложных масштабах»[85].

Здесь необходимо ввести в исследование понятие «когнитивной войны». Его, к примеру, использует Н.Г. Миронова, анализируя вопросы обеспечения безопасности в условиях информационного противоборства. Основным объектом воздействия в такой войне, по Мироновой, является «культурное и ментальное «пространство» противника: индивидуальное, групповое и коллективное сознание; системы образования и воспитания; коммуникативная практика; социальные ценности; мировоззренческие,

[84] Бартош, А. А. (2019). Стратегическая культура как инструмент «мягкой силы» российской дипломатии. *Вестник Московского университета. Серия 12. Политические науки*, (4), 19-31.
[85] Выходец Р.С. (2022) «Информационные доминанты» как инструмент информационно-психологических войн // Общественные науки и современность. № 4. С. 93–104.

научные, конфессиональные представления, поддерживающие целостность социальных структур»[86].

Отсутствие четкого определения когнитивных войн ставит вопрос о том, как они соотносятся с информационными войнами. Так, Е.О. Емалетдинов и Г.Д. Дубровский утверждают, что когнитивные войны включают информационный, психологический и когнитивный компоненты[87]. С этим определением контрастирует определение Л.В. Коцюбинской, рассматривающей понятие информационной войны с точки зрения лингвистики и определяющей ее как «информационные воздействия на общественное (массовое) сознание с целью внесения изменений в когнитивную структуру»[88].

Сходное определение дает англо-американский коллектив ученых, опубликовавших в журнале НАТО Ревью свою работу: «В когнитивной войне полем боя становится человеческий разум. Цель состоит в том, чтобы изменить не только то, что люди думают, но и то, как они думают и действуют. При успешном ведении она формирует и влияет на индивидуальные и групповые убеждения и поведение в пользу тактических или стратегических целей агрессора». [89] Эта работа посвящена якобы способам возможного использования цифровых технологий в когнитивной войне противниками альянса, однако представляется, что в первую очередь развитие этих технологий представляет интерес для самих стран альянса, в первую очередь, США.

А.П. Алексеев и И.Ю. Алексеева, рассматривая понятие когнитивной войны с позиций философской научной дисциплины, используют данное

---

[86] Миронова Н.Г. (2021) О проблеме обеспечения когнитивной безопасности. On the Problem of Ensuring Cognitive Security // Экономика и управление: научно-практический журнал. № 1. С. 119– 125.

[87] Емалетдинов, Е.О. and Дубровский, Г.Д., 2023. Когнитивная война: сущность, понятие, особенности. *Культура и природа политической власти: теория и практика.* Екатеринбург, *2023.* С. 236-241.

[88] Коцюбинская Л.В. Понятие «Информационная война» в современной лингвистике: новые подходы // Политическая лингвистика. 2015. №4. URL: https://cyberleninka.ru/article/n/ponyatie-informatsionnaya-voyna-v-sovremennoy-lingvistike-novye-podhody (дата обращения: 19.10.2024).

[89] John Hopkins University & Imperial College London. Countering Cognitive Warfare: Awareness and Resilience [Электронный ресурс] : NATO Review. 2021. May 20. URL: https://www.nato.int/docu/review/articles/2021/05/20/ countering-cognitive-warfare-awareness-and-resilience/index.html (дата обращения: 19.10.2024).

понятие в качестве полностью тождественного понятию «информационно-психологические войны» [90] . Этим обусловлена целесообразность рассмотрения данного явления в рамках настоящего параграфа. Для обозначения когнитивных войн, ведущихся в информационном поле с применением информационных технологий мы будем пользоваться термином «алгоритмические» когнитивные войны.

Алгоритмическая когнитивная война представляет собой совмещение алгоритмической войны и когнитивной войны. Когнитивная война рассматривается как военные операции, проникающие глубоко в сознание человека с целью изменения его восприятия. Этот подход не является новым и существует практически столь же давно, как и человеческие конфликты. В последнее время когнитивная война стала актуальной темой в военной сфере, наравне с такими аспектами как психологическая война, информационная война, война общественного мнения и кибервойна, которые взаимосвязаны, переплетаются и взаимодополняют друг друга, создавая сложное поле военных действий. Однако у каждого из этих аспектов свои особенности и направленность. Например, информационная война, кибервойна и когнитивная война сосредотачиваются на достижении преимущества в информационных, кибернетических и когнитивных сферах соответственно.

Когнитивная война имеет длительную историю достижения стратегических целей через воздействие и вмешательство в мыслительные процессы и познание, но её истинная мощь проявляется, когда она основывается на глобальных данных пользователей интернета, совмещается с широкомасштабным использованием искусственных интеллектов, а также реализуется через глобальное, целенаправленное и точное распространение информации от человека к человеку. Ключевым аспектом алгоритмической когнитивной войны является распространение контента, основанного на детализированных профилях пользователей, подкрепленное мощными разведывательными средствами, совместно с сотрудничеством и влиянием

[90] Алексеев А.П., Алексеева И.Ю. Цифровизация и когнитивные войны // Философия и общество. 2021. №4 (101). С. 39-51.

основных СМИ, а также с использованием обратной связи, взаимодействия, итерации и эскалации в условиях быстро меняющихся конфликтов и войн с целью формирования глобальной, непрерывной и высокоинтенсивной когнитивной деятельности, подавления разнообразных точек зрения и убеждений, формирования общественного мнения в стране и оказания воздействия на страны. Это особенно актуально в отношении решений и действий, которые оказывают непосредственное воздействие на ход конфликта и войны, такие как санкции и военная поддержка. По сравнению с традиционными методами ведения военных действий, алгоритмическая когнитивная война характеризуется глобальными политизированными нарративами, гибридными агрессивными действиями, когнитивным «замутнением» через технологии, а также стратегическим управлением и направлением (или, наоборот, недостаточным направлением) международных коммуникаций.

Подавляющее и контрподавляющее воздействие алгоритмической когнитивной войны осуществляется путем создания различных ложных событий и тактик, основанных на политических маневрах, в социальных сетях. По сравнению с традиционной когнитивной войной и другими формами конфликта, алгоритмическая когнитивная война обладает следующими характерными особенностями:

Она скрытая (латентная) и непрямая: алгоритмическая когнитивная война нарушает правила и границы «традиционной» войны, действуя в «серой зоне» (т.е. вне непосредственно и жестко контролируемого военными, полицейскими, политическими или правовыми институтами и механизмами пространства).

Алгоритмическая когнитивная война характеризуется тонкой, эффективной, массовой и иерархической природой, а также отличается высокой частотой, плотностью и постоянством использования различных инструментов, что создает высокую интенсивность когнитивного воздействия. Основой этой войны является изменение механизма

распространения социальной информации. Для более глубокого понимания и оценки алгоритмической когнитивной войны нам необходимо не только рассматривать технологические аспекты ее применения, но также изучать механизмы распространения социальной информации. Это включает в себя анализ внутренних законов и логики распространения информации, чтобы полноценно понимать процессы ее возникновения, развития и функционирования.

Алгоритмическая когнитивная война, основанная на ключевых дисциплинах, таких как искусственный интеллект, психология и кибернетика, все еще полагается на аппаратно-технические оперативные механизмы, обеспечивающие реальную поддержку. Эти механизмы можно условно разделить на следующие уровни:

1. Базовый уровень: этот уровень включает в себя арифметическую мощность, алгоритмы и доступ к данным. Это является ключевой способностью алгоритмической когнитивной войны, и она представляет собой сложнейшую техническую основу. Мощные вычислительные ресурсы, современные алгоритмы и доступ к большим объемам данных являются неотъемлемыми элементами для достижения преимущества в этой войне. Поэтому необходимо вложить значительные усилия в инфраструктуру для обеспечения таких ресурсов.

2. Создание и производство контента: ключевым аспектом функционирования алгоритмической когнитивной войны является способность создавать контент с использованием стратегического подхода. Это включает в себя производство контента сверху вниз и организацию контента внутри социальных платформ. Кроме того, контент может улучшаться с учетом глубокого понимания пользователей, а также использованием передовых технологических инструментов и алгоритмов.

3. Глобальные коммуникационные платформы: эти платформы представляют собой основу для алгоритмической когнитивной войны. Они предоставляют инструменты для анализа контента и пользователей.

Сотрудничество с большими данными и платформами контроля является необходимым для достижения успеха в этой войне. Ключевой момент заключается в блокировании нежелательной информации и усилении желаемой, чтобы создать асимметричное коммуникационное преимущество.

4. Традиционные СМИ: традиционные СМИ играют важную каталитическую роль в определении повестки дня и формировании общественного мнения. Их репортажи и позиции могут влиять на процессы алгоритмической когнитивной войны.

5. Массовые пользователи: они являются объектом воздействия, но также важным звеном в этой войне.

Изменение парадигмы распространения информации в последние десятилетия стало значительным фактором в эволюции алгоритмической когнитивной войны. Раньше доминировала парадигма массовой коммуникации "сверху вниз", но с развитием массовой социальной коммуникации, основанной на социальных сетях и управляемой пользователями интернета, стали возможным изменения в распространении информации, что стало ключевой особенностью алгоритмической когнитивной войны.

С развитием интеллектуальных технологий и ростом управляемой крупномасштабными динамическими данными в реальном времени интеллектуальная коммуникационная парадигма распространения информации становится все более доминирующей в обществе. Каждый механизм коммуникации появляется с целью увеличить возможности и скорость распространения информации, что становится разрушительным для старых парадигм. Таким образом, выбор механизма коммуникации становится важным вопросом "старого и нового", который определяет способ реагирования на изменения.

Смешивание разных механизмов коммуникации создает оптимальные условия для проведения алгоритмической когнитивной войны. Путем сочетания потока массовой информации в реальном времени с

систематически курируемым контентом становится сложнее обнаружить и отследить воздействие этой войны. Кроме того, алгоритмическая когнитивная война успешно стимулирует спонтанные итерации пользовательской коммуникации, что усиливает ее воздействие.

Использование алгоритмов искусственного интеллекта играет решающую роль в создании когнитивного преимущества, которое в конечном итоге преобразуется в преимущество в принятии решений и дает инициативу. Технологии глубокой подделки, фальшивых новостей, распознавания лиц и искусственного интеллекта все включены в инструментарий алгоритмической когнитивной войны. Однако важно отметить, что "умное" общение находится на начальном этапе развития, и социальные сети по-прежнему доминируют в большинстве стран. Интеллектуальные коммуникационные приложения объединяют особенности социальных сетей и алгоритмической когнитивной войны, что делает их значимыми актерами.

Алгоритмическая когнитивная война, хотя и остается незаметной, является полем битвы, на котором отсутствует «дым», но полностью зависит от мощных современных цифровых технологий. Ключом к успешной победе в алгоритмической когнитивной войне является наличие интеллекта, который обеспечивает когнитивное преимущество и подавляет мышление противника. Инфраструктура алгоритмической когнитивной войны включает в себя мощные вычислительные ресурсы, передовые алгоритмы и огромные объемы данных. Глобальное население интернета и глобальные сетевые платформы, которые лежат в основе алгоритмической когнитивной войны, позволяют создавать глобальную систему мгновенной коммуникации. В сочетании с широкомасштабным использованием искусственного интеллекта постепенно формируется глобальная интеллектуальная коммуникация, основанная на данных и алгоритмах.

С распространением смарт-технологий становится все более очевидной будущая тенденция: смарт-коммуникации продолжат доминировать как

основной механизм распространения глобальной информации. Эти коммуникации будут более быстрыми, широко распространенными, целенаправленными и мощными. В то же время, стратегические позиции алгоритмической когнитивной войны будут укрепляться еще больше. Страны будут продолжать увеличивать инвестиции в исследования и разработки технологий, создавая соответствующие возможности, включая глубокие технические преимущества в инфраструктуре, глобальный контроль над большими данными (универсальными, территориальными и голографическими ресурсами данных), систематическое сотрудничество на различных уровнях, включая сотрудничество между государственным и частным секторами, альянсами и другими формами сотрудничества. Кроме того, развиваются возможности применения искусственного интеллекта, включая анализ и использование данных, а также возможности глобальной мобилизации, особенно в контексте алгоритмической когнитивной войны.

Оптимизация социогуманитарных технологий в современной информационной войне должна включать несколько основных направлений.

Первое направление - развитие критического мышления у населения. Необходимо акцентировать внимание на образовании и совершенствовании критического мышления, то есть способности анализировать информацию, выделять достоверные источники и определять подлинность информации. Это поможет людям защитить себя от негативного воздействия пропагандистской информации, распространяемой различными сторонами конфликта.

Также критическое мышление позволит людям осмысленно и адекватно реагировать на различные ситуации и конфликты, не поддаваться манипуляциям, принимать взвешенные решения и действовать в интересах себя и общества.

Для развития критического мышления в населении необходимо сформировать в обществе культуру критического мышления и проводить специальные образовательные программы и проекты. В школьной программе

следует уделить большее внимание развитию критического мышления и создать условия для выработки у школьников навыков анализа информации и поиска достоверных источников.

Также взрослому населению необходимо предоставить обучающие курсы и тренинги, которые помогут развить критическое мышление и научат нескольким ключевым навыкам:

1. Анализировать информацию из разных источников и определять общую линию событий.

2. Использовать проверенные источники для подтверждения информации и информироваться о неизвестных изданиях и медийных источниках.

3. Определять цели, которые преследуются в распространении каких-либо мнений или событий.

Создание условий для развития критического мышления в обществе является важным шагом к повышению защиты информации от влияния различных угроз, включая информационные провокации.

Выводы по главе 1

В современном мире информация является одним из наиболее ценных ресурсов. Информационные технологии позволяют передавать, обрабатывать и хранить информацию в больших объемах и на невиданной ранее скорости. Однако это развитие информационных технологий также стало идеальной платформой для черных операций, связанных с информацией.

Информационные войны представляют собой одну из форм таких операций. Их сущность заключается в использовании информационных технологий для манипулирования общественным сознанием, распространения дезинформации и формирования негативного образа определенных стран, корпораций или личностей. Целью информационных войн является получение власти, контроля над рынками или доступа к определенным ресурсам.

Основными инструментами проведения информационных войн являются социальные сети, информационные порталы, новостные сайты, блоги и форумы. Огромное количество информации, распространяемой через эти каналы, позволяет создавать бесчисленное количество "подставных" новостей, комментариев и обзоров. Источники такой информации могут быть разнообразными, включая деятелей сторонних государств, хакерские группы и лиц, заинтересованных в нанесении ущерба определенным организациям.

Информационные войны имеют конкретные жертвы – общественное мнение и государственные учреждения. Цели проведения информационных войн часто связаны с созданием негативного образа определенной страны или предоставлением искаженной информации о значимых событиях. Информационные войны подрывают доверие к системам правосудия, формируют искаженное представление о событиях и могут иметь реальные последствия.

Информационные войны могут принимать разнообразные формы и проводиться на разных уровнях. Они могут включать в себя манипуляции данными, программное воздействие, атаки на сетевую инфраструктуру и социальную инженерию. Для борьбы с информационными войнами требуется сложные технические решения и организационные меры. Законы, регулирующие информационные технологии, а также системы обеспечения информационной безопасности играют важную роль в этом процессе. Участники информационных войн должны проявлять надежность и работать как единое целое, чтобы эффективно противостоять этому явлению.

Становление во второй половине XX века информационного, а в XXI веке – цифрового общества, что является ключевой глобальной трансформацией современности, цифровизация промышленности и управления, а также научные достижения в области психологии и социологии создали условия для появления как новых объектов для информационных атак (цифровая инфраструктура экономики и, особенно, промышленности, финансов, госуправления, социальные сети, базы личных

данных и т.д.), так и для технологизации информационно-психологического воздействия вплоть для использования технологий искусственного интеллекта для пропаганды или создания ложных нарративов. При этом круг объектов направленности информационно-психологических войн практически не со времен Второй мировой войны и даже с более раннего периода активизации противостояния России с коллективным Западом в XIX веке. В то же время с усилением значимости экологической составляющей жизни человечества, новыми трендами декарбонизации и экологизация появилась новая сфера информационного воздействия – осознание природно-экологической защищенности и комфорта населения противоборствующих и конкурирующих стран.

ГЛАВА 2. КИТАЙ, РОССИЯ И США В ИНФОРМАЦИОННЫХ ВОЙНАХ СОВРЕМЕННОСТИ

.

2.1. Стратегии США в информационных войнах

В начале 1980-х годов публикация книги американского социального прогнозиста Элвина Тоффлера «Третья волна» [91] вызвала значительное внимание представителей различных властных структур США, в том числе Вооруженных сил, и некоторые начали изучать вопросы войны в информационную эпоху. В ноябре 1990 года была опубликована книга Тоффлера «Метаморфозы власти» [92] , где одна из глав посвящена информационной войне, но, главным образом, с точки зрения маркетинга. В то же время в Вооруженных силах США началась волна изменений в области информационной войны. В этот период началась война в Персидском заливе в 1991 году, которую назвали первой информационной войной человечества.

Информационная война в понимании именно противостояния в киберпространстве была впервые упомянута в директиве Министерства обороны США, выпущенной в 1992 году. Сам же термин был впервые использован в отчете, подготовленном в 1976 году по заказу Департамента обороны США [93] . В 1996 году эксперты американского аналитического центра RAND Corporation [94] выпустили доклад «Стратегическая информационная война: новое лицо войны».

В 2000 году в докладе Института национальных стратегических исследований Национального университета обороны под названием «Совместное видение 2020. Американские военные – готовясь к завтрашнему

---

[91] Тоффлер Э. Третья волна. – М.: АСТ, 2010. – 784 с.

[92] Тоффлер Э. Метаморфозы власти. – М.: АСТ, 2004. – 672 с.

[93] Барабаш, В. В., Котеленец, Е. А., & Лаврентьева, М. Ю. (2019). Информационная война: к генезису термина. *Знак: проблемное поле медиаобразования*, (3 (33)), 76-89.

[94] Корпорация RAND «тесно связана с правительством США и военными структурами этой страны. RAND имеет большой опыт в области разработки стратегий сдерживания и уничтожения государств, которые рассматриваются как угрожающие США или неугодные по каким-либо иным причинам». Алексеев А.П., Алексеева И.Ю. Цифровизация и когнитивные войны // Философия и общество. 2021. №4 (101). С. 39-51.

дню» развитие информационных технологий было упомянуто в качестве одного из главных факторов, которые, как предполагалось, внесут наиболее масштабные изменения в проведение военных операций[95]. В настоящее время термин «информационная война» официально закреплен в боевом уставе Армии США «Психологические операции»[96].

Говорить об использовании Соединенными Штатами технологий информационной войны можно как минимум с начала 1990-х, хотя, как было показано нами ранее, использование таких технологий в их самых простых вариантах далеко предшествовало появлению самого термина «информационные войны».

Так, И.А. Крылова приводит в качестве ранних примеров информационной войны, развязанной США против СССР, следующие документы «Закон № 402, 1948 г., который заставлял СМИ оказывать планомерное и систематическое воздействие на общественное мнение других народов; … Директива № 68, 15 апреля 1950 г. ставила задачу «обеспечить коренное изменение природы советской системы, посеять внутри этой системы семена ее разрушения, поощрять и поддерживать беспорядки и мятежи в избранных, стратегически важно расположенных странах-соседях СССР» и отмечает, что «началом нынешнего витка информационной войны против России, по мнению А. Фурсова, можно считать 1953 г., когда был создан американский проект «Радио Свобода», который служил для поддержки «инакомыслия» в России. Поэтому именно американцы первыми начали информационную войну против СССР»[97].

О.Г. Карпович отмечает, что истоки современной ситуации, в рамках которой существует возможность для США «безнаказанно проводить информационно-психологические операции в различных странах и зонах

---

[95] Joint Vision 2020. America's Military – Preparing for Tomorrow / National Defense University, Institute for National Strategic Studies. Washington, D.C., 2000. P. 59.

[96] Манойло А. В. Технологии современных информационных войн // Политическая наука. 2017. № Спецвыпуск. С. 306–325. Манойло, А. В. (2016). Информационная война как угроза российской нации. *Вестник российской нации*, (6), 174-184.

[97] Крылова И. А. (2016). Информационные войны и безопасность России. *Россия: тенденции и перспективы развития*, (11-2), 116-121.

международных конфликтов и вмешиваться во внутренние дела других государств» восходят к 1980-м годам, когда «американским военным удалось успешно синтезировать методы психологической и информационной войны, что привело к созданию концептуальной модели информационных войн» [98] на фоне распространения предшественника Интернета – сети ARPANET. Во многом эти методы и технологии были отработаны в ходе тенденциозного освещения в СМИ «работы армейских органов информационно-психологических операций во время операции «Буря в пустыне» в 1991 году»[99].

В январе 1995 года глава Департамента обороны США сформировал Исполнительный совет по информационным войнам для содействия «разработке и достижению целей национальной информационной войны».

Были определены семь ключевых особенностей стратегической информационной войны:

1) «ценовая доступность» – разработка и использование приемов информационной войны зачастую обходятся намного дешевле, чем создание новых видов «традиционных» вооружений;

2) размывание границ – технологии информационной войны не привязаны к месту и времени какого-либо конкретного вооруженного конфликта, но могут быть в любой момент использованы против любого государства и/или негосударственного актора;

3) манипулятивность, осложняющая формирование поддержки населением какого-либо государственного решения или инициативы;

4) снижение эффективности классических методов сбора и анализа разведданных;

5) неспособность традиционных систем тактического предупреждения вовремя выявлять использование приемов и технологий информационной войны;

---

[98] Карпович О.Г. Практика проведения США операций информационной войны в сфере внешней политики // Национальная безопасность / nota bene. 2017. № 1. С. 112-126.
[99] Там же.

6) сложность поиска партнёров и создания коалиций;

7) уязвимость территории США.

Представляется, что именно последний, седьмой аргумент в значительной степени обусловил интерес США к технологиям информационных войн – а также служил своего рода «прикрытием», обоснованием необходимости разработки средств ведения информационных войн Соединенными Штатами для широкой публики – отнюдь не единственный раз некая «угроза США» использовалась этим государством для вторжения во внутренние дела других стран.

В документе Исполнительного совета по информационным войнам Департамента обороны США это положение раскрывалось следующим образом: «основанные на информации методы делают географическое расстояние несущественным; цели в континентальной части Соединенных Штатов столь же уязвимым, как и цели на театре военных действий. Учитывая возросшую зависимость экономики и общества США от высокопроизводительной сетевой информационной инфраструктуры, потенциальным противникам, вооруженным средствами ведения информационных войн, представляется новый набор прибыльных стратегических целей»[100].

В материале начала 2000-х годов, опубликованном RAND Corporation в виде научной монографии уже в открытую рассматривались техники и способы ведения наступательной информационной войны, якобы для повышения шансов США на успешную борьбу с новыми вызовами. Однако при этом в документе в открытую утверждалось, к примеру, что «основная цель информационного сдерживания — успешно манипулировать отношением потенциального противника в мирное время или во время кризиса, чтобы не дать ему когда-либо напасть на союзника» [101], что должно стать значительно проще с применением информационных технологий.

---

[100] Molander R.C., Riddile A., Wilson P.A. Strategic Information Warfare: A new face of war. RAND Corporation, 1996.

[101] Nichiporuk, B. (2002). US Military opportunities: Information-warfare concepts of operation. In: Z. Khalilzad &

В частности, информационное сдерживание, по мнению экспертов RAND, можно осуществить «тремя способами: **настроить международное мнение против** агрессора, изменить его восприятие военного соотношения сил на театре военных действий и **способствовать нестабильности** в его стране. Информационное сдерживание не требует чистой стратегии; оно может включать комбинацию из двух или трех вариантов, в зависимости от обстоятельств» [102] . Раскрывая тезис о манипулировании международным мнением, авторы аналитического материала отмечают, что «основная сила США заключается в их способности создавать широкие коалиции против потенциальных врагов, которые могут изолировать противников от внешней поддержки, как материальной, так и моральной»[103].

Этот сценарий полностью соответствовал тому, что происходило во время войны США с Ираком в начале XXI века – вернее, тому, что было запланировано американцами. Была разработана особая концепция ведения информационной войны против Ирака, получившая название «Шок и трепет», которой отводилась ключевая роль в поражении морального духа иракцев. Война должна была, по выражению В.В. Бедрань, уподобиться спектаклю, в котором противник должен был быть лишен всех средств коммуникации и сохранить доступ лишь к той информации (в большинстве случаев не соответствующей реальности, а зачастую и откровенно лживой), которую предоставляли американцы. Однако арабские СМИ и новостные агентства сумели стать альтернативными источниками информации, успешно развенчивавшими «мифотворчество» американцев[104].

По сути, речь здесь идет о таком инструменте США, как санкционная политика, которая не единожды применялась ими против различных стран на протяжении последних десятилетий, а также о манипулировании мнением и, порой, о прямом давлении на союзников (в этой роли, как правило,

---

J. Shapiro (eds). *Strategic appraisal: United States air and space power in the 21st century*. Rand Corporation, 2002. Pp. 187-219.

[102] Там же.

[103] Там же.

[104] Бедрань В. В. (2012). Механизмы информационной войны США против Ирака в начале XXI в. *Вестник РГГУ. Серия: Политология. История. Международные отношения*, (7 (87)), 186-195.

выступают другие государства коллективного Запада) с тем, чтобы добиться их поддержки и соблюдения ими вводимых США санкций против того или иного государства.

В документе напрямую отмечается, что «такие коалиции усиливают боевую мощь США, сокращают доступ противника к критически важным поставкам и обеспечивают большую легитимность действий США — легитимность, которая укрепляет внутреннюю поддержку США действий по сдерживанию и войны, если это станет необходимым. … Создание и поддержание таких коалиций требует, чтобы международное мнение рассматривало противников США как агрессоров, мало уважающих международное право или права человека. Оптимально, чтобы такая коалиция поддерживалась непрерывной и длительной информационной кампанией»[105].

В документе предлагался алгоритм конкретных действий по развертыванию информационной кампании перед началом военных действий – такая кампания должна была показывать намерения противника атаковать США и демонстрировать «дружественные намерения» самих Соединенных Штатов. Отмечается, что этот алгоритм применялся Соединенными Штатами как минимум начиная с Карибского кризиса, однако в настоящее время может быть дополнен различными технологическими новшествами, которые сделают установление наблюдения над противником более эффективным и менее опасным для вооруженных сил США.

В свете активного применения Штатами санкционной политики против «неугодных» государств, а также фабрикования доказательств к различным заявлениям (такого качества, что даже эксперты не могли быть уверены в подлинности или сфабрикованности того или иного изображения [106]), достаточно циничным выглядит заявление о том, что «нет смысла рисковать репутацией Америки как честного гражданина мира, фабрикуя

[105] Там же.

[106] Алексеев, А. П., & Алексеева, И. Ю. (2016). Информационная война в информационном обществе. *Вопросы философии*, (11). *Бедрицкий А.В.* Информационная война: концепции и их реализация в США. М.: РИСИ, 2008. С. 111.

видеоизображения» [107] , когда есть столько независимых СМИ – что полностью подтверждает тезис А.В. Манойло о роли «независимых» журналистов и их столь же «независимых расследований» в информационных войнах [108] . При этом якобы использование Россией «обширной экосистемы российских прокси-сайтов, отдельных лиц и организаций, которые кажутся независимыми источниками новостей» служит достаточным, по мнению Департамента обороны, основанием для того, чтобы навесить на Россию ярлык страны, стремящейся «посеять раздор внутри Соединенных Штатов и повлиять на избирателей и принятие решений в США»[109].

При этом в том же разделе материала эксперта RAND Б. Ничипорука, посвященном информационному сдерживанию, в открытую постулируется, что для США «наступательная информационная война предлагает много новых скрытых средств для использования напряженности, поскольку она увеличивает возможность прямого общения с составными частями общества противника. Поскольку информационная революция увеличивает количество и типы каналов связи в любом обществе, возможности введения ложных данных в коммуникационные связи между составными частями общества также увеличиваются»[110].

В том же документе в качестве метода информационного сдерживания было предложено поддержание нестабильности во внутренних делах «агрессора», в особенности принадлежащего к «недемократическим» странам. Важно подчеркнуть, что периодическое использование Соединенными Штатами наступательных методов информационной войны в мирное время (т.е. в отсутствие объявления войны) полностью

---

[107] Там же. С. 204.

[108] Манойло, А. В. (2016). Информационная война как угроза российской нации. *Вестник российской нации*, (6), 174-184.

[109] U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2023. P. 1. URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-Department-Of-Defense-Strategy-For-Operations-In-The-Information-Environment.PDF (дата обращения: 1.04.2025)

[110] Nichiporuk, B. (2002). US Military opportunities: Information-warfare concepts of operation. In: Z. Khalilzad & J. Shapiro (eds). Strategic appraisal: United States air and space power in the 21st century. Rand Corporation, 2002. Pp. 187-219. P. 205.

оправдывается в документе через использование концепции «стратегической досягаемости»[111].При этом Департамент обороны США в своей Стратегии операцией в информационной среде (издана в 2023 году) не только сохраняет, но и наращивает свою агрессивную риторику относительно «бросившей вызов» КНР и «крайне агрессивной» России, в то время как Иран и Северная Корея названы в одном ряду с воинствующими экстремистскими организациями [112] . Одновременно в этом документе отмечается, что «интеграция информационной мощи в стратегию, стратегическое искусство, оперативное искусство, оперативный дизайн и оперативное планирование с самого начала планирования обеспечивает … информационное преимущество» и потому должна стать одним из важнейших принципов политики США в этой сфере»[113].

Следует уделить внимание и предшествовавшей Стратегии операций в информационной среде, вышедшей в 2016 году. В том документе в качестве желаемого конечного результата реализации соответствующей политики была обозначена такая ситуация, в которой «благодаря операциям, действиям и мероприятиям в информационной среде, Департамент обороны имеет возможность влиять на принятие решений и поведение противников и других назначенных лиц, чтобы получить преимущество в диапазоне военных операций»[114]. При этом особо отмечалось, что «сегодняшние противники и другие субъекты все чаще нацеливаются на невоенную аудиторию с

[111] Nichiporuk, B. (2002). US Military opportunities: Information-warfare concepts of operation. In: Z. Khalilzad & J. Shapiro (eds). *Strategic appraisal: United States air and space power in the 21st century*. Rand Corporation, 2002. Pp. 187-219. P. 205-207.

[112] U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2023. P. 1. URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF (дата обращения: 1.04.2025)

[113] U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2023. URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF (дата обращения: 1.04.2025)

[114] U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2016. URL: https://dod.defense.gov/portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf (дата обращения: 1.04.2025)

помощью мощной, символической, стратегической коммуникации … оказывая глубокое влияние»[115].

Хотя правдивость данного заявления ничем не доказана, оно основано на важной черте современных информационных войн – на основе глобально интегрированного киберпространства происходит глобальная мобилизация и воздействие, и никто больше не может оставаться вне этого процесса. Постоянные изменения и всеобъемлющие конфликты стали структурными особенностями современной среды безопасности, и будущие конфликты больше не ограничены географическими рамками. Использование преимуществ глобальной природы киберпространства, выходящего за пределы национальных границ, оказывает разрушительное воздействие на традиционную концепцию военных операций в пространстве и времени.

В будущем информационная война представит серьезную угрозу не только военным, но и гражданским объектам. Вооруженные конфликты будут вестись с использованием компьютерных технологий, способных вывести из строя системы управления воздушным движением, связи и финансовые системы противника, что может привести к серьезным нарушениям в повседневной жизни гражданского населения. Несмотря на то, что информационная война может избегать кровопролития и физических жертв благодаря использованию новейших технологий, она все равно способна нанести массированный и комплексный удар, вызывая широкомасштабную панику среди населения противника и добиваясь эффекта победы без прямых военных столкновений.

Таким образом, информационная война становится столь же угрожающей, как и любая другая форма военных действий. В последние годы США используют весь инструментарий информационных войн, чтобы подавить мощь Китая и выставить его в роли агрессора, обвиняя его в промышленном шпионаже и кибератаках, вводя протекционистские меры

[115] U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2016. URL: https://dod.defense.gov/portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

для ИТ-отрасли под видом защиты информационной безопасности, развязывая на фоне информационной войны полноценную торговую войну – и одновременно наращивая свое военное присутствие в Азиатско-Тихоокеанском регионе[116].

США также ведут информационную войну против России на самых разных фронтах – от передела европейского газового рынка[117] до борьбы российских войск с террористическими формированиями в Сирии[118]. А.В. Манойло убедительно показывает, что США, упустив возможность прямого военного вмешательства в ситуацию в Крыму в 2014 году, когда тот добровольно стал российским, обратились к единственному остававшемуся доступным инструменту агрессивного ответа – к информационным операциям[119].

Значительное внимание уделяется в США и такому смежному с информационными войнами явлению, как кибервойны. На основе всесторонних научных исследований можно определить кибервойны так: это действия субъектов международных отношений, которые причиняют ущерб другим субъектам международных отношений на материальном или когнитивном уровне через киберпространство или с использованием кибертехнологий, в рамках действий по достижению своих политических целей. При этом киберпространство является частью информационной среды. С развитием и расширением киберпространства оно становится важным компонентом процесса принятия решений. Понимание киберпространства и его взаимосвязи с информационной средой критично для тех, кто ведет тактическую информационную войну.

---

[116] Каткова, Е. Ю., & Юнюшкина, А. С. (2022). Китайские концепции и возможности в информационной войне: соперничество КНР и США в киберпространстве. *Вестник Российского университета дружбы народов. Серия: Всеобщая история*, *14*(2), 197-210.

[117] Гадзацев, К. В. (2020). Политическое давление и информационная война США против России на европейском газовом рынке: состояние и перспективы. *Информационные войны*, (1), 11-17.

[118] Мартыненко, Е. В. (2016). Характер информационной войны между Россией и США в Сирии. *Общество: политика, экономика, право*, (9), 9-12.

[119] Манойло, А. В. (2021). Информационная война и новая политическая реальность (I). *Российский социально-гуманитарный журнал*, (1), 100-132.

Кибервойна, по нашему представлению, делится на два основных типа: кибертехническую войну и киберкогнитивную войну.

Кибертехническая война включает в себя вмешательство, манипуляции и разрушение целей, связанных с военно-политическими операциями, в реальном мире, но с использованием киберактивности. Сюда относятся атаки типа "распределенный отказ в обслуживании" (DDoS), атаки с использованием вредоносных кодов и другие действия, направленные на инфраструктуру и военные объекты. Можно сказать, что США ведут кибертехническую войну как минимум с 1989 года, после того как в 1988 году Интернет был заражен вредоносной программой-«червем»[120].

Напротив, киберкогнитивная война представляет собой кампанию, в ходе которой субъекты используют социальные медиа и иные средства массовой коммуникации для изменения самопредставления людей в целевой стране, разрушения их национальной идентичности и изменения образа мышления и поведения целевой аудитории с помощью ложной информации, «фейков» и др.

Из-за того, что определение информационных войн до сих пор не выработано, сложно точно определить границы этого явления и явления кибервойн, а также четко определить, в какой части они пересекаются, накладываются друг на друга. Однако несомненно то, что они тесно переплетаются, поскольку наступательные информационные войны, методы ведения которых активно использует США, ведутся в том числе и в киберпространстве, а сам наступательный подход тесно связан с концепцией «защиты на опережение», используемой в киберстратегии Департамента обороны США (впервые упоминается в Киберстратегии 2023 года, но по сути восходит еще к Киберстратегии 2018 года).

Действительно, «для достижения максимальной эффективности информационная война должна взаимодействовать с киберпространством и

[120] Spafford, Eugene H., "The Internet Worm Incident" (1989). Department of Computer Science Technical Reports. Paper 793. https://docs.lib.purdue.edu/cstech/793.

включать в себя … активное использование киберресурсов» [121]. Вполне осознавая это, руководство США еще в 2010 году учредило Единое боевое командование США в сфере киберпространства – USCYBERCOM. К непосредственным обязанностям этого командования относятся защита информационных систем Департамента обороны США, руководство операциями в киберпространстве и защита страны от кибератак.

Изначально USCYBERCOM являлся составной частью Стратегического командования США и был продолжением начавшейся еще в 1970-х годах работы военных и разведывательных служб США по защите информационных систем. Новый виток осознания необходимости структуры, сфокусированной на защите «интересов США» в киберпространстве, пришелся на 2004 год. В Национальной военной стратегии США от 2004 года киберпространство было объявлено «областью» конфликта наряду с воздушным, наземным, морским и космическим пространствами.

Еще во второй половине 1990-х годов предпринимались попытки создать оперативную группу, способную противодействовать удаленным атакам; это подразделение не единожды модифицировалось и переподчинялось. В 2004 году глава Департамента обороны Дональд Рамсфелд разделил это подразделение «на оборонительные и наступательные компоненты: Объединенная оперативная группа по глобальным сетевым операциям, отвечающая за оборону; и Объединенное функциональное компонентное командование по сетевой войне для планирования наступательных операций в киберпространстве»[122]. В 2010 году они вновь были объединены и стали Киберкомандованием США, из чего логически вытекает сочетание оборонных и наступательных функций у данного подразделения.

В 2014 – 2015 годах в структуру Киберкомандования добавились два компонента – Cyber National Mission Force, отвечающий за операции в

[121] U.S. Cyber Command. Our History / U.S. Cyber Command. URL: https://www.cybercom.mil/About/History/ (дата обращения 10.04.2025)
[122] U.S. Cyber Command. Our History / U.S. Cyber Command. URL: https://www.cybercom.mil/About/History/ (дата обращения 10.04.2025)

киберпространстве, и Joint Force Headquarters–DoD Information Network, защищающий информационные сети Департамента обороны. В 2016 году добавился еще один компонент, JTF–Ares, чьей ключевой миссией является борьба с террористическими угрозами. В 2018 году в структуре Киберкомандования была создана «малая группа по России», якобы для защиты промежуточных выборов в США, в 2020 году – «Группа безопасности выборов».

Эти организационные перестройки происходили в контексте концепции «Защита на опережение» Киберстратегии Департамента обороны США. В заявлении USCYBERCOM, сделанном в марте 2018 года, утверждается: «Защита на опережение как можно ближе к источнику активности противника расширяет наши возможности по выявлению слабых сторон противника, изучению его намерений и возможностей и отражению атак вблизи его источника. Постоянное взаимодействие создает тактические трения и стратегические издержки для наших противников, заставляя их переключать ресурсы на оборону и сокращать атаки. Мы будем преследовать злоумышленников по всем сетям и системам … одновременно получая большую свободу маневра для противодействия и борьбы с опасной деятельностью противника, прежде чем она нанесет ущерб нашей национальной мощи»[123].

По сути, концепция «защита на опережение» означает попытку США легитимизировать свое право на нападение на любую «неугодную» страну в любой момент, прикрываемое риторикой о «враждебном настрое» той или иной страны.

И США активно пользуются этой концепцией – по утверждению представителей собственно Департамента обороны США, «с 2018 года Департамент провел значительное количество операций в киберпространстве в рамках своей политики защиты на передовой, активно пресекая вредоносную киберактивность до того, как она сможет повлиять на

[123] U.S. Cyber Command. Our History / U.S. Cyber Command. URL: https://www.cybercom.mil/About/History/ (дата обращения 10.04.2025)

территорию США»[124]. При этом Департамент обвиняет КНР и Россию в использовании «вредоносной киберактивности», направленной на снижение боеспособности военных сил США, утверждая, что «продолжит обороняться», хотя в реальности его действия зачастую являются нападением, а не защитой.

Это позволяет рассматривать действия США не только как информационную войну, но и как кибервойну – в первую очередь, с КНР и Россией.

[124] U.S. Department of Defense. 2023 Cyber Strategy of the Department of Defense. Summary. Washington, D.C.: U.S. Department of Defense, 2023. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF (дата обращения:1.04.2025).

2.2. Становление и развитие подхода Китая к противостоянию и ведению информационных войн

Руководство КНР в полной мере осознает значимость ИКТ для всех сфер развития человечества, в том числе и в течении социально-политических конфликтов, и в ведении современных войн. Китайская концепция комплексного стратегического сдерживания все больше внимания уделяет таким технологиям наряду с космическими. Однако понимание Китаем информационных войн отличается от понимания таковых в западных странах – действительно, китайские эксперты считают, что суть информационной боеспособности государства и информационного воздействия на противника состоит в том, «чтобы сломить волю противников, их установки и убеждения, что повлияет на волю и моральный дух противников, чтобы они не смогли продолжать бороться»[125].

Согласно китайской концепции, информационная война имеет наступательный и оборонительный аспект. Оба аспекта важны для нормального функционирования государства и защиты его собственных интересов. Оба аспекта направлены в конечном итоге на снижения воздействия высокотехнологичных противников на развитие Китая и китайское общество.

«Мягкая сила» Китая

Наступательный аспект информационной войны связан не только с деятельностью армейских подразделений, сколько с проникновением в информационное поле противников (а также потенциальных союзников) и создание в нем образа Китая, отвечающего стратегическим целям страны, а также донесение до их населения не искаженной точки зрения КНР по тем или иным событиям на международной политической арене. Важным инструментом против манипуляции западных СМИ общественным

[125] Vuletić, D. V., & Stanojević, P. (2022). Concepts of information warfare (operations) of the United States of America, China and Russia // Review of International Affairs. *2022.* Vol. 73, No 1185. P. 51–70. P. 58.

сознанием западных стран относительно Китая стало развитие собственного китайского информационного агентства Синьхуа и постепенное развитие различных направлений его работы, в первую очередь, появление зарубежных филиалов. Например, это проявилось в период глобальной пандемии, когда западные СМИ стремились представить принятые Китаем меры по ограничению распространения вируса COVID-19 в «недемократическом» свете, напирая на якобы «ограничение прав человека», в то время как Синьхуа демонстрировало выступления китайского руководства (в том числе в сфере здравоохранения), неоднократно подчеркивавшего, что в основе принятых строгих мер и контроля над их соблюдением лежит забота о здоровье китайского населения.

Китай активно применяет разнообразные технологии и методы для воздействия на общественное мнение в других странах с целью недопущения очернения образа Китая, проводимого американскими СМИ, и донесения до глобальной аудитории не искаженной позиции Китая по тем или иным вопросам. Для этого Китай вкладывает значительные средства в мягкую силу, используя свое экономическое и культурное влияние для формирования глобальных нарративов и продвижения своих интересов. Это включает финансирование культурных обменов, предоставление развивающимся странам помощи в развитии и инвестирование в средства массовой информации и инфраструктуру в других странах.

В рамках усилий по созданию положительного образа Китая и противодействия его искажению западными СМИ, а также с целью популяризации китайской культуры и китайского языка, КНР активно развивает такой инструмент «мягкой силы», как Институты Конфуция. Это сеть некоммерческих образовательных учреждений, сформированная и активно расширяемая Китаем на базе образовательных учреждений как в странах коллективного Запада, так и в странах мирового большинства. По

состоянию на июнь 2024 года в 160 странах и регионах мира насчитывается 495 Институтов Конфуция и 763 Класса Конфуция[126].

Более 100 этих заведений функционировало в образовательных учреждениях США; однако в 2018 году Конгресс США начал компанию по ограничению федерального финансирования для школ, на базе которых работали институты и классы Конфуция, после чего практически все американские учебные заведения закрыли их. Согласно отчёту Национальной ассоциации учёных, опубликованному в июне 2022 года, из 118 институтов Конфуция в Соединённых Штатах 104 были либо закрыты, либо находились в процессе закрытия. Однако десятки закрытых Институтов Конфуция возродились в других формах: университеты внедрили аналогичные программы, поддерживают тесные связи с закрывшимися Институтами Конфуция, переносят Институты Конфуция в другие места или запускают новые программы сотрудничества с Китаем[127].

Информационная война США с Китаем

Что касается непосредственно информационных войн, на них распространяется китайская доктрина сдерживания. Киберпространство осознается китайским руководством как одна из сфер, в которых возможно возникновение угроз национальной безопасности КНР со стороны внешнеполитических сил, еще с начала 2000-х годов. Народно-освободительная армия Китая (НОАК) стремится к полному технологическому суверенитету для достижения доминирования в информационном пространстве, полагаясь на свои компьютерные сети и информационные системы и разрабатывая инструменты для подавления аналогичных ресурсов противника[128].

---

[126] Институты Конфуция. Уральский федеральный университет. URL:https://ci.urfu.ru/ru/about/ (дата обращения:1.04.2025).
[127] Peterson, R., Oxnevad I., Yan F. After Confucius Institutes// National Association of Scholars, 15 June 2022 URL: https://www.nas.org/reports/after-confucius-institutes/full-report (дата обращения: 1.04.2025).
[128] Cheng, D. Cyber dragon: Inside China's information warfare and cyber operations. Bloomsbury Publishing USA, 2016.

Вопреки распространенному представлению о том, что китайская армия предпочитает делать ставку на количество скорее, чем на качество вооружений, НОАК понимает всю важность высокотехнологичных средств, необходимых армии для сдерживания высокотехнологичных противников, и уже достаточно давно наращивает свой потенциал в области инструментария информационных войн. Информационные и коммуникационные средства могут использоваться совместно с «обычными» и кибератаками на радары противника и другие виды электронного оборудования, снижая способность противника использовать информационное поле в своих интересах и позволяя Китаю перехватить инициативу в случае нападения на него[129].

В 2015 году в китайской Белой книге по военной стратегии киберпространство впервые было определено как «критическая область безопасности» (*zhongda anquan lingyu*), наряду с океанами, космическим пространством и ядерной сферой. В конце того же года были созданы Силы стратегической поддержки НОАК в качестве специализированных сил для разработки и эксплуатации космических и кибервозможностей Китая. Широкий спектр космических, кибер и радиоэлектронных средств ведения войны, ранее находившихся в ведении отдельных учреждений НОАК, был затем передан Силам стратегической поддержки НОАК, которые теперь отвечают как за информационную поддержку, так и за отражение атак в информационных войнах[130].

Геополитическая нестабильность на глобальной арене в последние годы свидетельствует о том, что решение Китая подкреплять реализацию своей доктрины сдерживания средствами для сдерживания противника в информационном поле является совершенно правильным для обеспечения безопасности страны. Как было рассмотрено в предыдущем параграфе, США рассматривают нарушение социально-политической стабильности в государстве-противнике как одно из направлений ведения информационных

[129] Там же.
[130] Dossi, S. (2020). On the asymmetric advantages of cyberwarfare. Western literature and the Chinese journal Guofang Keji. *Journal of Strategic Studies*, *43*(2), 281-308.

войн. При этом США в настоящее время являются главным антагонистом Китая, пытаясь всевозможными путями воздействовать на его самостоятельное технологическое развитие, преследуя и ограничивая китайские ИТ-компании и их продукцию[131].

Приоритетная ориентация Китая на борьбу с угрозами для национальной безопасности как один из ключевых векторов осуществления его внешней политики, в том числе в информационном поле, четко проявилась в 2015 г., с принятием в стране закона «О государственной безопасности КНР». В значительной степени положения этого закона явились ответом на вызовы, брошенные Китаю в принятой несколькими месяцами ранее «Стратегии национальной безопасности США», и в целом были ориентированы на то, чтобы принести в глобальное информационное поле представление Китая о собственной траектории развития, в том числе геополитического, и границах национальной безопасности, а также четко позиционировать КНР как глобального игрока на международной арене. Статья 24 Закона «О национальной обороне» постулирует развитие проприетарных инноваций и достижение технологического суверенитета как краеугольный камень национальной безопасности КНР.

После принятия этих документов все нормативные правовые акты, так или иначе касающиеся технологического развития и развития информационного пространства КНР, рассматривали его (в первую очередь) с точки зрения национальной безопасности.

Особо стоит отметить Закон «О кибербезопасности» от 2017 г., в котором была выстроена система принципов и мер сетевой безопасности на трех уровнях – предупреждение, контроль, экстренное реагирование. В ст. 1 документа сказано, что Закон направлен на обеспечение сетевой безопасности, защиту суверенитета в киберпространстве и национальной безопасности. Особое значение в плане предупреждения развертывания конфликтов в информационном поле и информационных войн против Китая

[131] Мельникова О. Опыт Китая в защите национального киберсуверенитета // Международная жизнь. 13.12.2022. URL: https://interaffairs.ru/news/show/38218 (дата обращения 16.10.2024)

его высокотехнологичными противниками имел запрет, установленный этим законом для организаций, работающих с критической инфраструктурой КНР. Таким организациям было запрещено хранить данные где-либо за пределами Китая.[132]

Общая стратегия противодействия Китая информационной войне, навязываемой ему Соединенными Штатами, заключается в продолжении построения и расширения обособленного китайского интернет-пространства, в котором распространяемые США и их союзниками ложные сообщения, порочащие Китая, тщательно отфильтровываются. Позиция Китая, в соответствии с его стратегическими целями, делает больший акцент на контроле своего информационного пространства. Китайские власти отдают приоритет вопросу информационной безопасности, и эта концепция подчеркивает важность контроля над нарративами, информацией и контентом, распространяемыми среди своих граждан. Китай выступает за суверенитет в информации (киберпространстве), т. е. контроль над тем, что распространяется среди граждан через ИКТ.

Получение власти и превосходства в киберпространстве стало важной проблемой в Китае. Чтобы достичь доминирования в киберпространстве, вооруженные силы Китая ускорят модернизацию вооружения и оборудования и будут работать над разработкой систем вооружения и оборудованием, которые смогут эффективно реагировать на информационную войну и помогать выполнять миссии и задачи. Вооруженные силы Китая продолжат стратегический проект по подготовке кадров, который может соответствовать требованиям информационной войны. В 2024 году в китайской армии создано новое подразделение — Силы информационной поддержки, которое будет непосредственно подчиняться Центральному военному совету. Тем самым Китай готовится к усилению международного кибер-противостояния. До этого функционировали Силы

[132] Меньшиков П.В., Михина Л.К. Система противодействия угрозам информационной безопасности КНР // Вестник ЗабГУ. 2022. Т. 28. №1. С. 124 – 139.

стратегической поддержки, которые создавались для усиления возможностей в космосе, киберпространстве, политике и радиоэлектронной борьбе[133].

Говоря об информационных войнах, нельзя не сказать и о технологической конкуренции Китая и США, победа в которой принесет победителю мировое лидерство в развитии информационных технологий нового технологического уклада, а значит, и крупные преимущества в сдерживании противника от кибер- и информационных атак. Суверенитет в Интернете в частности и в информационном поле в целом немыслим без достижения технологической независимости. США выделили в 2021 году почти 250 млрд долларов «на обеспечение технологической конкурентоспособности с Китаем. Пятая часть этой суммы должна пойти на разработку и производство чипов и телекоммуникационного оборудования, а остальное (190 млрд долларов) – на развитие технологий и научных исследований в сфере ИКТ» [134].

Китай не озвучивает общий объем своих инвестиций в победу в этом технологическом противостоянии, однако раскрываемые КНР цифры по вложениям в развитие отдельных направлений ИКТ весьма значительны. Так, за последние годы Китай «инвестировал более 43,5 млрд юаней (6,12 млрд долларов США) в общенациональный проект по строительству вычислительных центров обработки данных» [135] ; вложил «более 47 миллиардов долларов в крупнейший в истории страны фонд инвестиций в чипы»[136]; выделил 15 млрд долларов на квантовые исследования, что в два раза превышает бюджет Евросоюза и в 8 раз – бюджет США на это направление[137].

---

[133] Китай готовится к усилению кибервойн. Создана особая армейская структура для ИТ-поддержки войск// СиНьюс, 22 Апреля 2024 года. URL: https://gov.cnews.ru/news/top/2024-04-22_kitaj_sozdal_novuyu_voennuyu (дата обращения: 1.04.2025)

[134] Мельникова О. Опыт Китая в защите национального киберсуверенитета / Международная жизнь. 13.12.2022. URL: https://interaffairs.ru/news/show/38218 (дата обращения 16.10.2024)

[135] China invests US$6.1 billion in data centre infrastructure amid surge in demand for AI chips / South China Morning Post. 29.08.2024. URL: https://www.scmp.com/tech/tech-trends/article/3276455/china-invests-us61-billion-data-centre-infrastructure-amid-surge-demand-ai-chips (дата обращения 18.10.2024).

[136] China invests $47 billion in largest ever chip fund / Techxplore. 27.05.2024. URL: https://techxplore.com/news/2024-05-china-invests-billion-largest-chip.html (дата обращения 16.10.2024).

[137] Chinese Quantum Companies and National Strategy 2023 / The Quantum Insider. 13.04.2023. URL:

Суверенитет в Интернете как защита в информационной войне

Начало этому процессу было положено практически сразу после появления Интернета в Китае – действительно, доменная зона .cn была зарегистрирована и начала активно развиваться в 1990 году, всего тремя годами после того, как в 1987 г. в Пекинском институте физики и высоких энергий был запущен интернет. Отметим, что исторически средства массовой информации стали активно развиваться в КНР после экономической реформы 1978 года, и содержание их публикаций подвергалось многоуровневому контролю (в первую очередь, со стороны отдела пропаганды ЦК КПК). В этом свете цензурирование публикаций в Интернете стало логичным продолжением изначально взятого курса на регулирование СМИ и информационной среды в целом.

Уже в середине 1990-х годов правительство Китая осознало значительный деструктивный потенциал новых информационно-коммуникационных технологий в руках противников КНР, и в 1998 году началась работа над масштабным проектом «Золотой щит», который был полностью завершен и начал функционировать в масштабах всей страны в 2003 году. Этот проект на тот момент являлся одной из самых совершенных систем фильтрации нежелательного интернет-контента в мире, а его национальный масштаб можно считать беспрецедентным. По сути он представлял собой «группу специальных серверов, осуществляющих фильтрацию интернет-трафика между китайскими провайдерами и международными сетями передачи информации, сквозную идентификацию пользователей, антивирусную защиту и контент-фильтрацию»[138]. Позднее

---

https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/ (дата обращения 16.10.2024). Betting big on quantum / McKinsey. 13.09.2022. URL: https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/charts/betting-big-on-quantum (дата обращения 16.10.2024).

[138] Chinese Quantum Companies and National Strategy 2023 / The Quantum Insider. 13.04.2023. URL: https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/ (дата обращения 16.10.2024). Betting big on quantum / McKinsey. 13.09.2022. URL: https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/charts/betting-big-on-quantum (дата обращения 16.10.2024).

функция контент-фильтрации была выделена в отдельную систему, названную «Большой китайский файрвол»; свою эффективность эти две системы, работающие совместно, сохраняют до сих пор благодаря регулярным техническим усовершенствованиям – к примеру, в 2021 году был разработан «Интернет-цензор» – это поисковый алгоритм с использованием искусственного интеллекта, который «позволяет находить подлежащие цензуре тексты с точностью в 91%» [139] . Система «Большой китайский файрвол» позволяет на время или навсегда блокировать отдельные веб-сайты или даже результаты поиска по определенным ключевым словам или словосочетаниям. Исследователи определили, что «чаще всего в Китае блокируются сайты, связанные с бизнесом, далее следуют ресурсы с порнографическими материалами, а за ними – домены, связанные с IT. Также блокируются сайты, предлагающие инструменты по обходу GFW, online-казино, личные блоги, развлекательные ресурсы, СМИ и домены с вредоносным контентом»[140].

В 2010 году руководство КНР назвало Интернет «кристаллизацией человеческой мудрости», но пояснило, что намерено бороться с распространением незаконной информации в нем и оберегать население страны от такой информации. Это стратегическое видение было затем закреплено в серии нормативных правовых актов. Так, 2013 год ознаменовался принятием закона об ответственности за публикацию недостоверной или ложной информации, а также критику властей; ответственность «вплоть до уголовной по этому закону наступает от 500 перепубликаций размещенного сообщения или от 5 тыс. просмотров» [141]. В 2014 г. было основано Управление Центральной комиссии по делам киберпространства.

---

[139] Китайцы создали высокоэффективного ИИ-цензора / SecurityLab.ru. 15.04.2021. URL: https://www.securitylab.ru/news/518922.php (дата обращения 16.10.2024)

[140] Исследователи установили, какой контент чаще всего блокируется в Китае / SecurityLab.ru. 12.07.2021. URL: https://www.securitylab.ru/news/522101.php (дата обращения 16.10.2024)

[141] Люлина А. Г., Ефименко Е. С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник РУДН. Серия: Всеобщая история. 2022. Т. 14. №2. С. 175–188.

На 24-м заседании Постоянного комитета 12-го Всекитайского собрания народных представителей в ноябре 2016 года был принят Закон «О кибербезопасности»; однако главная цель его не ограничивается обеспечением кибербезопасности, но включает также обеспечение суверенитета китайского киберпространства (обе эти цели оказываются подчинены генеральной задаче обеспечения национальной безопасности КНР в целом). Одним из главных нововведений в этом законе стал отказ от анонимности в китайском сегменте Интернета. Закон гласит: «при регистрации доступа в интернет, регистрации в социальной сети, подключении стационарного телефона или мобильной связи, предоставлении клиенту услуг публикации информации или ее передачи, при подписании соглашения (об оказании услуг) клиент должен предоставить подлинное удостоверение личности. Если оно не будет предоставлено, то оператор услуг не имеет права на обслуживание клиента»[142]. В продолжение этой инициативы в 2020 году вышло постановление, обязывающее пользователей онлайн-игр в обязательном порядке удостоверять свою личность перед получением доступа, собственно, к игре.

В июне 2021 года в Китае был принят закон, предусматривающий наказание за распространение недостоверной информации о военнослужащих КНР, клевету на них и распространение сведений, порочащих их честь и достоинство.

В настоящее время правительство Китая строго регулирует интернет-пространство, цензурируя нежелательную информацию и блокируя доступ к запрещенным сайтам. Китай считается одной из стран с наиболее жесткой и эффективной системой интернет-цензуры. Сразу несколько государственных ведомств осуществляют надзор и контроль над соблюдением законов в китайском сегменте Интернета, однако каждое из них имеет свои функции. Так, Министерство промышленности и информатизации КНР отвечает за

[142] Китай вводит обязательную идентификацию интернет-пользователей / Digital.Report. 29.08.2017. URL: https://digital.report/kitay-vvodit-obyazatelnuyu-identifikatsiyu-internet-polzovateley/ (дата обращения 16.10.2024).

техническую сторону регулирования; в зону ответственности Департамента интернет-безопасности и защиты Министерства государственной безопасности входит собственно осуществление контроля и стремительное блокирование Интернет-ресурсов, угрожающих социально-политической стабильности и национальной безопасности Китая, активное противодействие попыткам высокотехнологичных противников Китая проникнуть в китайский сегмент Интернета с вредоносными целями коррумпирования социалистической морали; Центральная комиссия по делам при ЦК КПК ответственна за общий «курс» Китая в вопросах Интернет-цензуры; Национальное управление радио и телевидения отвечает за блокирование интернет-провайдерами доступа к порнографическим ресурсам и сайтам, предлагающим азартные игры. Контроль и надзор в китайском сегменте интернета осуществляется не только силами перечисленных выше государственных органов, но и с участием территориальных киберподразделений полиции, каждое из которых отслеживает деятельность в Интернете населения небольшого городского или сельского района. Вовлечены и китайские ИТ-гиганты: действительно, «в крупных китайских IT-компаниях, таких как «Sina», «Baidu», «Weibo» и «Tencent», есть большой штат работников, занимающихся фильтрацией интернет-контента. В местах общественного пользования Глобальной сетью на компьютеры дополнительно устанавливается специальное программное обеспечение, фильтрующее контент» [143].

Примеры ограничений в Китае включают блокировку доступа к западным сайтам, таким как Google, Facebook [144], Twitter [145] и YouTube, а также наложение строгих ограничений на содержание и диалоги в китайских социальных сетях. Однако при этом практически для всех заблокированных крупных западных ресурсов имеются активно функционирующие китайские

[143] Мельникова О. Опыт Китая в защите национального киберсуверенитета / Международная жизнь. 13.12.2022. URL: https://interaffairs.ru/news/show/38218 (дата обращения 16.10.2024)

[144] Организация признана экстремистской, ее деятельность на территории Российской Федерации запрещена.

[145] Организация признана экстремистской, ее деятельность на территории Российской Федерации запрещена.

аналоги: Wechat – социальная сеть с более чем 1 млрд пользователей, Weibo – китайский сервис микроблогов, Youku – популярная видео- и стриминговая платформа, поисковая система Baidu и т.д. Фильтрация и блокировка контента, рассматриваемого как чувствительный, выполняется на основе ключевых слов, созданных для отслеживания определенных тем. Китайские интернет-медиа обязаны следовать законам и правилам, установленным правительством, и удалять любой контент, считающийся незаконным, недопустимым или противоречащим государственной политике. Из-за этой практики распространение некоторых новостей ограничено и может быть снято с общего доступа, если они противоречат политическим или идеологическим интересам страны в целом. О. Мельникова справедливо отмечает, что в КНР создана целая «экосистема» информационных сервисов, полностью удовлетворяющих потребности китайских граждан.

Структура управления Интернетом в Китае сформирована таким образом, что выход в международное Интернет-пространство возможен лишь из нескольких шлюзов национального уровня, которых в стране насчитываются лишь единицы. Прямой выход в международное Интернет-пространство для физических и юридических лиц запрещен. Это обусловливает чрезвычайно высокий уровень автономности китайского сегмента интернета, который даже при отключении от глобального Интернета (в случае массированной кибератаки и/или дальнейших попыток США подавить и ограничить развитие цифровизации в Китае) может превратиться в национальный интранет и практически не пострадать при этом[146]. Это очень важное достоинство политики в отношении развития Интернета, проводимой китайскими властями. Отметим, что с началом беспрецедентной волны санкций США в отношении России, РФ также предприняла меры по «изоляции Рунета» и приняла соответствующий закон,

[146] Cimpanu C. Oracle: China's internet is designed more like an intranet / ZDNet. 23.07.2019. URL: https://www.zdnet.com/article/oracle-chinas-internet-is-designed-more-like-an-intranet/ (дата обращения 16.10.2024).

призванный обеспечить функционирование российского сегмента Интернета в случае отключения от глобальной Сети.

За период с начала 2015 по конец 2017 гг. китайские органы, ответственные за цензуру в китайском сегменте Интернета, заблокировали более 13 тыс. веб-сайтов за нарушения китайского законодательства; опрос Синьхуа показал, что политику осуществления такой цензуры поддерживало более 90% населения страны, и значительно больше половины респондентов (63,5%) указали, что видят результативность этой политики, поскольку нежелательного контента они видят в этом сегменте Интернета гораздо меньше, чем в прошлые годы[147].

Социальные медиа в КНР

Китайская концепция, связанная с информационными возможностями, направлена на позиционирование Китая как одной из ведущих мировых держав в информационном пространстве. Кроме того, огромное внимание уделяется контролю и управлению информационной сферой на национальном уровне путем предоставления так называемого «цифрового суверенитета». Они осознают риски, связанные с социальными сетями, и пытаются советовать, но также контролировать граждан, чтобы они использовали социальные сети ответственно. На этих платформах хранится большой объем личной информации, относящейся к конкурентам. Социальные сети могут представлять угрозу национальной безопасности и политической стабильности, особенно учитывая, что создатели этих сетей происходят из определенных стран, отмеченных как конкуренты.

Одним из ключевых инструментов, которыми Китай пользуется, являются социальные медиа. Китайские компании, такие как WeChat, TikTok и Sina Weibo, имеют огромное количество пользователей по всему миру и используются для распространения китайской культуры и точки зрения на

[147] China closes more than 13,000 websites in past three years / Reuters. 24.12.2017. URL: https://www.reuters.com/article/us-china-internet/china-closes-more-than-13000-websites-in-past-three-years-idUSKBN1EI05M/?feedType=RSS&feedName=technologyNews (дата обращения 16.10.2024).

мировом уровне, а также для противодействия вестернизации традиционных китайских ценностей. Кроме того, Китай активно применяет различные технологические инструменты, включая системы массового наблюдения и взаимодействия, для мониторинга и контроля своей национальной и международной аудитории. Китай также активно продвигает свои геополитические интересы через мировые СМИ, используя собственные социальные и информационные платформы.

Китай может использовать социальные сети и другие средства массовой информации для создания и распространения определенных сообщений или мнений, чтобы воздействовать на общественное мнение. Китай активно использует эти методы для воздействия на мнение населения, как внутри страны, так и за ее пределами. Китай создает свой собственный контент и платформы, ориентированные на зарубежную аудиторию. Например, платформа Tik Tok, созданная в Китае, позволяет создавать и распространять короткие видеозаписи, некоторые из которых могут быть использованы для освещения точки зрения Китая по тем или иным вопросам.

Как верно отмечает О. Мельникова, «Государственная политика Китая в информационной сфере направлена на включение государства в мировое информационное пространство при сохранении национальной идентичности, государственного контроля над обществом и учете существующих политических и социально-экономических условий его развития» [148].

Итак, основным оружием Китая в информационной войне является ограничения своего информационного пространства для внешних информационных атак. Вместе с тем, имидж страны имеет значение, и он подвергается постоянным попыткам «коллективного Запада» быть приниженным.

Китай – по мере своего развития, становясь конкурентом Запада, подвергается мощным информационным атакам. Особенно ярко они проявились в пандемию 2020-2022 гг., когда Китай обвинялся чуть ли не в

[148] Мельникова О. Опыт Китая в защите национального киберсуверенитета / Международная жизнь. 13.12.2022. URL: https://interaffairs.ru/news/show/38218 (дата обращения 16.10.2024).

создании коронавирус, однако, имели место и раньше – по нарастающей все 2010е годы. В конце 2019 года возник скандал с так называемым «синьцзянское досье», составленным «прокси-силой» западных стран в информационной войне, так называем Международный консорциумом журналистов-расследователей (ICIJ). Досье содержало фейковую информацию о массовых репрессиях китайских властей против мусульманского населения в Синьцзян. Действительно, после социально-политического обострения на Ближнем Востоке в 2010-е годы («Арабская весна») в регионе стали развиваться экстремистские течения, однако действия властей были точечными и оправданными. При этом сами мусульманские страны практически не высказывали возмущения по этому поводу. возмущались[149].

Таким образом, данный пример конца 2019 года обнажил методы информационной войны – фабрикация и использования ложных новостей, подачу их якобы независимыми организациями, распространение в якобы авторитетных СМИ и обсуждение этих новостей «международным сообществом», создание неблагоприятного информационного фона, вредящего имиджу, продвижению политических, экономических и культурных интересов Китая в мире. В этом отношении до недавнего времени действительно ощущалась нехватка инструментария для противостояния таким атакам извне, однако, по мере укрепления проектно-идеологической деятельности руководства и научного сообщества страны (в том числе, в сотрудничестве с Россией) по формированию идеологии справедливого многополярного мироустройства основания для такого инструментария появляются.

[149] Щекоян И. Поднебесная правда: кто и зачем ведет информационную войну с КНР// Известия. 28 ноября 2019 года. URL: https://iz.ru/947921/irena-shekoian/podnebesnaia-pravda-kto-i-zachem-vedet-informatcionnuiu-voinu-s-knr (дата обращения: 1.09.2025).

2.3. Россия в информационном противостоянии с коллективным Западом: стратегические аспекты

Как официально заявил пресс-секретарь Президента России Д. Песков: «Сейчас мы находимся в состоянии информационной войны с законодателями моды в информационном пространстве, прежде всего, с англосаксами, их СМИ»[150]. Действительно, со второй половины нулевых годов стали неуклонно обостряться российско-американские отношения. В решающей степени это было связано с попытками руководства России восстановить информационный суверенитет страны и постепенно начать преследовать на международной арене национальные интересы.

Так, по замечанию И.А. Крыловой, «в 2014 г. после украинского «Евромайдана» и вхождения Крыма в Российскую Федерацию против нашей страны США и странами Евросоюза была развязана крупномасштабная информационно-психологическая война, главной целью которой является дестабилизация социально-экономической ситуации в России, инициация социального недовольства и «цветной революции» для свержения «режима Путина». Преследуя свои геополитические интересы, США и другими западными странами с целью ослабления Российской Федерации были введены антироссийские санкции (ущерб от которых для самих стран ЕС оценивается более чем в 1 трлн евро)»[151].

В своей более ранней работе И.А. Крылова справедливо утверждала, что «санкции Запада носят долговременный характер (введены даже не на годы, а скорее, на десятилетия подобно поправке Джексона-Веника) и включают в себя полный спектр инструментов экономического, политического и информационного давления на Россию. В конечном счете

---

[150] Песков: РФ находится в состоянии информационной войны с англосаксами [Электронный ресурс]. URL: http://rg.ru/ 2016/03/26/peskov-rf-nahoditsia-v-sostoianii-informacionnoj-vojny-s-anglosaksami.html

[151] Крылова И. А. Информационно-психологические войны как фактор дезинтеграционных процессов в современном мире //Большая Евразия: развитие, безопасность, сотрудничество. – 2021. – №. 4-1. – С. 106-110.

они направлены на дестабилизацию социально-экономической ситуации, смену лидера и политического режима в нашей стране»[152].

Н.Р. Красовская с коллегами показывают, что «ключевой целью информационных войн является лишение власти или ее ослабление ради навязывания своей воли и лишения суверенитета другой страны. Способы реализации власти в России являются ключевыми объектами информационных атак Запада, и прежде всего США»[153], при этом «ведущей технологией проведения информационных войн против России является создание крайне негативного образа государства и общества. В самом общем и крайнем своем выражении этот образ имеет русофобский характер … . Следовательно, идеологическая подоплека технологий информационной войны против России сводится к одному из проявлений ксенофобии – русофобии»[154].

При этом понятия объекта и мишени информационно-психологической войны неравнозначны – подтверждение этого тезиса находим у А.П. Сковородникова и Э.А. Корольковой, полагающих, что «если объектом такой войны считать сознание, то мишенями являются понятия и представления о связанных с объектом сторонах действительности, которые подвергаются негативной оценке. Так, в настоящее время мишенями информационно-психологической войны являются властная вертикаль, Русская православная церковь, внешняя политика руководства страны, русский язык, русская литература и т. д.»[155].

В этих условиях все большее число военных, представителей разведывательного сообщества, политтехнологов, профессионалов информационных коммуникаций стали высказываться за необходимость

---

[152] Крылова, И. А. (2016). Новые виды войн и безопасность России. *Знание. Понимание. Умение*, (3), 58-71.
[153] Красовская, Н. Р., Гуляев, А. А., Лахтин, А. Ю., & Вакуленко, А. Н. (2019). Технологии информационных войн против России. *Власть*, (3), 42-47.
[154] Красовская, Н. Р., Гуляев, А. А., Лахтин, А. Ю., & Вакуленко, А. Н. (2019). Технологии информационных войн против России. *Власть*, (3), 42-47.
[155] Сковородников А. П., Королькова Э. А. Речевые тактики и языковые средства политической информационно -психологической войны в России: этико-прагматический аспект (на материале «Новой газеты») // Политическая лингвистика. 2015. № 3 (53). С. 160—172.

существенного расширения инструментария противоборств [156] . Информационное противоборство существенно обострилось даже в такой сфере, как спорт высоких достижений, его особенно острые всплески фиксируются с проведением очередных Олимпийских Игр (что напрямую противоречит самому духу и историческим традициям, сопутствовавшим этому мероприятию и призывавшим останавливать все военные конфликты в период проведения Игр)[157].

Беспрецедентного масштаба достигло давление стран коллективного Запада на Россию после начала СВО. Как подчеркивает директор Московского центра Карнеги Д. Тренин, «гибридная война» против России уже идет на разных полях: политическом (изоляция), экономическом (санкции), информационном (в СМИ), в киберпространстве и т.д.[158]

Примечательно при этом, что инструментарий «мягкой силы», используемый в информационно-психологических войнах странами коллективного Запада, применительно к России становится все более жестким. Как отмечает Р.С. Выходец, «с начала боевых действий западные СМИ и социальные сети наполнились ярко выраженным русофобским содержанием, активно создаются и тиражируются фейки в отношении действий российских вооруженных сил на территории Украины, блокируются пророссийские каналы в YouTube и группы в социальных сетях. 11 марта 2022 г. американская компания Meta Platforms[159] подтвердила снятие ограничений в Facebook[160] и Instagram[161] на призывы к насилию в

---

[156] Кугушева, А. (2016). От информационных войн к поведенческим. *Информационные войны*, (1), 11-22. С. 14.

[157] Бутусов, А. В. (2018). Политический характер информационных войн в сфере спорта. *Вестник Тамбовского университета. Серия: Общественные науки*, *4*(14), 76-79. Бутусов, А. В. (2018). Политический характер информационных войн в сфере спорта. *Вестник Тамбовского университета. Серия: Общественные науки*, *4*(14), 76-79. Воинов, Д. Е. (2015). «Мягкая сила» Игр «Сочи-2014» и зарубежные медиа: анализ политико-информационного фона российской Олимпиады. *Вестник Московского университета. Серия 25. Международные отношения и мировая политика*, *7*(2), 155-181.

[158] Тренин Д. Конфликт уникальностей. Как будут складываться отношения России и США после послания Путина // Российский совет по международным делам. 2018. 5 марта. URL: http://russiancouncil.ru/analytics-and-comments/comments/konfl ikt-unikalnostey-kak-budut-skladyvatsya-otnosheniya-rossii-i-ssha-posleposlaniya-putina/#detail

[159] Признана экстремистской и запрещена на территории РФ.

[160] Признана экстремистской и запрещена на территории РФ.

[161] Признана экстремистской и запрещена на территории РФ.

отношении российских военных. В ответ Роскомнадзор 14 марта 2022 г. заблокировал Facebook и Instagram на территории России»[162].

При этом России предъявляют обвинения в активном распространении дезинформации и пропаганды с целью воздействия на мировую политику и общественное мнение. Одним из примеров такого «вмешательства» было якобы имевшее место воздействие на президентские выборы в США в 2016 году. Взлом Национального комитета Демократической партии во время выборов в США в 2016 году был приписан российским хакерам. По голословным обвинениям «экспертных» и политических кругов США, российские спецслужбы якобы организовали скоординированную кампанию с целью распространения ложной информации и разжигания разногласий среди американских избирателей. Эта кампания также якобы включала использование социальных медиаплатформ и распространение фейковых новостей.

Россию также обвиняют в распространении дезинформации с целью продвижения своей политической повестки, особенно в контексте отношений с другими странами. Например, после украинской революции в 2014 году Россию обвинили в использовании СМИ для распространения ложной информации о событиях и для оправдания «аннексии» Крыма, грубо пренебрегая фактов изъявления своей политической воли населением Крыма на законном референдуме.

На современном этапе Россия подвергается обвинениям в чрезмерной активности в иностранных информационных конфликтах. Лавина таких бездоказательных обвинений, к примеру, была обрушена на Россию Великобританией в контексте «дела Скрипалей»[163]. Пошаговый анализ этого

---

[162] Выходец Р.С. (2022) «Информационные доминанты» как инструмент информационно-психологических войн // Общественные науки и современность. № 4. С. 93–104. С. 94-95.

[163] Тагильцева, Ю. Р. (2018). Стратегии и тактики информационно-психологической войны в контексте российско-британских отношений. *Экология языка и коммуникативная практика*, (4), 92-104. Ананьева, Е. В., & Годованюк, К. А. (2018). Матрёшка “дела Скрипалей”. *Современная Европа*, (3 (82)), 16-26. Годованюк, К. А. (2019). Кибербезопасность и борьба с дезинформацией: опыт Великобритании. *Научно-аналитический вестник Института Европы РАН*, (4), 87-92. Ананьева, Е. В. (2018). Сумеют ли США и Британия сделать из России страну-изгой?. *Научно-аналитический вестник Института Европы РАН*, (2), 5-12.

дела именно как информационной операции представлен выдающимся российским политологом А.В. Манойло[164].

Более того, некоторые зарубежные эксперты говорят о резком ухудшении международной обстановки, усилении информационных противоречий и возрождении холодной войны. В настоящее время, по мере углубления российско-украинского конфликта, давление Запада на Россию усиливается за счет введения дополнительных санкций. США и Европа продолжают поставлять оружие, технологии и финансовую помощь на передовую линию конфликта между Россией и Украиной с намерением добиться того, чтобы Россия не могла восстановить свои позиции.

Запад также использует свое влияние на общественное мнение и медийные ресурсы для представления военных действий, которые были вызваны длительным обманом и провокациями со стороны Запада, как, якобы, давно спланированной и жестокой агрессии против демократической страны. Конфликт между Россией и Украиной из-за различия в геополитических интересах представляется как некое столкновение интересов зла и справедливости. При этом намеренно игнорируется история возникновения этого конфликта между Россией и Украиной, и целью коллективного Запада является дискредитация, экономическое ослабление и физическое изолирование России.

В рамках кампании Запада по формированию общественного мнения голос и позиция России постепенно утрачивают актуальность в мировых медийных и информационных источниках. Даже страны, которые поддерживают нормальные партнерские отношения с Россией, включая Китай, сталкиваются с дискредитацией в глазах западного общества.

В свете западных попыток манипулирования общественным мнением, международное сообщество, особенно развивающиеся страны, должно преодолеть сложные иллюзии, создаваемые западными СМИ и политиками, чтобы лучше понять основные факты российско-украинского конфликта и

[164] Манойло, А. В. (2019). " Дело Скрипалей" как операция информационной войны. *Российский социально-гуманитарный журнал*, (1), 72-97.

осознать потенциальные угрозы, стоящие за шумом общественного мнения. Ведь то, что происходит в России сегодня, может повлиять на будущее всех развивающихся стран.

История вражды между Россией и США и Западом – это история манипуляций и угрозы со стороны США потенциальным конкурентам в мировой гегемонии. «Гегемон» или «гегемония» - признанные термины в политической науке, это - лицо, государство или общественный класс, осуществляющие гегемонию (политическое, экономическое, военное превосходство) Исторически они имели нейтральную окраску как констатация факта, но в последние десятилетия приобрела негативную коннотацию. После распада Советского Союза Россия попыталась приблизиться к Европе и США в надежде на признание и поддержку. Она даже несколько раз подавала заявку на вступление в НАТО, и первого президента России, Бориса Ельцина, часто называли "европеистом". 28 сентября 1994 года президент США Билл Клинтон и президент России Борис Ельцин подписали в Белом доме декларацию о сотрудничестве в области экономики и безопасности между США и Россией.

Добросердечные попытки России не смогли развеять подозрения и опасения США и Европы. Несмотря на явные попытки сблизиться с Западом и заключить ряд так называемых соглашений о сотрудничестве, включая "Партнерство ради мира", каждый раз, когда Россия полагала, что она получила билет в западный мир и выразила интерес к официальному вступлению в западные клубы, такие как ЕС или НАТО, ей постоянно отказывали.

В то же время ЕС и НАТО продолжали расширяться на восток, принимая в свои ряды Польшу, Венгрию, Эстонию, Латвию и Литву, что уменьшило стратегическое пространство России. На саммите НАТО, который прошел в Испании 8 июля 1997 года, была объявлена первая волна восточного расширения, включающая в себя Польшу, Чешскую Республику и Венгрию в члены НАТО. Когда Россия, наконец, осознала, что Запад, с

которым она рассматривала перспективы партнерства, наносит ей удар в спину, военная мощь НАТО уже подошла к дверям России и образовала окружение вокруг Москвы.

И только после того, как Россия осознала, что она была обманута Западом, она начала принимать контрмеры. Возникновение российско-украинского конфликта также явилось прямым результатом политики со стороны Запада. Прежде чем Россия начала СВО, она ясно выразила желание получить гарантии от США в том, что Украина не будет включена в НАТО. Однако США воздержались от занятия четкой позиции.

На сегодняшний день Украина стала объектом интереса Запада в контексте его противостояния с Россией. Западный блок, с США во главе, неохотно поддерживает усилия по мирным переговорам между Россией и Украиной, в надежде использовать конфликт в своих стратегических интересах, включая устранение России как потенциальной угрозы для западного мирового порядка.

Для многих незападных стран российский опыт становится уроком, не подлежащим сомнению. Запад готов приветствовать только те страны, которые не оспаривают его гегемонию и выполняют его указания. Однако если какая-либо развивающаяся страна наберет достаточную силу, чтобы противостоять западному порядку, «дружественная» политика Запада может мгновенно превратиться в полномасштабную гибридную войну.

Отношения между Россией и Китаем представляют собой исторический феномен, важный в рамках многополярного мира, и обусловлены необходимостью геобалансировки. Растущее партнерство между Китаем и Россией сегодня воспринимается США и Западом как серьезная угроза их гегемонии. Запад прикладывает все усилия для провокации и дискредитации нормальных отношений между Китаем и Россией в попытке разделить и подчинить обе эти страны. Тем не менее, эти усилия обречены на провал.

С точки зрения внутренних мотиваций, Китай и Россия являются соседями, которых невозможно разорвать, и их экономические структуры взаимодополняют друг друга, что делает дружбу между ними выигрышной стратегией. С учетом глобальных тенденций дружба между Китаем и Россией становится исторической необходимостью в условиях многополяризации и геополитического баланса в современном мире. Кроме того, Соединенные Штаты продолжают препятствовать и подавлять эти отношения, что побуждает крупные и быстро развивающиеся страны, включая Китай и Россию, к сближению.

В 2010 году Китай официально превзошел Японию по объему ВВП, став второй по величине экономикой мира после США. Впервые после Второй мировой войны незападная страна вошла в верхний эшелон мировой экономики, и это вызвало беспокойство в США, поскольку означало, что Китай представляет прямой вызов их гегемонии. Скоро после этого, тогдашний президент США Барак Обама объявил о начале реализации своей стратегии «Возвращение в Азиатско-Тихоокеанский регион», основным направлением которой было объединение союзников США в данном регионе и сдерживание Китая. В 2022 году Министерство обороны США опубликовало доклад о стратегии национальной безопасности, в котором Китай четко определяется как глобальный конкурент номер один.

Реальная цель США в сдерживании и окружении Китая и России заключается в том, чтобы остановить процесс глобальной многополярности и сохранить международную модель доминирования США. Однако несмотря на усилия США объединить своих союзников в попытке противостоять потенциальным новым «центрам силы» и замедлить убыль гегемонии, тенденция многополяризации и геополитического баланса в современном мире необратима, и она следует из роста и восхождения развивающихся стран и общего вектора глобализации.

Как развивающиеся страны, выступающие против односторонней гегемонии и за многополярность, Китай и Россия, находясь под давлением

США, играют ключевую роль в поддержании глобального геополитического баланса. Если Китай и Россия сближаются, многополярность в мире будет усиливаться; если наоборот, односторонняя гегемония станет еще более безумной. Лидеры многих стран, включая президента Бразилии Лулу и премьер-министра Индии Моди, дали понять, что они не присоединятся к антироссийскому лагерю.

Нынешняя осада России Западом достигла критического момента. Однако влияние военного лобби и сторонников жестких (в том числе и военных) мер в отношении России в американском истеблишменте будет только нарастать, а это значит, что милитаризация внешнеполитического курса США будет продолжена.

В Главе 1 мы перечислили некоторые из наиболее значимых инструментов информационных войн. Все они активно применяются коллективным Западом в отношении России в настоящий момент:

- использование «фейков», в том числе «фейковых» новостей – такие новости активно генерируются и распространяются Украиной и СМИ стран коллективного Запада (в том числе о якобы применении Россией тех или иных запрещенных видов оружия);
- использование технологий искусственного интеллекта для создания заведомо ложных визуальных изображений с целью дискредитации противника – этот инструмент также активно применяется Украиной с одобрения ее западных партнеров, в том числе с активным использованием западных социальных сетей (таких, как Instagram и Facebook – именно поэтому обе сети признаны экстремистскими и запрещены на территории России);
- использование комментаторов-«троллей» для массового комментирования сообщений и/или постов в социальных сетях, посвященных тем или иным событиям (явлениям), в определенном ключе, целью которого является создание определенного отношения к описываемым событиям (явлениям) у остальных читателей и

комментаторов – этот инструмент также массово применяется Украиной в социальных сетях;

- «демонизация» лидера Российской Федерации и ключевых лиц, принимающих решения, достигла абсурдных масштабов (что выразилось в выдаче Международным уголовным судом ордера на арест Президента России В.В. Путина); новый виток консолидации западного мира, как верно отмечают О.М. Шевченко и Л.Л. Штофер, осуществляется «на основе конструирования образа врага в лице России», украинские и западные СМИ активно насаждают русофобию, преподнося образ России как воплощения абсолютного зла, а на Украине процесс «формирования национальной идентичности … сопровождается использованием агрессивной русофобии в качестве эффективной технологии политического конструирования украинской нации»[165].
- фальсификация истории – этот инструмент на протяжении десятилетий используется коллективным Западом, в особенности США, относительно истории России, в частности, заслуг СССР в победе над фашизмом; к примеру, К.А. Демин с коллегами указывали, что далеко не в полной мере Россией задействуется потенциал такого инструмента, как компьютерные игры военно-исторического жанра, в то время как США массово используют этот инструмент, и создаваемые ими псевдоисторические и, в большинстве случаев, антироссийские по духу игры, способствуют весьма эффективной фальсификации истории в глазах подростков и молодежи, среди которых эти игры активно распространяются[166];
- тщательные чистки информационного пространства от информационных ресурсов и контента противника с одновременным активным распространением собственных – в этом контексте чрезвычайно показательна история полномасштабной кампании, развернутой Штатами

[165] Шевченко, О. М., & Штофер, Л. Л. (2015). Ксенофобия как эффективная технология современных информационных войн. *Гуманитарий Юга России*, (1), 98-108.
[166] Демин, К. А., Пушкарева, И. Н., & Тагильцева, Ю. Р. (2016). Компьютерные игры военного жанра как элемент пропаганды в информационной войне России и США. *Политическая лингвистика*, (5), 110-116.

против финансируемого Россией телеканала Russia Today, который круглосуточно вещает на английском языке через кабельные и спутниковые сети по всему миру. В 2013 г. телеканал Russia Today первым из новостных ТВ мира преодолел отметку в миллиард просмотров на YouTube [167] . Подобная популярность ресурса, освещающего независимую точку зрения России по значимым глобальным событиям, не устроила американцев. Еще в середине 2010-х некоторые американские «эксперты» предлагали заморозить активы RT, хотя телеканал Russia Today не является госсобственностью России. В ответ на эти нападки главный редактор Russia Today Маргарита Симоньян «написала, что ей было забавно слышать призывы ограничить деятельность российского телеканала от тех людей, которые, по идее, должны прославлять достоинства демократии и свободы слова»[168].

- технологии «управляемого хаоса», применяемые Западом в отношении России, имеют своей целью «вытеснение России с мировой политической арены и внесение ее в список так называемых государств-изгоев. Именно это, по мнению русофобски настроенных американских политических деятелей, позволит устранить Россию с политической арены как субъект политики»[169], а также ставят такую цель, как «организация «оранжевой революции» с последующим захватом власти проамериканскими силами»[170].

Стратегические документы, касающиеся информационных войн и национальной безопасности Российской Федерации в глобальном информационном поле, позволяют проследить нарастающее осознание информационных угроз со стороны стран коллективного Запада. Так, в

---

[167] Суходолов, А. П. (2015). Идеологическая функция средств массовой информации в условиях информационных войн. *Вопросы теории и практики журналистики*, *4*(2), 117-126.
[168] Мартыненко, Е. В. (2016). Характер информационной войны между Россией и США в Сирии. *Общество: политика, экономика, право*, (9), 9-12.
[169] Шевченко, О. М., & Штофер, Л. Л. (2015). Ксенофобия как эффективная технология современных информационных войн. *Гуманитарий Юга России*, (1), 98-108.
[170] Соколов, Д. В. (2016). Способы защиты российских национальных интересов от информационных угроз извне, спровоцированных в результате обострения восточно-украинского политического конфликта. *Общество: политика, экономика, право*, (3), 53-58.

Концепции национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации № 24 от 10.01.2000 г. были определены следующие угрозы в информационной сфере: «стремление ряда стран к доминированию в мировом информационном пространстве, вытеснению России с внешнего и внутреннего информационного рынка; разработкой рядом государств концепции информационных войн, предусматривающей создание средств опасного воздействия на информационные сферы других стран мира; нарушение нормального функционирования информационных и телекоммуникационных систем, а также сохранности информационных ресурсов, получение несанкционированного доступа к ним»[171].

В пришедшей на смену ей Стратегии национальной безопасности Российской Федерации до 2020 года отмечаются «попытки создания структуры международных отношений, основанной на доминировании в международном сообществе развитых западных стран при лидерстве США и рассчитанной на односторонние, прежде всего военно-силовые, решения ключевых проблем мировой политики в обход основополагающих норм международного права»[172]. Однако термин «информационная война» в этом документе, как и в предыдущем, рассмотренном выше, не использовался.

Пришедшая ей на смену Стратегия национальной безопасности, утвержденная в 2015 году, упоминала, что «укрепление России происходит на фоне новых угроз национальной безопасности, имеющих комплексный взаимосвязанный характер. Проведение Российской Федерацией самостоятельной внешней и внутренней политики вызывает противодействие со стороны США и их союзников, стремящихся сохранить свое доминирование в мировых делах. Реализуемая ими политика сдерживания России предусматривает оказание на нее политического, экономического,

[171] Указ Президента Российской Федерации № 24 от 10.01.2000 «О Концепции национальной безопасности Российской Федерации» URL: https://docs.cntd.ru/document/901751578 (дата обращения 14.11.2024)
[172] Указ Президента Российской Федерации № 537 от 12.05.2009 «О Стратегии национальной безопасности Российской Федерации до 2020 года» URL: https://docs.cntd.ru/document/902156214 (дата обращения 14.11.2024)

военного и информационного давления»[173]. Таким образом, речь шла об информационном давлении – но, опять-таки, не об информационной войне.

В Стратегии 2021 года в качестве одной из задач по обеспечению обороны страны обозначен «своевременный учет тенденций изменения характера современных войн и вооруженных конфликтов, создание условий для наиболее полной реализации боевых возможностей войск (сил), выработка требований к перспективным формированиям и новым средствам вооруженной борьбы»[174], однако содержание понятия «современных войн» не раскрывается и потому остается неоднозначным вопрос, учитывает ли это понятие информационные войны (как кибервойны, так и информационно-психологические). Это представляется довольно существенным упущением в документе, поскольку, как верно отмечает Р.С. Выходец, «Запад серьезно ограничен в применении военной силы в отношении России, а также несет издержки от собственных санкций и российских контрмер в финансово-экономической плоскости, которые подкрепляются зависимостью стран ЕС от поставок российских энергоносителей. Соответственно, значительную часть своих усилий данная сторона сосредоточила на информационной войне против России»[175].

Выводы по главе 2

Подводя итог, в условиях заката однополярной системы и попыток США «закрепить» ускользающую гегемонию и подавить новые мировые центры силы, Китай нацелен стать безусловным мировым лидером в сфере информационных технологий, и при этом должен давать адекватный ответ на нападки США и развязывание ими информационной войны против КНР.

В частности, Китай уделяет значительное внимание технологиям кибербезопасности и защиты информации, укреплению собственной

[173] Указ Президента Российской Федерации № 683 от 31.12.2015 «О Стратегии национальной безопасности Российской Федерации» URL: https://docs.cntd.ru/document/420327289#6520IM (дата обращения 14.11.2024)
[174] Указ Президента Российской Федерации № 400 от 02.07.2021 «О Стратегии национальной безопасности Российской Федерации» URL: https://docs.cntd.ru/document/420327289#6520IM (дата обращения 14.11.2024)
[175] Выходец Р.С. (2022) «Информационные доминанты» как инструмент информационно-психологических войн // Общественные науки и современность. № 4. С. 93–104. С. 94.

информационной безопасности (а также вопросам информационной безопасности в целом, на международном уровне) и использует различные инструменты для недопущения в свое интернет-пространство (и информационное пространство в целом) продуцируемых США месседжей, направленных на очернение Китая, подрыв его традиционной культуры и ценностей, а также на расшатывание внутренней социально-политической стабильности КНР. Важно отметить, что стратегия Китая в информационных войнах в значительной степени ориентирована на долгосрочное воздействие и укрепление своего влияния на мировой арене.

Впервые необходимость наращивания российского потенциала отражения атак информационного характера стала очевидной в период грузино-осетинского конфликта в августе 2008 г. После этого Россия предприняла многие меры по укреплению этого потенциала (в частности, учреждение международного информационного агентства «Россия сегодня», а также поддержка развития международного телеканала Russia Today). С учетом информационной войны беспрецедентных масштабов, развернутой в настоящее время коллективным Западом против России, представляется необходимым дополнить стратегические документы, регламентирующие защиту национальной безопасности страны, понятием гибридных войн, а также информационных войн и, в особенности, информационно-психологических войн, поскольку их ключевое отличие от традиционных войн – а именно воздействие на сознание масс гражданского населения – требует разработки и внедрения новых инструментов противодействия.

ГЛАВА 3. ТЕНДЕНЦИИ И ПЕРСПЕКТИВЫ ИЗМЕНЕНИЙ ХАРАКТЕРА ИНФОРМАЦИОННЫХ ВОЙН И ИХ НАУЧНОГО ОСМЫСЛЕНИЯ В УСЛОВИЯХ ГЛОБАЛЬНЫХ СОЦИАЛЬНЫХ ТРАНСФОРМАЦИЙ

3.1. Проблема информационных войн в научных исследованиях: наукометрический срез

Целью информационной войны в самом ее базовом определении является получение информационного превосходства над противником. Более детальные определения рассматривают ее как «манипулирование информацией, которой доверяет цель, без ее ведома, так что цель будет принимать решения против своих интересов, но в интересах того, кто ведет информационную войну[176],[177]. Нередко концепция информационной войны переплетается с концепцией кибервойны. Между ними можно провести различие на том основании, что кибервойна связана с конкретными атаками на компьютеры, программное обеспечение и цифровизированные системы связи, в том числе – на поле боя. Что же касается информационной войны, НАТО, развязавшее многие информационные войны в мире, в одном из своих документов отмечает следующее: «Киберпространство и связанная с ним область новых технологий предоставляют важное поле для информационной войны. Действия кибервойны могут состоять из кибератак, уничтожающих информационные системы противника, но они могут также включать в себя так называемые социальные кибератаки, создавая в сознании людей определенный образ мира, соответствующий целям информационной войны, ведущейся данной страной»[178]. Информационная война никогда не объявляется явно, она может предшествовать боевым действиям, следовать

[176] Glenn J.C., Florescu E., The Millennium Project Team. State of the Future 19.1. Washington, DC: The Millennium Project, 2018.
[177] Lewis B.C. Information Warfare / Federation of American Scientists. Intelligence Resource Program. URL https://irp.fas.org/eprint/snyder/infowarfare.htm (дата обращения 15.10.2024).
[178] Information warfare / NATO. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (дата обращения 15.10.2024).

параллельно им или за ними, равно как и заменять их. Отсутствие единого общепринятого определения информационной войны на фоне бурного развития этого многомерного явления, изменяющего собой основные принципы ведения войн, обусловливает наш интерес к исследованиям информационных войн, ведущимся в разных странах.

Значительный массив научных публикаций по тематике информационных войн накоплен сейчас не только в западных странах, но и в российской научной среде – поскольку проблема принудительного вовлечения России в информационные войны странами коллективного Запада актуализировала необходимость изучения технологии данного явления для выработки противодействия им. Соответственно, логично предположить, что всплески интереса российских ученых к информационным войнам должны быть связаны собственно с информационными военными кампаниям, развертываемыми против Российского государства.

Для проверки этого предположения обратимся к российской библиографической базе данных научного цитирования РИНЦ. В ней индексируется более 39 млн научных публикаций и патентов. Для начала можно рассмотреть и проанализировать результаты поиска в этой базе, проведенного по ключевым словам «информационная война».

Этот поиск дает более 111 тыс. результатов – статей в журналах и сборниках, монографий (индивидуальных и коллективных), глав в монографиях, тезисов в материалах конференций. При этом присутствуют публикации не только на русском, но и на некоторых других языках.

Рассмотрим теперь, как эти публикации распределены во времени. Для этого построим график, где отразим численность таких публикаций в год за период с 2000 по 2024 год– см. Рисунок 3.1.

Рисунок 3.1 – Ежегодное количество публикаций в РИНЦ по тематике «информационная война» с 2000 года

Источник: данные получены автором в апреле 2025 года по поиску термина «информационная война» в названии, ключевых словах или аннотации статьи.

Наше предположение подтверждается. По мере обострения во взаимоотношениях России и Запада, выливающегося в прокси-конфликты, происходил рост интереса российских ученых к данной теме.

Как видно из Рисунка 3.1 с середины 2000 годов происходило три волны роста исследовательского интереса к данной тематике. Все они приурочены и, очевидно, взаимосвязаны с изменениями военно-политической ситуации, в которой находилась Россия – сначала это было пятидневное «принуждение к миру» в Грузии, в середине 2010-х годов – события в Сирии и на Украине, наконец, в 2022 году началась Специальная военная операция России на Украине, сопровождающаяся всеми современными проявлениями информационной войны и ее технологического оснащения.

Логично предположить, что тематика публикаций российских ученых по информационным войнам должна быть в наибольшей степени связана с

Россией – но также и со странами, проявляющими агрессию по отношению к России, заставляющими ее вступать с ними в конфликты. В первую очередь, это США, но и другие западные страны могут представлять интерес для российских ученых, исследующих стратегии и тактики ведения современных информационных войн. Для этого нужно оценить, сколько публикаций, выданных поиском по запросу «информационная война», посвящены конкретно той или иной страны (название страны присутствует в наименовании, ключевых словах или аннотации публикации). Результаты этого нашего расчета представлены на Рисунке 3.2.

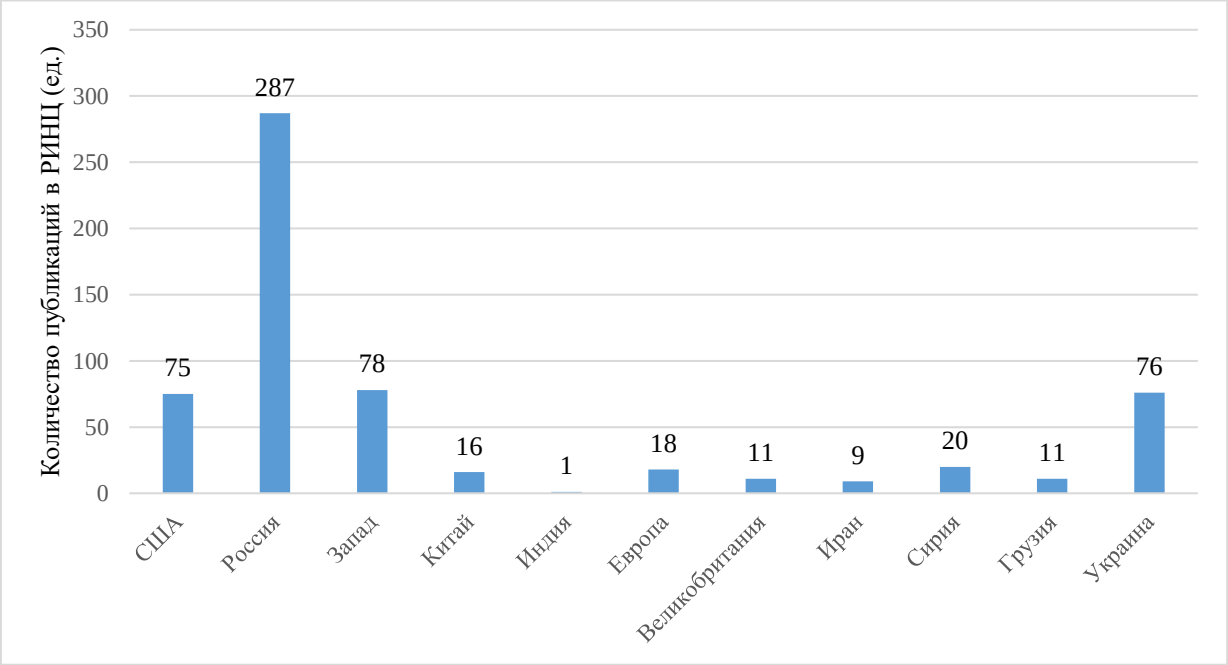

Рисунок 3.2 – Количество публикаций в РИНЦ (ед.) на август 2024 года по теме «информационная война» в сочетании с названием страны или группы стран в наименовании, ключевых словах или аннотации публикации

Источник: данные получены автором в августе 2024 года.

С учетом нагнетаемой в США и их союзниках антироссийской истерии, можно выдвинуть еще одно предположение – поскольку такие прокси-конфликты используются для генерации всплесков антироссийских настроений в западных обществах, политический «заказ» на исследование информационных войн в выгодном для «заказчиков» свете должен

способствовать значительному числу публикаций по информационным войнам и в этих обществах.

Предположим также, что, поскольку в информационную войну США также активно втягивают не только Россию, но и Китай, то китайские исследователи должны также уделять значительное внимание тематике информационных войн, причем это внимание должно с течением времени расти в количественном отношении, поскольку попытки США навязать информационную войну Китаю все более интенсифицируются.

Российская база научных публикаций РИНЦ для поиска ответа на такой вопрос уже не подходит, поэтому мы обратились к базе Scopus – это «единая библиографическая и реферативная база данных рецензируемой научной литературы».

Поисковый запрос мы сформулировали двумя словосочетаниями: *information war* и *information warfare*, поскольку в англоязычной литературе используются оба этих термина (чаще второй). Как и в случае с РИНЦ, мы задали такие условия поиска, чтобы по нему выдавались в качестве результата такие статьи, которые имеют хотя бы одно из двух этих словосочетаний в аннотации, ключевых словах, и/или названии статьи.

После этого для каждой найденной по данному запросу статьи учитывались аффилиации авторов с той или иной страной (а также с тем или иным учреждением в данной стране, но это был следующий этап поиска, на нем мы остановимся подробнее чуть ниже).

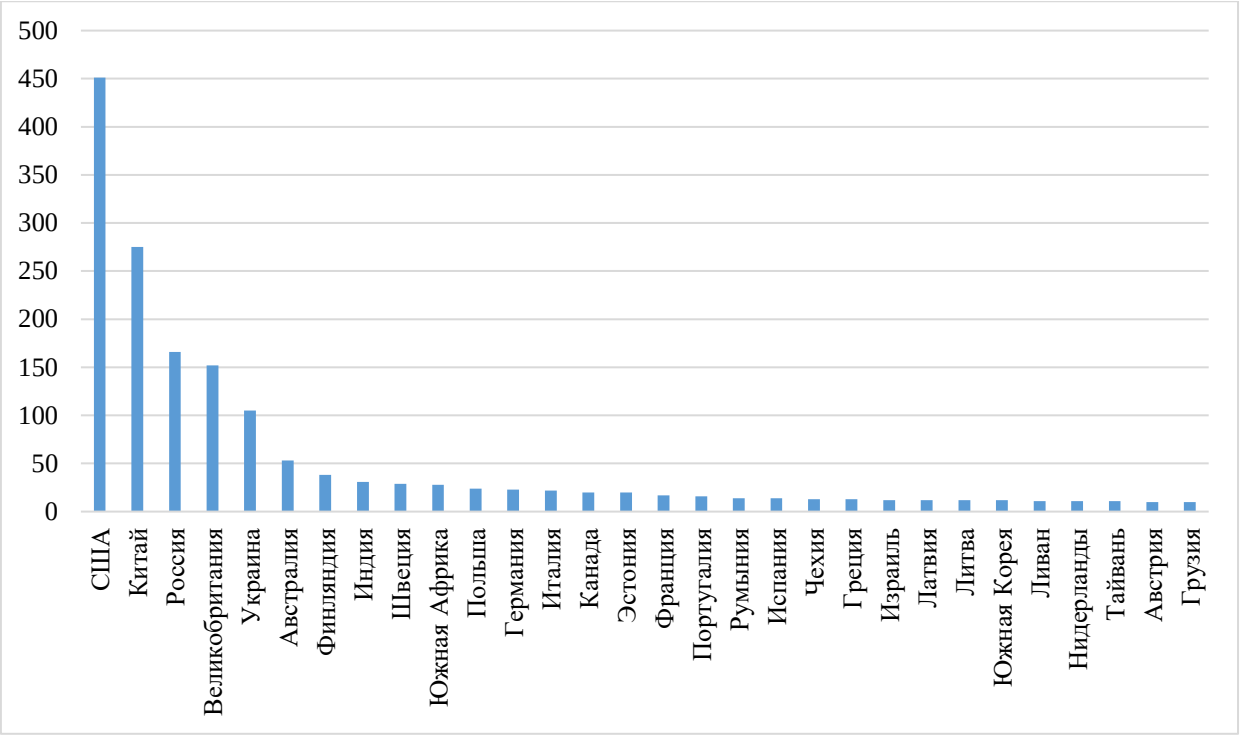

Рисунок 3.3 – Распределение числа публикаций в Scopus по теме «информационная война» (поиск по наличию словосочетания “information war” или “information warfare” в названии, ключевых словах или аннотации к статье)

Источник: данные получены автором по поиску в БД Scopus в августе 2024 года.

Рисунок 3.3 показывает характерную картину распределения внимания к информационным войнам в разных странах. Как и предполагалось, первое место по количеству научных публикаций по этой тематике занимает США – наиболее агрессивная в этом отношении страна, использующая самые разные приемы и технологии информационных войн для навязывания своей воли другим странам. Не вызывает удивления и четвертое место в «рейтинге» у Великобритании – страны, активно ведущей информационные кампании против РФ, равно как и пятое место у Украины.

Второе и третье места занимают Китай и Россия – два государства, которые США считают своими главными антагонистами и применяют весь арсенал оружия информационных войн – соответственно, Китай и Россия

должны пристально изучать этот арсенал для выработки адекватного ответа на разбойнические действия США и недопущения очернения своей репутации на международной арене и настраивания против себя стран мирового большинства.

Рассмотрим теперь, как изменялось ежегодное число публикаций по тематике информационных войн, публикуемых учеными трех ведущих в этом отношении стран – США, Китая и России (см. Рисунок 3.4).

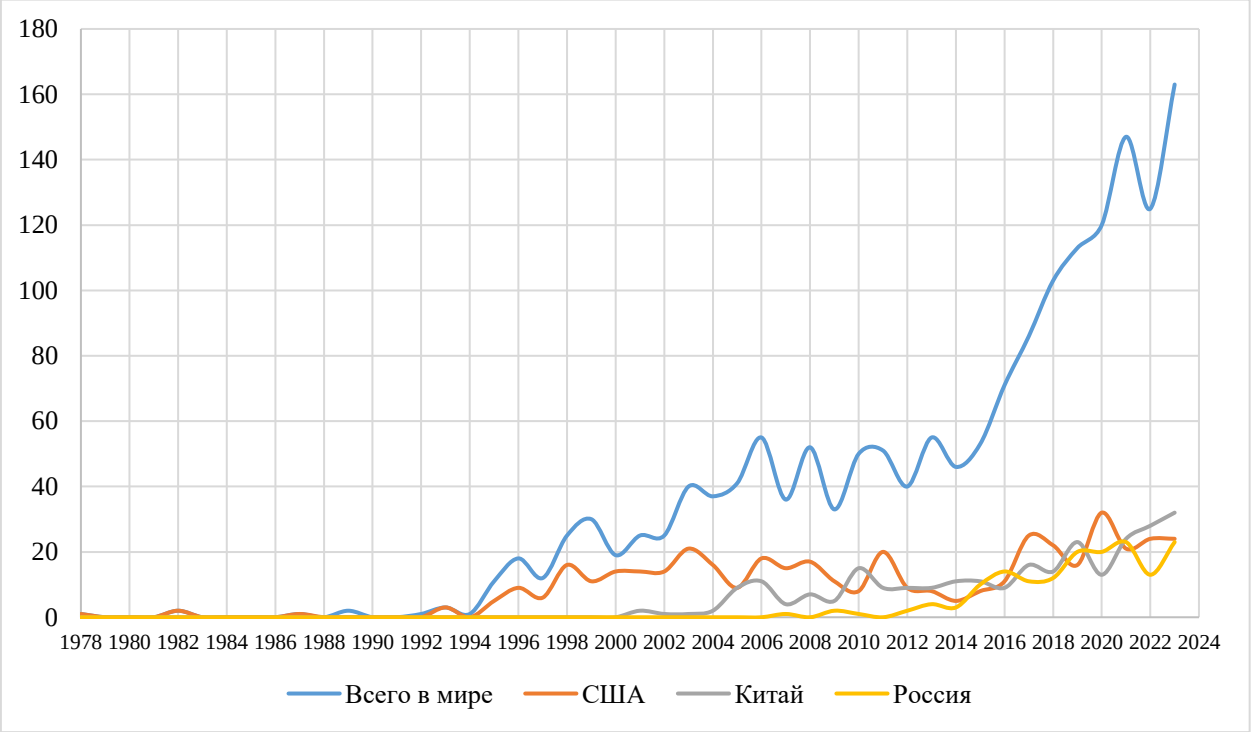

Рисунок 3.4 – Ежегодное число публикаций по теме «информационная война» – всего в мире и ученых 3 ведущих в изучении данной тематике странам (по годам)

Источник: данные получены автором по поиску в БД Scopus в августе 2024 года.

Из Рисунка 3.4 видно, что ежегодное число публикаций по информационным войнам начало стремительно увеличиваться с 2014 года, когда в мире начался новый виток обострения геополитических противоречий.

База данных Scopus дает возможность узнать аффилиацию автора не только со страной, но и с конкретным учреждением – научным, образовательным, «фабрикой мысли» и т.п. – к которому принадлежит автор той или иной публикации. Распределение исследователей из США представлено на Рисуноке 3.5.

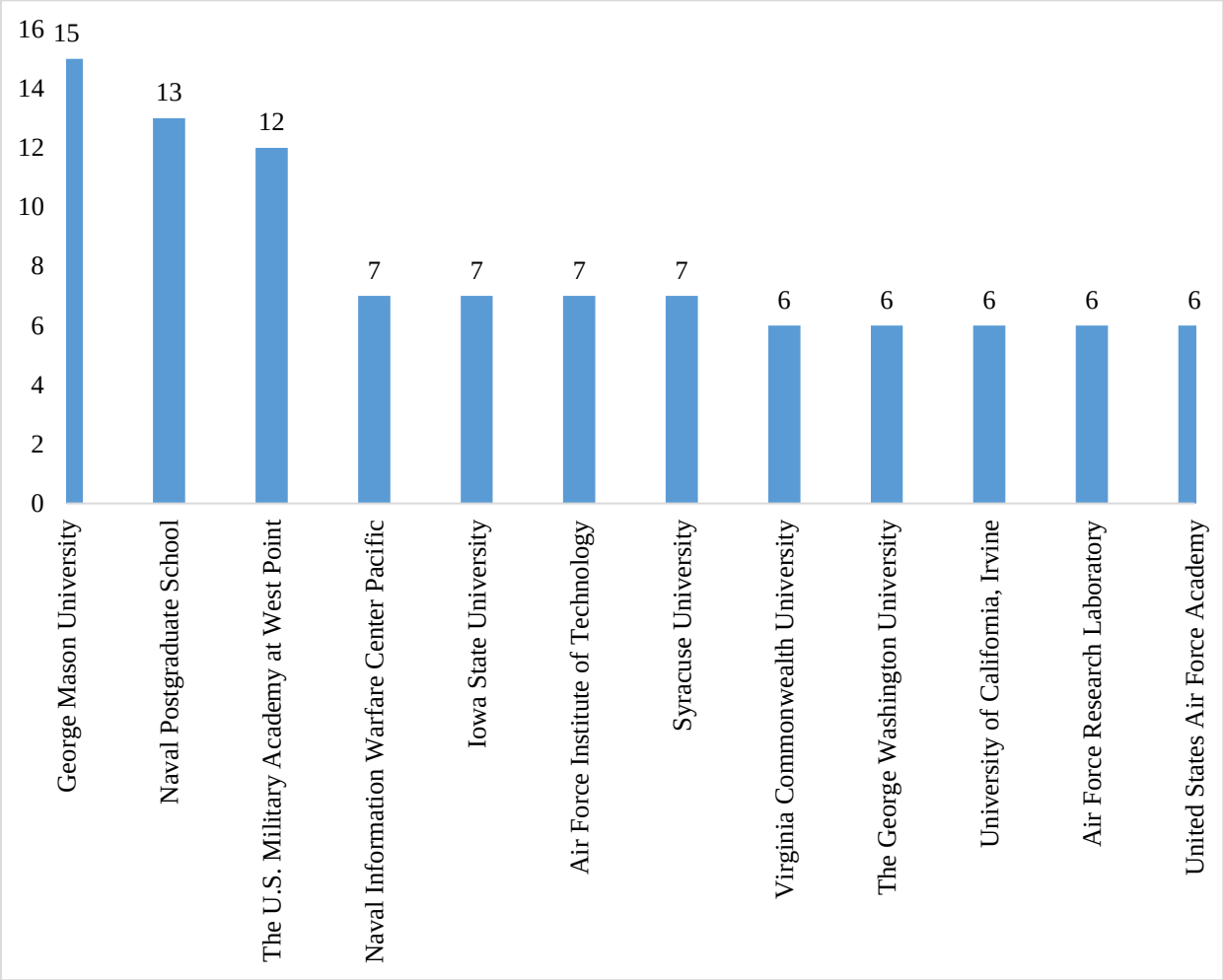

Рисунок 3.5 – Распределение авторов публикаций по тематике «информационные войны» из США по аффилиациям с различными американскими учреждениями

Источник: данные получены автором по поиску в БД Scopus в августе 2024 года.

Как ни парадоксально, наибольшее количество публикаций по информационным войнам, опубликованных американскими учеными, приходится на ученых из «гражданского» учебного заведения, а именно Университета Джорджа Мэйсона, входящего в топ-50 публичных

университетов США. Следующие три места занимают военные учреждения – Школа повышения квалификации офицерских составов ВМС, Военная академия США в Вест-Пойнте, Военно-морской Тихоокеанский центр информационных операций в компьютерных сетях; с этим центром делят четвертое место (имеют равное количество публикаций по информационным войнам) Университет штата Айова, технологический институт ВВС США, а также Сиракузский университет.

На Рисунке 3.6 представлено распределение авторов публикаций по тематике «информационные войны» из Китая по учреждениям.

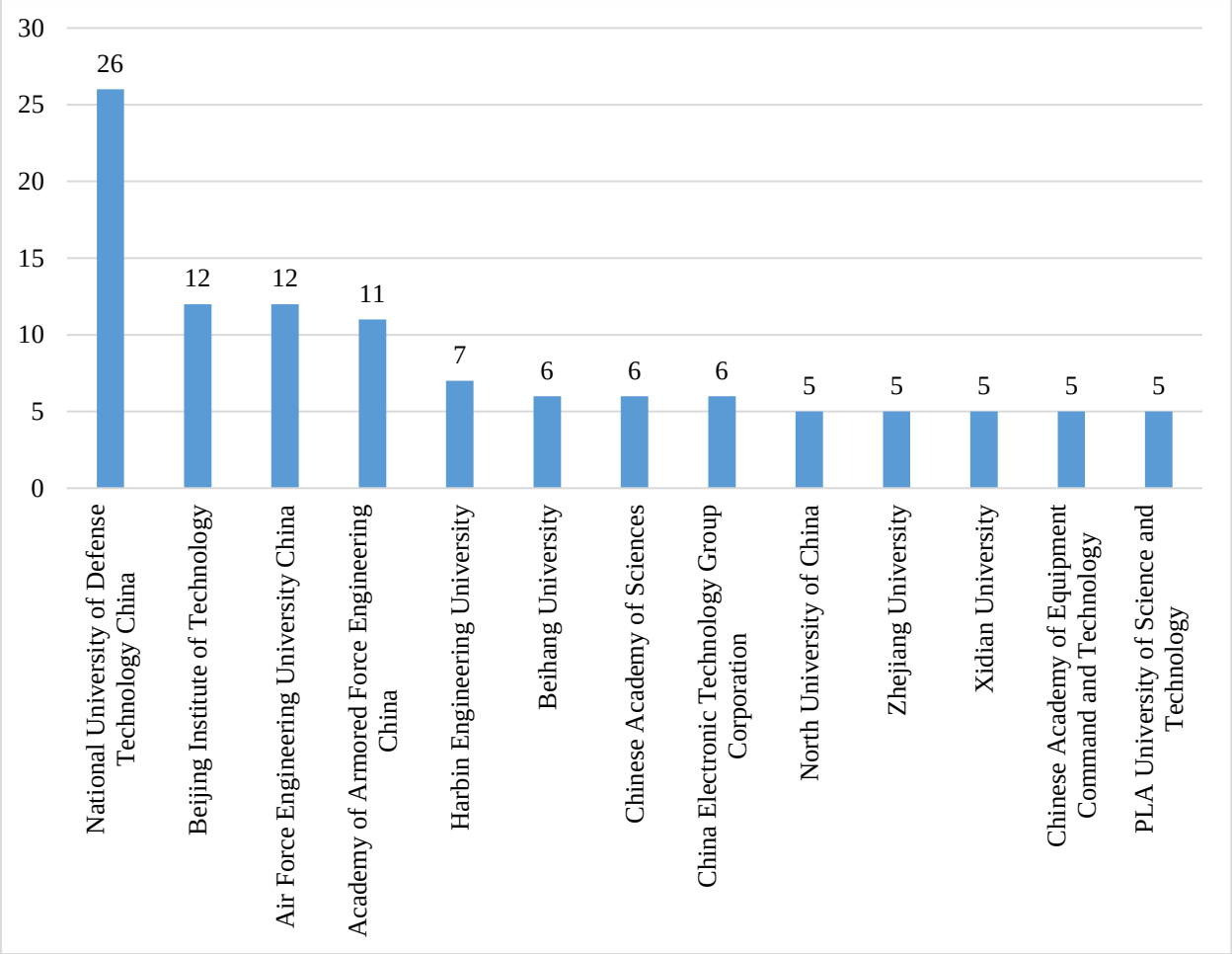

Рисунок 3.6 – Распределение авторов публикаций по тематике «информационные войны» из КНР по аффилиациям с различными учреждениями

Источник: данные получены автором по поиску в БД Scopus в августе 2024 года.

С большим отрывом от остальных учреждений – более чем в два раза – среди китайских учреждений, ученые и эксперты из которых публиковали исследования по информационным войнам, лидирует Национальный университет оборонных технологий Китая. Второе место делят Пекинский технологический институт и Инженерный университет ВВС КНР, на третьем располагается Инженерная академия бронетанковых сил КНР, за ней следует Харбинский инженерный университет. Преобладание военных и инженерных институтов в исследованиях информационных войн, проводимых в КНР, вполне оправданно и логично, потому что стране необходимы передовые технологии для отражения информационной агрессии США.

Рассмотрим теперь распределение по учреждениям российских ученых – авторов статей об информационных войнах, проиндексированных в системе Scopus. Это распределение представлено на Рисунке 3.7.

Первое место среди российских учреждений, ученые и эксперты из которых публиковали исследования по информационным войнам, занимает Российская академия наук – РАН. Второе – Санкт-петербургский государственный университет. Третье – Российский университет дружбы народов. Четвертое – Московский государственный университет имени М.В. Ломоносова. Наконец, пятое место занимает Институт прикладной математики и кибернетики имени М.В. Келдыша.

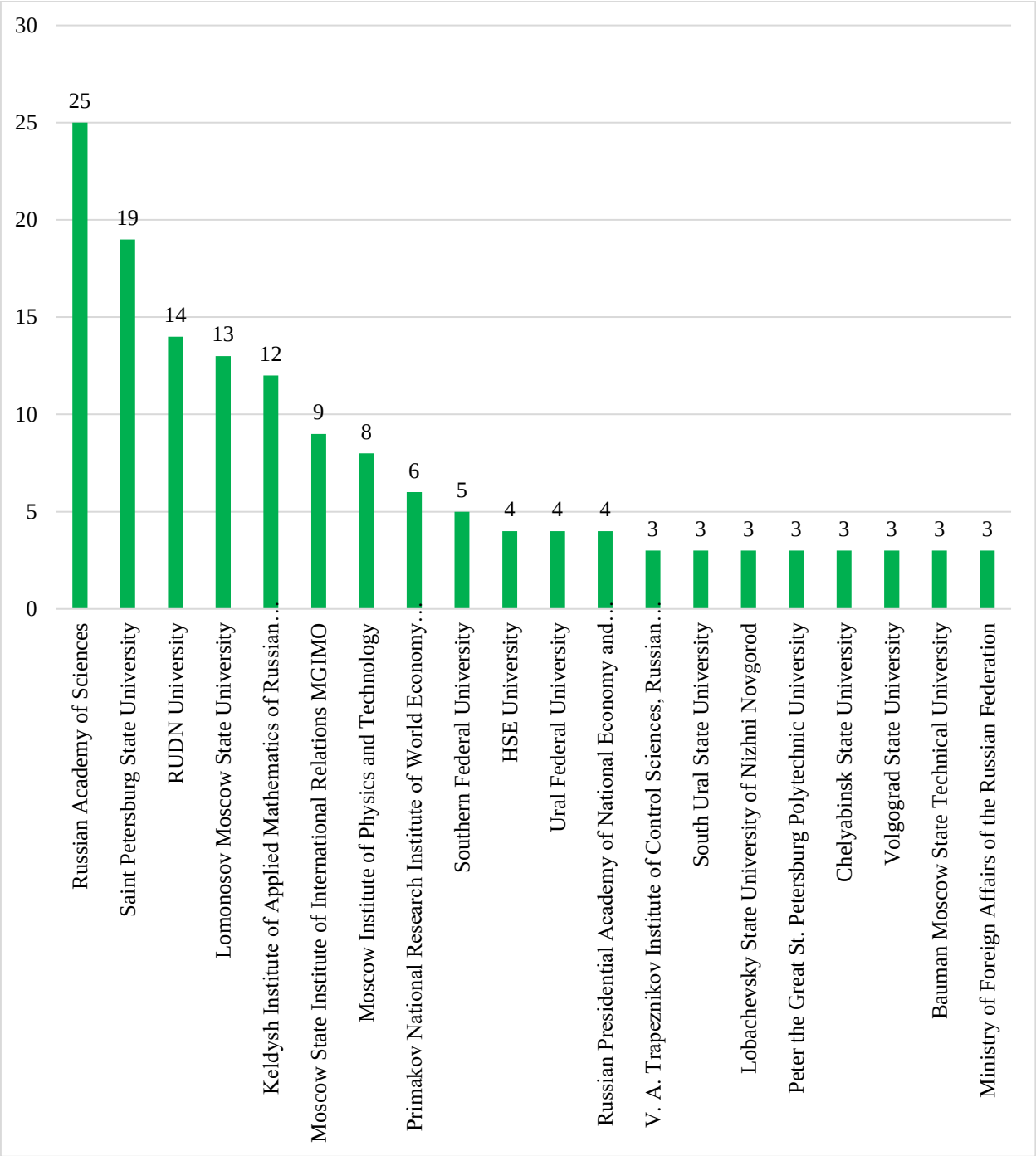

Рисунок 3.7 – Распределение авторов публикаций по тематике «информационные войны» из России по аффилиациям с различными российскими учреждениями

Источник: данные получены автором по поиску в БД Scopus в августе 2024 года.

Обращает на себя внимание разительное отличие структуры учреждений, ведущих в отношении исследования информационных войн, в России и Китае. Если в Китае преобладают учреждения инженерные и

оборонные, в России первые места занимают научные и образовательные учреждения, казалось бы, далекие от обороны. Однако дело в том, что Российская академия наук является «зонтичным» учреждением, объединяющим большое число научных институтов самой разнообразной направленности. Здесь представлены институты и точных, и естественных, и гуманитарных наук – в структуре Академии даже отдельно выделено Отделение нанотехнологий и информационных технологий. Соответственно, авторами статей по информационным войнам могут являться как сотрудники инженерных и технических институтов, так и, к примеру, специалисты по лингвистике и языкознанию (исследующие, например, языковые средства, используемые в публицистике, сопровождающей информационные войны). Отметим, что занявший пятое место Институт прикладной математики и кибернетики имени М.В. Келдыша также является институтом в составе РАН.

Такая «зонтичность» характерна и для двух ведущих вузов, МГУ имени М.В. Ломоносова и СПбГУ – они объединяют большое количество факультетов и кафедр, как точных, так и естественных, и гуманитарных наук. В меньшем масштабе это характерно и для РУДН.

Рассмотрим теперь картину распределения публикаций по информационным войнам по научным дисциплинам – см. Рисунок 3.8.

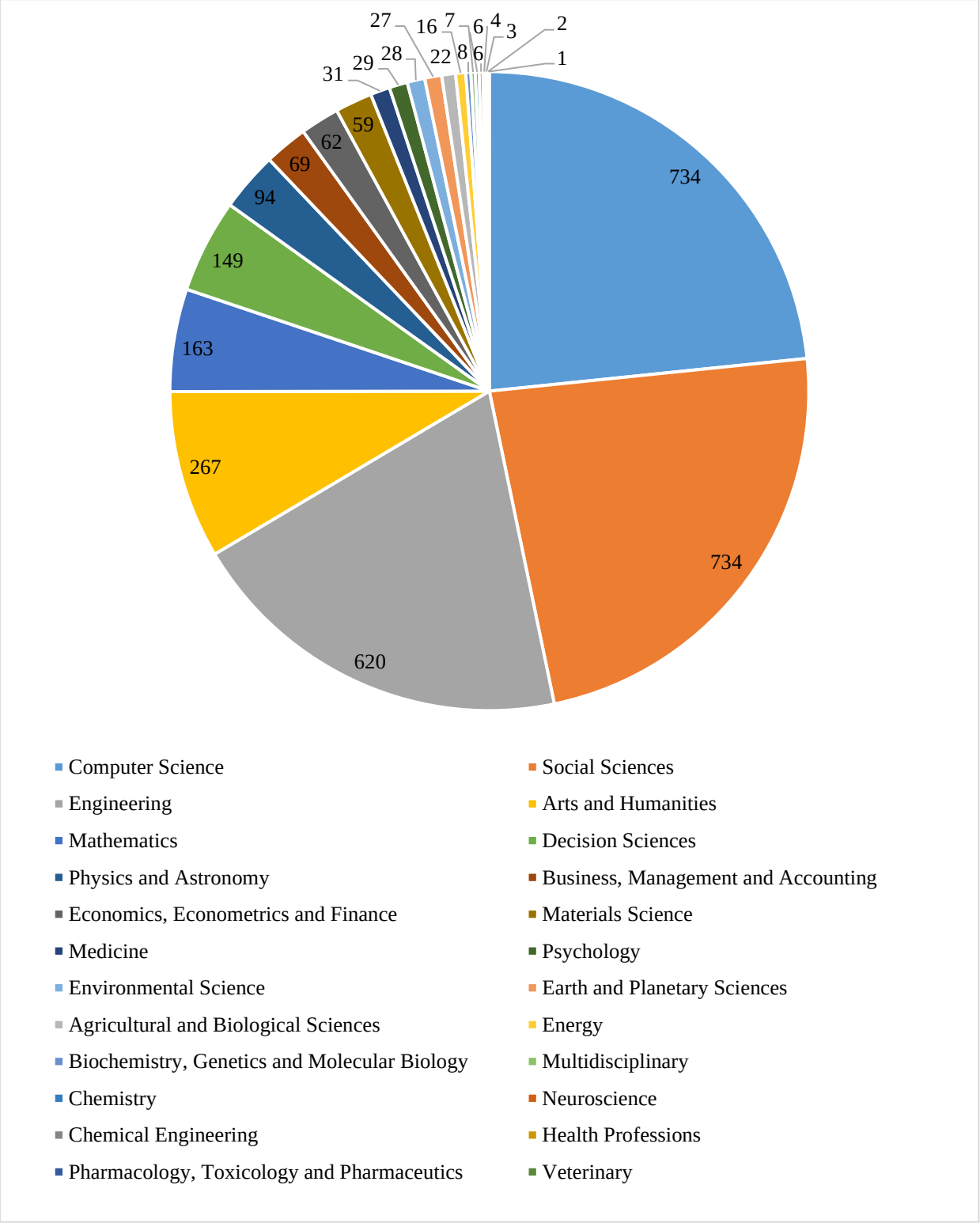

Рисунок 3.8 – Распределение публикаций по информационным войнам по научным дисциплинам, штук.

Источник: данные получены автором по поиску в БД Scopus в августе 2024 года.

Итак, по распределению научных публикаций по информационным войнам первое место делят две научные дисциплины – компьютерные науки

и общественные науки (по 734 тематических публикации в каждой), второе место занимают инженерные науки (620 тематических публикаций), третье с большим отрывом – гуманитарные науки (267 тематических публикаций), замыкают пятерку дисциплин математические науки (163 тематических публикации). Можно с уверенностью говорить о междисциплинарном характере научной проблематики информационных войн, вовлекающем не только компьютерные и информационные, но также гуманитарные технологии.

Для получения более точной картины рассмотрим динамику во времени числа научных публикаций, индексируемых базой Scopus, по двум ведущим в этом отношении дисциплинам – компьютерным наукам и социальным (общественным) наукам. Для этого представим на одном графике ежегодное число публикаций по информационным войнам в той и другой дисциплине – см. Рисунок 3.9.

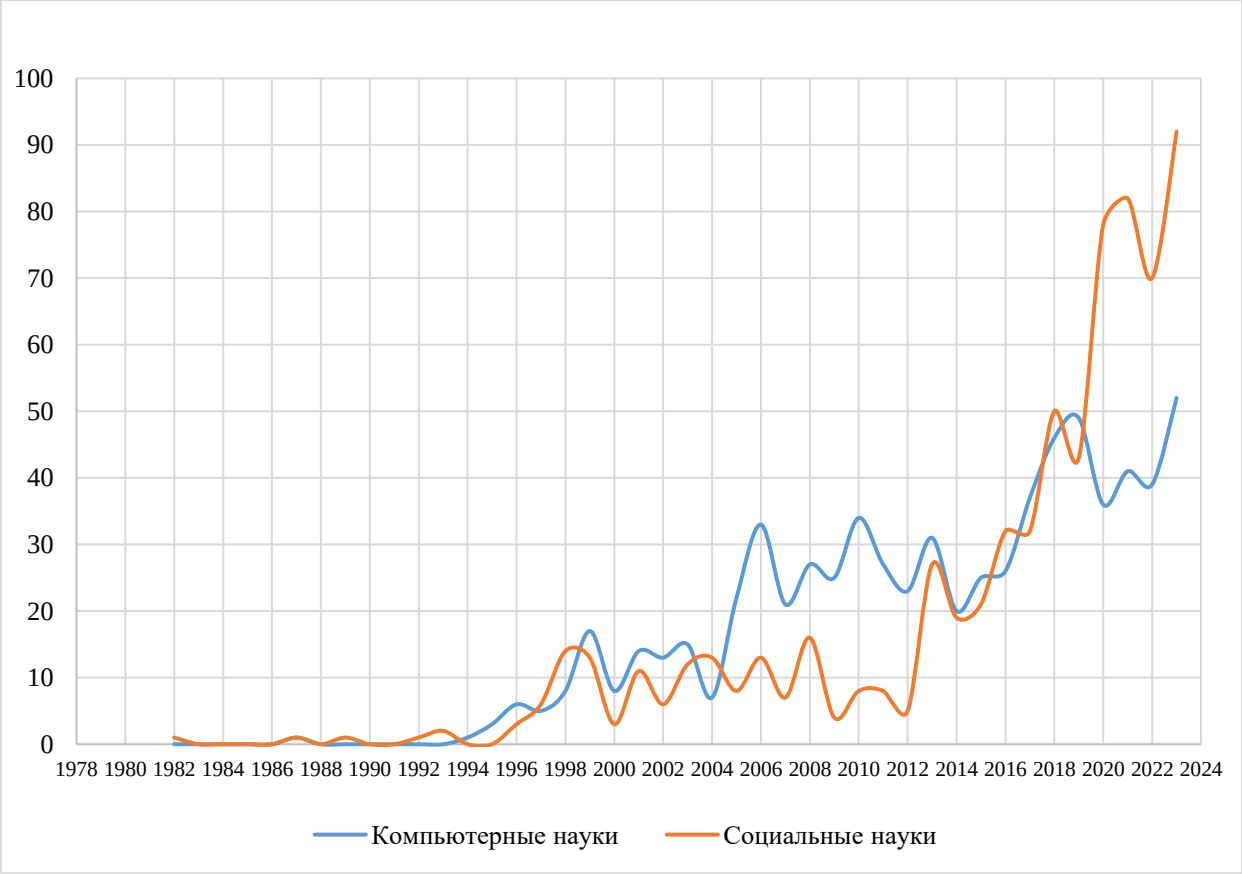

Рисунок 3.9 – Ежегодное число публикаций по теме «информационная война» в компьютерных и социальных (общественных) науках

Источник: данные получены автором по поиску в БД Scopus в августе 2024 года.

Из Рисунка 3.9 можно видеть, что число публикаций по информационным войнам в области компьютерных наук стало расти в середине и второй половине 1990-х годов, затем резко поднялось в 2004 – 2006 гг. и пережило еще один период быстрого роста в 2014 – 2019 гг. Число публикаций по информационным войнам в общественных науках оставалось относительно небольшим до 2012 года, когда совершило первый «скачок», после чего сравнялось с числом таковых публикаций в компьютерных науках и росло практически параллельно с ним (и одинаково быстро) в 2014 – 2019 гг. После этого происходит важное расхождение – число публикаций по интересующей нас тематике в компьютерных науках остается колебаться в пределах 35–50 публикаций в год, в то время как число таких публикаций в общественных науках демонстрирует стремительный взлет и в 2023 году превышает 90 единиц в год. Это свидетельствует о том, что акцент в изучении информационных войн смещается с технических аспектов на социогуманитарные технологии, применяемые в ходе таких кампаний.

Представляется, что этот процесс возглавили США, чем и объясняется лидирование общественного университета (а не военного) в изучении американцами информационных войн и написании статей по этой тематике. Это также подтверждает процитированное в начале параграфа определение информационных войн, данное НАТО, а именно его часть о социальных кибератаках, направленных на формирование у населения страны, против которой ведется информационная война, определенного образа мира, выгодного нападающей стороне.

3.2. Международное регулирование информационных войн и кибервойн

Современная информационная война разворачивается в основном в пространстве Интернета, ставшего с начала столетия практически общедоступным для большинства жителей планеты.

Интернет, несмотря на более чем 40-летнюю историю глобального распространения, остается весьма слабо отрегулированной сферой. Китай – уникальная страна, сразу получившая контроль над всеми входящими и выходящими потоками цифровой информации, для всех других стран фактически киберпространство остается достаточно прозрачным для высокоэффективных кибератак. Благодаря глобальной «свободе» внутри сети источник атак зачастую очень трудно или просто невозможно технически идентифицировать[179]. При этом, как показано в настоящей работе, самим объектом атак может быть сознание граждан, и зачастую быстро уточнить, какова природа и направленность этого воздействия, каковы его возможные последствие, для структур безопасности является сложным [180] . Международная информационная безопасность на сегодня в основном обеспечивается активными действиями отдельных стран в предотвращении и противостоянии конкретным военно-политическим угрозам, которые также включают внешнее деструктивное воздействие на их население и защиту своего киберпространства и связанной с ним критической инфраструктуры, противостоянию киберпреступности, в том числе, международной[181].

Внутри отдельных интеграционных политических, политико-экономических, военно-политических блоков и объединений решение данных проблем происходит относительно более просто. К таким кейсам

---

[179] Павловский А. А. Некоторые аспекты угроз информационной безопасности в международной сфере // Информационная безопасность как составляющая национальной безопасности государства: материалы Междунар. науч.-практ. конф., Минск, 11–13 июля 2013 г. : в 3 т. / Ин-т нац. безопасности Респ. Беларусь; редкол. С. Н. Князев (гл. ред.) [и др.]. Минск, 2013. Т. 2. С. 105–109.

[180] Довгань Е. Ф., Мороз Н.О. ОДКБ и информационная безопасность // Организация Договора о коллективной безопасности и планирование на случай чрезвычайных обстоятельств после 2014 г. / Е. Ф. Довгань, А. В. Русакович (ред.). Женева – Минск: Женевский центр демократического контроля над вооруженными силами, Центр изучения внешней политики и безопасности, 2015. С. 207–236.

[181] Мороз Н.О. Международно-правовые основы обеспечения международной информационной безопасности // Труд. Профсоюзы. Общество. 2016. № 1 (51). С. 77–81.

можно отнести взаимодействие внутри ОДКБ, НАТО, ШОС, ЕС и др. Так, работают Консультационный координационный центр ОДКБ по вопросам реагирования на компьютерные инциденты, Комитет по кибероборонеНАТО, Управление НАТО в сфере кибероборонеы, Агентство по коммуникациям и информации НАТО и созданный в его рамках Центр по реагированию на киберугрозы, Агентство по сетевой и информационной безопасности Европейского союза, Европейский центр по киберпреступности (Европол). В то же время, всеобщие, глобального масштаба договора и соглашения на этот счет отсутствуют[182].

Информационная сфера, несмотря на имеющееся колоссальное технологическое неравенство, в том числе – в области цифровизации между развитыми и большинством развивающихся стран – обеспечивает не только уязвимость более слабых в технологическом отношении, но и аналогичную, если не большую уязвимость сильных, зависимых от цифровизации в гораздо большей степени. Данное обстоятельно является стимулом к договоренностям – так, на женевской встрече президентов в России и США в июне 2021 года американская сторона, понимая его, проявила стремление к заключению международных отношений по регулированию киберпространства[183].

В начале марта 2022 года в ООН состоялась субстантивная сессия Специального межправительственного комитета ООН по разработке всеобъемлющей международной конвенции по противодействию использованию информационно-коммуникационных технологий в преступных целях. Данный процесс был начат именно по инициативе России[184]. В мае 2022 года Группа правительственных экспертов ООН по продвижению ответственного поведения государств в киберпространстве в

---

[182] Мороз Н.О. Международно-правовые основы обеспечения международной информационной безопасности // Труд. Профсоюзы. Общество. 2016. № 1 (51). С. 77–81.

[183] Встреча с Президентом США Джозефом Байденом// Официальный Интернет-сайт Президента России. 7.12.2021. URL: http://www.kremlin.ru/events/president/news/67315 (дата обращения: 1.09.2022).

[184] О первой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности / Сайт Министерства иностранных дел Российской Федерации. 12.03.2022 URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1803908/ (дата обращения: 1.09.2022).

контексте международной безопасности представила и получила одобрение на соответствующий доклад. Причем эта группа была создана по инициативе США еще в 2018 году. Активно функционирует и рабочая группа ООН открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, сформированная также по инициативе России во исполнение резолюции ГА ООН 75/240[185].

Россия – одна из самых активных стран в стремлении к обеспечению международной информационной безопасности. Еще в январе 2021 годы был разработан и утвержден документ в этой сфере о Диалоге Россия-АСЕАН. Более успешно развивается взаимодействие со стратегическими партнерами России по СНГ, ОДКБ и ШОС. К 2024 году Россией заключено 11 соответствующих межправительственных соглашений, включающих договора с такими странами как Иран и Киргизия, прозвучало 6 совместных двусторонних и многосторонних заявлений глав государств[186].

Как было показано выше, кибератакам подвергаются как государственные структуры, так и бизнес[187], это создает значительные барьеры для совместного использования данных при формировании системы цифрового управления экономическими процессами, а также непосредственные политические угрозы, в том числе, прямые угрозы национальной безопасности.

По мере «восхождения» стран Глобального Большинства растут внутренние противоречия и проблемы в странах коллективного Запада, источники которых находятся внутри самой западной системы, однако, ответственность за происходящие благодаря им политические конфликты

---

[185] Об итогах деятельности Группы правительственных экспертов ООН по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности / Сайт Министерства иностранных дел Российской Федерации 02.06.2021 URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1423809/ (дата обращения: 1.09.2022).

[186] Интервью директора Департамента международной информационной безопасности МИД России А.В.Крутских «Глобальная киберповестка: дипломатическая победа» журналу «Международная жизнь», 7 июня 2021 года / Сайт Министерства иностранных дел Российской Федерации. 08.06.2022. URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1752094/ (дата обращения: 1.08.2022).

[187] Hampson F. O., Jardine E. Look Who’s Watching: Surveillance, Treachery and Trust Online. Waterloo, ON, Canada: Centre for International Governance Innovation, 2016. 364 p.

правящие круги этих стран пытаются переложить на «враждебную» информационную деятельность Китая и России. В 2022 году в ЕС вступил в силу Закон о цифровых услугах [188] , открывающий правительствам и спецслужбам доступ к платформам и возможность модерации контента. Данный закон активно используется в преследовании политических оппонентов европейских элит, так, в Румынии был отменен первый тур выборов в 2024 году из-за якобы российского вмешательства в выборы через «китайский» TikTok.

Глобальный цифровой договор, принятый ООН в сентябре 2024 году (но не поддержанный Россией и Китаем), несмотря на якобы прогрессивные цели, так и не нашел баланс между уважением государственного суверенитета, правами человека, коммерческими интересами и интересами гражданского общества в киберпространстве, а также делает слишком большой и непонятный многим упор на гендерную тематику[189].

Уже в декабре 2025 года состоится Всемирная встреча на высшем уровне по вопросам информационного общества готовится к кардинальному обновлению принципов управления глобальным Интернетом. ООН признает необходимость к стремлению к регулированию Интернета, при этом в качестве основного рассматривается так называемый «мультистейкхолдерный подход», как та модель позволяла техническим экспертам, правительствам, бизнесу и гражданскому обществу совместно принимать решения о развитии глобальной сети. На первом плане стоит вопрос о контроле технической архитектуре Интернета. В настоящее время этим занимаются Корпорация по присвоению имен и номеров в Интернете (ICANN), 5 региональных Интернет-Регистратур и Целевая группа по инженерным задачам интернета (IETF), работающим на основе консенсуса технического сообщества. Однако, развивающиеся стран требуют большего

[188] REGULATION (EU) 2022/2065 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (дата обращения: 1.10.2025)

[189] Зиновьева Е. Что не так с Глобальным цифровым договором?// РСМД, 31 октября 2024 URL:https://russiancouncil.ru/analytics-and-comments/analytics/chto-ne-tak-s-globalnym-tsifrovym-dogovorom/ (дата обращения: 1.10.2025).

контроля над внутренним киберпространством. Несмотря на критику ведущих стран Глобального Большинства, прежде всего, России Глобального цифрового договора, данный Договор сделал возможным более активное участие отдельных стран в управлении внутренним киберпространством. При этом сам технологический прогресс – развитие технологий ИИ, квантовых вычислений – формирует новые обстоятельства, важные для учета в развитии регулирования. В целом, от принятых решений в декабре 2025 года зависят стратегические перспективы развития Интернета[190].

В целом, международный диалог по кибервопросам остается сложным. Нынешнее состояние дел в области международной кибербезопасности остается запутанным. В отличие от войны в физическом пространстве, война в киберпространстве не подразумевает формального объявления войны. Это создает условия для распространения кибервойн. Однако, учитывая, что кибербезопасность включает в себя информационную, разведывательную и национальную безопасность, страны осторожны. Многие страны держат свои действия в области кибербезопасности в секрете, что ведет к недостатку прозрачности и усложняет диалог.

В данной ситуации страны редко обмениваются информацией в области кибербезопасности, что оставляет много места для недоразумений и неправильных толкований. Продолжает оставаться сложным достижение дипломатического компромисса между странами, чтобы избежать кибератак и установить взаимное доверие.

Практика подтверждает это пессимистическое предположение. Например, США редко прибегают к дипломатии и переговорам, вместо этого используя кибератаки как средство стратегического давления. Когда страны подвергаются кибератакам, они отвечают ответными атаками, вместо поиска дипломатических решений. Даже в обозримом будущем эта ситуация вряд ли изменится значительно.

---

[190] ООН пересматривает принципы интернет-управления через 20 лет// DIGITAL-REPORT, 26.05.2025. URL:https://digital-report.ru/oon-peresmotrit-printsipy-internet-upravleniya/ (дата обращения: 1.10.2025)

Поэтому вопрос о том, как правильно сбалансировать различия в кибернаступательных и кибероборонительных возможностях между странами и сохранить разумное и сдержанное поведение в условиях «необъявленной войны», остается значительной практической проблемой, которая продолжает испытывать мудрость политиков разных стран.

В международном праве ведутся активные дебаты относительно кибервойны как новой формы военных действий. Законодательство в области кибервойны значительно отстает от реальной практики. Одной из наиболее интуитивных характеристик войны остается "применение силы." Статья 11 Таллиннского руководства определяет применение силы в контексте кибератак следующим образом: «Кибероперация представляет собой применение силы, если её последствия и масштаб соизмеримы с уровнем силы, применяемой в некибернетической операции».

Однако здесь следует подробнее остановиться на том, что по сути своей представляет из себя Таллиннское руководство – это результат многолетнего проекта под эгидой НАТО, стартовавшего с 2009 году. В рамках проекта западные эксперты по международному праву изучали, как существующие нормы и принципы международного права могут применяться к кибернетической войне, «включая как право, регулирующее применение силы в межгосударственных отношениях (jus ad bellum), так и право, регулирующее ведение международных и немеждународных вооруженных конфликтов (jus in bello). Оно не касается деятельности в кибернетическом пространстве, не достигающей порога «применения силы» (jus ad bellum) или вооруженного конфликта (jus in bello)»[191]. Этот документ содержит 95 правовых норм, основанных на международном праве, регулирующем «традиционные» конфликты, и адаптирующих его для конфликтов в киберпространстве. Однако этот документ не является юридически обязательным и не обязательно выражает взгляды и мнения

[191] Schmitt M. (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013. 300 p.

НАТО или любой другой организации или государства, но лишь коллектива экспертов, участвовавших в его разработке.

Документ получил продолжение в 2017 году, когда был разработан документ «Таллинн 2.0». Основное внимание в оригинальном Руководстве уделяется наиболее разрушительным кибернетическим операциям, которые квалифицируются как «вооруженные нападения» и, следовательно, позволяют государствам реагировать в порядке самообороны, а также тем, которые происходят во время вооруженного конфликта. В «Таллин 2.0» говорится об «информационных операциях», а не о «конфликтах». Однако и в этом продолжении остается значительное число нерешенных вопросов, решение которых является принципиальным для правового регулирования информационных (особенно информационно-психологических) войн. В документе отмечается, что для того, чтобы «конфликт назывался «вооруженным», нет необходимости, чтобы в нем были задействованы вооруженные силы», но при этом остаются непонятными другие критерии отнесения конфликта к вооруженному. Документ дает лишь весьма расплывчатое определение: «Международный вооруженный конфликт имеет место, когда существуют враждебные действия между двумя или более государствами, которые могут включать в себя или ограничиваться операциями в киберпространстве». Более конкретный характер имеет определение кибернетического нападение (cyber attack) – оно «представляет собой операцию в киберпространстве, которая может носить наступательный или оборонительный характер и целью которой является причинить вред или вызвать смерть людей или причинить ущерб или разрушить объекты». Тем не менее, этот документ также не имеет обязательного характера.

В 2011 году была опубликована Международная стратегия правительства США для киберпространства, в которой утверждается, что американские военные могут, при наличии неизбежного конкретного ущерба, применить силу. В этой стратегии правительства США подтвердили, что американские военные могут использовать "превентивную" силовую

защиту в ответ на потенциальные последствия кибератак. С другой стороны, Россия долгое время настаивает на том, что кибератака равносильна применению силы, поскольку, по сути, представляет собой замаскированную форму нападения, способную нанести непосредственный ущерб и повреждение противнику, сопоставимые с огневыми атаками. В общем и целом, несмотря на разногласия между странами по деталям кибератак, большинство стран признают, что кибератака может рассматриваться как «применение силы».

Тем не менее, несмотря на то что на данный момент низкая интенсивность и контролируемый характер кибервойны делают ее отчасти более «гуманной» по сравнению с «традиционными» боевыми действиями, это не гарантирует, что в будущем кибервойны не приведут к массовым человеческим жертвам. Использование кибероружия для атаки критически важных объектов гражданской инфраструктуры или даже для манипуляции оружием массового поражения не является исключением.

Проблема заключается в том, что, в отличие от физического пространства, где существует соглашение между государствами относительно базовых норм международного права во времена военных конфликтов, таких как запрет на биологическое оружие, химическое оружие, пытки и другие, в киберпространстве ситуация иная. В настоящее время кибервойны являются новым, быстро эволюционирующим явлением в международном праве, и развитие законодательства не поспевает за ними. К тому же международное сообщество пока не достигло общего согласия по базовым правилам проведения кибервойны, что затрудняет установление законодательных норм, регулирующих кибервойны. В настоящее время существует недостаточно правил для проведения кибервойны, и многие страны действуют без особого раздумья и принципов в сфере кибервойн. В этом контексте разработка Женевской конвенции в области киберпространства является неотложной необходимостью, и ее разработка требует совместных усилий международного сообщества.

Что касается текущей ситуации в кибервойнах, несмотря на увеличивающееся количество атак на информационную инфраструктуру, страны по-прежнему отвечают на кибератаки в основном через интернет, и пока нет случаев, когда кибервойна привела к реальным военным действиям. Тем не менее, это не означает, что кибервойна не может перейти в физическое пространство. Более вероятный сценарий заключается в том, что, когда две стороны в кибервойне находятся на неравных позициях в атаке и защите, и доминирующая сторона наносит больше вреда людям и имуществу другой стороны через киберпространство, другая сторона может ответить силовыми действиями в физическом пространстве.

Эта дилемма усугубляется сложностью отслеживания источника кибератак. Если сторона подвергается кибератаке и не может однозначно определить ее происхождение, то обычно первым подозреваемым становится страна, обладающая возможностями для осуществления таких атак. Исторически западные страны, подвергшиеся кибератакам, часто подозревали Китай и Россию в причастности к этим атакам. Такой метод выявления источника атаки, основанный на возможностях, а не на фактических доказательствах, может усугубить стратегические подозрения между государствами. В этом контексте даже небольшое и изолированное событие в киберпространстве может иметь катастрофические последствия.

На данный момент нельзя отрицать, что кибервойна не обладает разрушительной мощью, сравнимой с традиционными видами войны, и она может казаться более «гуманной» в своем подходе. Однако важно не впадать в безосновательный оптимизм и не полагать, что кибервойна каким-то образом устраняет вечную проблему войны, существующую в человеческом обществе на протяжении тысячелетий. На самом деле, в этой новой форме войны насильственная сущность войны (как физической, так и духовной) принципиально не изменилась. Скорее наоборот, кибервойна сделала войну гораздо более сложной и непредсказуемой.

Быстрое развитие новых технологий изменяет наше общество и оказывает влияние на вопросы безопасности и военный ландшафт. В современных вооруженных конфликтах использование кибертехнологий стало реальностью. Кибероперации обладают специфическими техническими характеристиками и могут иметь гуманитарные последствия, особенно в случаях, когда кибератаки направлены на медицинский сектор или другие критически важные объекты гражданской инфраструктуры, такие как электроснабжение, водоснабжение и санитарные системы, что может повлечь серьезные негативные последствия для гражданского населения. Поэтому для обеспечения защиты гражданского населения и гражданской инфраструктуры во вооруженных конфликтах важно признать, что кибервойна не является правовой лакуной, а регулируется международным правом, включая Женевские конвенции. Тем не менее, характеристики этой новой технологии создают ряд сложностей при интерпретации правил международного гуманитарного права).

Цифровая трансформация также оказывает влияние на безопасность и военный ландшафт как внутри стран, так и на международном уровне. В последние несколько лет наблюдается значительный рост кибервойн против частных компаний и правительств. Эти действия оказывают влияние как в киберпространстве, так и в реальном мире: они нарушают работу ключевых инфраструктурных систем, таких как электроснабжение или медицинское обслуживание, и причиняют физический ущерб определенным объектам. В целом, такие атаки обходятся правительствам и частному сектору в миллиарды долларов. Использование кибертехнологий также стало частью современных вооруженных конфликтов. Хотя многие кибероперации часто называют «кибератаками», важно подчеркнуть, что большинство из них не имеют прямого отношения к вооруженным конфликтам. Тем не менее, некоторые государства заявляют, что киберсредства использовались в современных вооруженных конфликтах, и все больше государств утверждают, что они развивают свой кибервоенный потенциал.

Примеры использования кибервойны в вооруженных конфликтах включают следующие аспекты: шпионаж; определение важных целей; информационную войну с целью воздействия на моральное состояние и боевой дух противника; блокирование, подмену или создание дезинформации в коммуникационных системах противника с целью дезориентировать его силы и средства; а также проведение кибероперaций в поддержку реальных боевых действий. Примером последнего является отключение военных радиолокационных станций противника для поддержки воздушных атак.

С быстрым развитием кибертехнологий и их потенциальной человеческой ценой в вооруженных конфликтах существует необходимость в их постоянном мониторинге и оценке.

Использование киберсредств в качестве средства или метода ведения войны предоставляет военным возможность достижения своих целей без необходимости причинения непосредственного физического вреда гражданскому населению или гражданским объектам. В зависимости от обстоятельств, кибероперации с большей вероятностью, чем использование других средств ведения войны, могут снизить предсказуемый побочный ущерб гражданским объектам при нанесении ударов по военным целям.

Однако кибероперации, произошедшие в последние несколько лет (в основном не связанные с вооруженными конфликтами), показали, что кибератаки могут повлиять на предоставление гражданских услуг и состояние ключевых объектов гражданской инфраструктуры. Это выявляет уязвимость таких услуг, включая сектор здравоохранения, который подвержен особой опасности из-за своей цифровой трансформации и повышенной уязвимости к кибератакам. Подобным образом, критически важная гражданская инфраструктура, такая как системы электроснабжения, водоснабжения и канализации, также может быть подвержена риску, особенно при атаках на промышленные системы управления. Хотя атаки на такие системы не происходят так часто, как другие виды кибероперaций, их

частота возрастает, и серьезность угрозы развивается быстрее, чем предполагалось несколько лет назад.

В условиях вооруженного конфликта международное гуманитарное право обеспечивает полную защиту медицинского сектора и запрещает нападения на гражданскую инфраструктуру, за исключением случаев, когда объект становится военной целью. По крайней мере три фактора, характерные для киберпространства, вызывают дополнительные опасения:

1) Сложность приписывания кибератак государству или негосударственному субъекту, что затрудняет выявление нарушителей международного гуманитарного права (МГП) в киберпространстве и привлечение их к юридической ответственности.

2) Риск распространения вредоносных киберсредств и технологий, что может усилить возможность их неправомерного использования.

3) Риск чрезмерной реакции и эскалации в кибероперациях, так как объекту атаки часто трудно определить, какие цели преследует злоумышленник.

Потенциальные гуманитарные последствия кибероперацій пока не изучены подробно с учетом быстрого развития кибертехнологий и эволюции средств и методов ведения войны в киберпространстве. Важно учитывать, что несмотря на низкий уровень гуманитарных издержек на текущий момент, динамика развития кибероперацій неопределенна, и поэтому требует более пристального наблюдения.

Применение МГП к кибероперациям вооруженного конфликта остается спорным вопросом. Однако использование новых и развивающихся технологий в кибероперациях не исключает возможности применения МГП, когда эти технологии используются как средства и методы ведения войны в рамках вооруженного конфликта. МГП защищает гражданское население и гражданские объекты от последствий военных действий, ограничивая выбор средств и методов ведения войны воюющими сторонами, независимо от правомерности применения силы.

Факт, что МГП применимо, не препятствует государствам продолжать развивать и усовершенствовать МГП, соглашаться о добровольных нормах или работать над общим толкованием существующих норм. Например, при создании Открытой рабочей группы по безопасности при использовании информационно-коммуникационных технологий в 2018 году, Генеральная Ассамблея ООН приветствовала набор международных правил, норм и принципов ответственного поведения государств (всего 13), разработанных Группой правительственных экспертов ООН за несколько лет.

Другим примером потенциальных новых норм в области информационной безопасности является Международный кодекс поведения по информационной безопасности, представленный в ООН в 2011 году Китаем, Российской Федерацией, Таджикистаном и Узбекистаном, который обязывает государства воздерживаться от распространения информационного оружия и связанных с ним технологий.

В январе 2015 г. государствами-членами ШОС внесены в качестве официального документа ООН «Правила поведения в области обеспечения международной информационной безопасности (МИБ)». Документ опирается на подходы, заложенные в проекте «Правил поведения в области обеспечения МИБ», распространенном от имени государств-членов ШОС в ходе 66-й сессии Генеральной Ассамблеи ООН в 2011 г.[192] В этом документе «закреплено обязательство государств не применять информационно-коммуникационные технологии в целях нарушения международного мира и безопасности, а также для вмешательства во внутренние дела других государств и подрыва их политической, экономической и социальной стабильности»[193], то есть речь идет не о регулировании кибервойн, а об их предотвращении в принципе.

---

[192] Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря / ГА ООН. Шестьдесят девятая сессия Пункт 91 повестки дня Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https://www.mid.ru/ru/foreign_policy/un/organs/1582262/ (дата обращения 06.11.2024).

[193] Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» // МИД РФ. 29.01.2015. URL:

Что касается МГП, вопрос о том, как применяются существующие принципы и правила, требует более глубокого обсуждения. Необходимо оценить их адекватность и, при необходимости, внести коррективы на основе существующего права. Признание применимости МГП к кибероперациям, связанным с вооруженным конфликтом, представляет собой лишь первый шаг. Специфика этой новой технологии создает ряд проблем при интерпретации норм МГП (включая нормы о применении оружия), которые требуют специального обсуждения и разработки.

МГП применяется только к кибероперациям, которые являются частью вооруженного конфликта или связаны с ним, а также к кибероперациям, которые в рамках определенных контекстов могут рассматриваться как вооруженный конфликт (хотя такие случаи в настоящее время маловероятны). Если кибероперации происходят в контексте существующего международного или немеждународного вооруженного конфликта, который проводится реальными средствами, соответствующее международное гуманитарное право может регулировать такие операции.

Отдельный вопрос заключается в том, может ли МГП регулировать отдельные кибероперации (без фактических вооруженных действий), когда эти действия не связаны с текущим вооруженным конфликтом. Этот вопрос требует анализа с учетом общих статей 2 и 3 Женевских конвенций 1949 года, которые регулируют международные и немеждународные вооруженные конфликты. Эти два типа вооруженных конфликтов различаются по характеру участвующих сторон и уровню насилия. Что касается международных вооруженных конфликтов, МККК не видит оснований для различения между одной или несколькими кибероперациями, приводящими к уничтожению гражданского или военного имущества, гибели или ранению солдат или гражданских лиц, и аналогичными атаками, осуществляемыми с использованием более традиционных средств и методов ведения войны.

---

https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1582268/ (дата обращения 06.11.2024).

Однако вопрос о том, подпадают ли отдельные кибероперации (которые не связаны с текущим вооруженным конфликтом, не включают фактических вооруженных действий и не имеют последствий, аналогичных реальным вооруженным операциям – например, кибероперации, которые лишь мешают, но не разрушают гражданские или военные объекты) в сферу международного гуманитарного права, применимого в международных вооруженных конфликтах (и, следовательно, регулирующего их), остается вопросом для обсуждения. На практике остается неясным, распространяется ли международное гуманитарное право, применимое в международных вооруженных конфликтах, на кибероперации (и, следовательно, ограничивает ли их).

Что касается вооруженных конфликтов немеждународного характера, возникают различные вопросы. Во-первых, вооруженные конфликты немеждународного характера могут возникать только между сторонами, которые достаточно организованы. Если государственные вооруженные силы могут быть классифицированы как достаточно организованные, то для негосударственных вооруженных групп требуется более детальное изучение. Когда вооруженные группы существуют исключительно в онлайн-пространстве, определение их организационного характера становится чрезвычайно сложной задачей.

Во-вторых, в отличие от международного гуманитарного права, которое применяется к международным вооруженным конфликтам и регулирует любое применение силы между государствами, независимо от степени интенсивности, в немеждународных вооруженных конфликтах существует требование достаточной интенсивности насилия между двумя или более организованными участниками. Кроме того, хотя такие случаи возможны в исключительных обстоятельствах, предположение, что интенсивность для немеждународного вооруженного конфликта может быть обеспечено исключительно сетевыми действиями, остается нереалистичным. В общем контексте военных действий, включая кибервойны, государства

иногда используют негосударственных субъектов, такие как негосударственные вооруженные группы, для выполнения определенных операций, включая кибероперации.

Специфическая природа киберпространства, включая разнообразные возможности субъектов скрывать или фальсифицировать свою личность, делает выявление авторства действий и приведение поведения к конкретным лицам или сторонам вооруженного конфликта чрезвычайно сложными задачами.

Этот вопрос представляет собой серьезную проблему при определении применимости международного гуманитарного права в конкретной ситуации. Если невозможно определить участников конкретного действия (и, следовательно, связь между действием и вооруженным конфликтом), то крайне сложно определить, применимо ли МГП к этому действию.

Во-первых, существуют различные пороги насилия, которые применяются для квалификации кибератаки как вооруженного конфликта, будь то со стороны государства или негосударственного актора. Поэтому неясно, какой порог применяется, если не известен государственный или негосударственный характер действия. Более того, некоторые нормы МГП, применимые к международным и немеждународным вооруженным конфликтам, не одинаковы.

Во-вторых, кибератаки, не связанные с вооруженным конфликтом (например, преступные действия, не имеющие отношения к конфликту), не регулируются МГП, даже если имеет место вооруженный конфликт. Невозможность установить виновных в кибероперациях может помешать выявить наличие связи с конфликтом.

Эти примеры демонстрируют юридическую важность определения того, кто является субъектом кибердействия и может ли это действие быть приписано государству или негосударственной стороне конфликта. В МГП не определены конкретные критерии для определения того, действует ли частное лицо или негосударственный субъект от имени государства. Поэтому

ответ следует искать в нормах общего международного права, регулирующих присвоение, самой изысканной из которых является право ответственности государств. Согласно как обычному МГП, так и общему международному праву, государство несет ответственность за действия, нарушающие МГП и приписываемые ему, включая:

1. Действия государственных органов, включая вооруженные силы.

2. Действия лиц или организаций, осуществляющих элементы государственной власти.

3. Действия лиц или групп лиц, которые фактически направляются государством или находятся под его руководством или контролем.

4. Действия частных лиц или групп, которые государство признает и принимает как свои собственные.

Понимание и применение этих норм помогают устанавливать ответственность в случае кибератак и определять, применимо ли МГП к данным действиям. Это заключение справедливо независимо от того, совершено ли нарушение международного гуманитарного права кибернетическими или любыми другими средствами.

В отсутствие норм МГП, конкретно регулирующих кибероперации, существует множество проблем, связанных с толкованием общих норм МГП и их применением к таким операциям. В то время как многие общие правила военных действий ограничиваются действиями, представляющими собой нападения, как они определены в МГП, некоторые нормы МГП, регулирующие военные действия, применяются ко всем военным операциям, в основном те, которые обеспечивают специальную защиту определенных видов объектов.

Примером таких правил являются конкретные положения МГП о защите медицинских услуг или объектов, от которых зависит выживание населения. Для большинства военных операций эти положения обеспечивают достаточно широкую защиту, включая операции, которые не являются нападением. Учитывая жизненно важное значение медицинских услуг для

гражданского населения, затронутого вооруженным конфликтом, воюющие стороны должны всегда уважать и защищать медицинские учреждения и медицинский персонал.

В условиях вооруженного конфликта кибератаки на медицинский сектор в большинстве случаев являются нарушением международного гуманитарного права. Аналогичным образом, в дополнение к общему запрету на нападение на любой гражданский объект, международное гуманитарное право конкретно запрещает нападать, уничтожать, удалять или делать бесполезными предметы, необходимые для выживания гражданского населения.

Однако на сегодняшний день лишь немногие государства сформулировали подробные взгляды на то, как концепция нападения в Международном гуманитарном праве (МГП) должна применяться к кибероперациям.

Статья 49 Дополнительного протокола I определяет нападение как "акт насилия против врага, будь то в целях нападения или защиты". Теперь ясно, что понятие "насилие" в этом определении может относиться как к средствам борьбы, так и к ее последствиям, то есть действия, имеющие насильственный эффект, могут представлять собой нападение, даже если средства, ведущие к этому эффекту, не были предприняты в реальном мире.

Утверждается, что все действия, которые, как ожидается, приведут к смерти, травмам или физическому ущербу, представляют собой нападение, включая случаи, когда такой ущерб вызван предсказуемыми косвенными последствиями нападения, например смерть пациента в отделении интенсивной терапии в результате кибератаки на электросеть, которая прекращает подачу электроэнергии в больницу.

Однако существуют споры о том, являются ли кибердействия, которые приводят к потере функций, но не наносят реального ущерба, нападением, как это определено в МГП.

Международный комитет Красного Креста утверждает, что в контексте вооруженного конфликта действия, направленные на вывод из строя компьютера или компьютерной сети, следует рассматривать как нападение в соответствии с правилами международного гуманитарного права о враждебных действиях, независимо от того, осуществляется ли вывод объекта из строя реальными или кибернетическими средствами. Эта интерпретация обосновывается двумя основными причинами. Первая из них вытекает из контекстуальной интерпретации понятия "атака".

Учитывая, что "военный объект", как определено в статье 52(2) Дополнительного протокола I, подразумевает не только его уничтожение или захват, но также "сделан бесполезным" как возможный результат нападения, понятие "нападения" в статье 49 Дополнительного протокола I также следует трактовать как включающее в себя действия, направленные на нарушение функции объекта (то есть делающие его бесполезным), но не обязательно приводящие к физическому ущербу или уничтожению. В противном случае прямая ссылка на утрату полезности в статье 52(2) Дополнительного протокола I была бы избыточной. Поэтому не имеет значения, достигается ли бесполезность объекта путем его уничтожения или другими методами.

Вторая причина заключается в том, что слишком строгое толкование концепции нападения вряд ли соответствует назначению и цели правил ведения военных действий, которые предназначены для обеспечения защиты гражданского населения и гражданских объектов от последствий военных действий. Действительно, при таком уж слишком строгом толковании сетевые операции, направленные на то, чтобы сделать гражданские сети (электрические, банковские, коммуникационные или другие сети) неэффективными или создающие риск достижения такого результата, могут не попадать под общие правила МГП, касающиеся защиты гражданского населения и гражданских объектов.

В то же время, не все кибероперации вооруженного конфликта будут рассматриваться как "нападение" согласно МГП. Понятие нападения в МГП

не включает в себя акты шпионажа. Более того, правила ведения военных действий не запрещают все действия, которые могут нарушать гражданские системы связи; вмешательство в радиосвязь или телепередачи традиционно не рассматривается как нападение в контексте МГП.

Что касается защиты "гражданских объектов" от кибератак, принцип разграничения играет важную роль. Он утверждает, что "стороны в конфликте должны всегда проводить различие между гражданским населением и боевиками и между гражданскими объектами и военными целями, чтобы военные операции сторон в конфликте направлены только против военных целей".

Статья 52(1) Дополнительного протокола I подтверждает, что "гражданские объекты не должны быть объектом нападения или репрессий" и определяет "гражданские объекты" как "все объекты, которые не являются военными целями." Как уже отмечалось, несмотря на растущее признание того, что принцип разграничения и другие фундаментальные принципы МГП применимы к кибервойнам, цифровой и нефизический характер киберпространства и взаимосвязанность военных и гражданских сетей в этом пространстве создают ряд практических и юридических проблем в применении и интерпретации этих правил. В контексте кибервойн утверждается, что взаимосвязанность киберпространства делает применение основных правил МГП, проводящих различие между гражданскими объектами и военными целями, и обязательства избегать чрезмерного сопутствующего ущерба гражданскому населению, сложным, но не невозможным (см. пункт 1 ниже). Тем не менее, остаются два ключевых вопроса, связанных с защитой критически важной гражданской киберинфраструктуры от военных атак. Во-первых, существуют разногласия по поводу того, могут ли считаться эти объекты объектами с точки зрения международного гуманитарного права (см. пункт 2 ниже). Во-вторых, ведутся споры о том, как применяются правила МГП относительно объектов, которые могут иметь как гражданское, так и военное назначение, таких как

объекты двойного назначения, которые широко распространены в киберпространстве. Этот вопрос остается предметом дискуссии. С технической точки зрения, кибератаки могут быть направлены на конкретные военные цели с соблюдением принципов различия, пропорциональности и запрета на неизбирательные атаки. Эти принципы требуют, чтобы атака была направлена исключительно на военную цель и действительно была направлена на нее, а не причиняла чрезмерного сопутствующего ущерба гражданским лицам или гражданским объектам. Несмотря на то, что некоторые аргументировали, что в киберпространстве эти принципы могут быть неактуальными из-за его взаимосвязанности, внимательное изучение характеристик киберсредств позволяет предположить, что они не обязательно нарушают принципы неизбирательности. Разработчики вредоносного ПО или организаторы кибератак могут создать инструменты, не способные к самораспространению. Это означает, что кибератаки могут быть нацелены точно на определенные цели и, таким образом, могут соответствовать требованиям принципов и правил МГП. Некоторые известные киберсредства были разработаны для самораспространения и могли вызвать существенный вред для широко используемых гражданских компьютерных систем. Однако даже такие атаки могут быть запрещены МГП в контексте вооруженного конфликта.

Действительно, МГП запрещает средства и методы ведения войны, включая киберсредства и методы, которые не могут быть направлены на конкретные военные цели, или которые, как можно ожидать, будут выведены из-под контроля пользователя, или которые, при нападении на военный объект, как ожидается, нанесут чрезмерный сопутствующий ущерб гражданскому населению по сравнению с ожидаемым конкретным и прямым военным преимуществом.

Данные играют важную роль в цифровой сфере и являются угловым камнем многих социальных аспектов жизни: личные медицинские записи,

социальные страховки, налоговые документы, банковские счета, клиентские досье компаний или списки и записи кандидатов - все это неотъемлемые элементы эффективного функционирования гражданской жизни. Они составляют ключевой аспект для обеспечения нормального функционирования гражданского общества.

В настоящее время растет обеспокоенность вопросами защиты этих важных гражданских данных. В случае данных, относящихся к определенным категориям объектов, специально охраняемых МГП, правила защиты данных должны рассматриваться в обширном контексте. Например, обязательство уважать и защищать медицинские учреждения должно охватывать и медицинские данные, принадлежащие этим учреждениям.

Аналогичным образом, запрещается удалять или подделывать данные, чтобы сделать бесполезными объекты, необходимые для выживания гражданского населения, такие как установки питьевой воды, объекты водоснабжения и ирригационные сооружения.

Однако важно уточнить, в какой степени гражданские данные, на которые не распространяется такая специальная защита, защищены установленными общими правилами ведения боевых действий. В частности, существует широкое обсуждение относительно того, являются ли данные объектами и подпадают ли кибердействия в отношении данных (например, их удаление) под действие принципов различения, пропорциональности и мер предосторожности, а также под защиту, которую они обеспечивают гражданским объектам.

Удаление или изменение таких данных может быстро привести к полной остановке государственных служб и частных предприятий и нанести значительный ущерб гражданскому населению, превышающий потенциальные последствия уничтожения физических объектов. В современном мире, все более зависящем от информационных сетей, МГП не запрещает совершать такие действия, будь то потому, что удаление или изменение таких данных не рассматривается как "нападение" в рамках МГП

или по причине того, что такие данные не считаются "объектами" в смысле запретов на нападение на гражданские объекты. Такое положение вряд ли соответствует цели и задачам этого правового режима.

Замена бумажных документов и файлов цифровыми данными не должна уменьшать уровень защиты, предоставляемой МГП данным информационным ресурсам. Важно не только защищать критически важные гражданские инфраструктуры, зависящие от киберпространства, но также обеспечивать защиту самой киберинфраструктуры. Однако существует сложность в вопросе взаимодействия гражданских и военных сетей.

Большинство военных сетей зависят от гражданских сетевых средств, таких как подводные оптоволоконные кабели, спутники, маршрутизаторы или узлы. Глобальные навигационные спутниковые системы, такие как ГЛОНАСС, GPS или Galileo, которые все более используются гражданскими секторами, также могут иметь военное применение. Гражданские логистические сети поставок (включая продовольствие и медицинские товары) и другие предприятия также могут разделять сети и коммуникационные инфраструктуры с военными системами. За исключением некоторых сетей, специально предназначенных для военных нужд, практически невозможно провести четкое разграничение между чисто гражданскими и исключительно военными сетевыми инфраструктурами.

Согласно МГП, нападения должны строго ограничиваться военными целями. В случае объектов, военные цели определяются как те, которые по своему характеру, местоположению, назначению или использованию вносят эффективный вклад в военные действия, и их полное или частичное уничтожение, захват или нейтрализация в данных обстоятельствах обеспечивает определенное военное преимущество.

Согласно МГП, все объекты считаются гражданскими объектами, если они не соответствуют этому определению военных целей, и поэтому не должны быть объектом нападения или репрессий. Объект, который обычно используется в гражданских целях, считается гражданским и, следовательно,

охраняется, если есть сомнения в том, вносит ли он эффективный вклад в военные действия.

Традиционное понимание заключается в том, что объект считается военным, если он используется в военных целях и соответствует определению военного объекта, даже если он также используется в гражданских целях. Расширенное толкование этого правила может привести к выводу, что многие объекты, входящие в сетевую инфраструктуру, могут быть рассмотрены как военные цели, и, следовательно, перестают пользоваться защитой от кибернетических или реальных атак. Это вызывает серьезную обеспокоенность в связи с увеличивающейся зависимостью гражданского населения от киберпространства. Однако этот вывод не является окончательным.

Во-первых, данный анализ не может быть применен к киберпространству или Интернету в целом; воюющие стороны должны определить, какие конкретные компьютеры, узлы, маршрутизаторы или сети могут считаться военными целями. Следовательно, необходим анализ отдельных компонентов сети, конкретных компьютеров или другого оборудования, которое может быть выделено из сети или системы.

Во-вторых, сети проектируются с высокой степенью резервирования, что означает, что одной из их характеристик является способность быстро перенаправлять потоки данных. Согласно определению военной цели, этот встроенный запас прочности также должен учитываться при оценке, действительно ли повреждение или утрата полезности объекта принесут явную военную выгоду. Если это не так, объект остается гражданским и не может быть атакован.

В-третьих, любая атака должна соответствовать правилам, запрещающим неизбирательные нападения, и принципам пропорциональности и предосторожности при нападении. Даже если объект признан военной целью, нарушение любого из этих принципов, которое

приводит к прекращению или затруднению использования гражданских объектов, считается незаконной атакой.

Важность юридического анализа киберсредств и методов ведения войны для обеспечения соблюдения МГП.

Учитывая особые проблемы, создаваемые характеристиками киберпространства при толковании и применении некоторых принципов МГП, регулирующих ведение боевых действий, разработка и использование киберсредств и методов ведения войны сторонами вооруженного конфликта требует тщательного юридического анализа. Как уже отмечалось ранее, государства-участники Дополнительного протокола I, разрабатывающие или приобретающие потенциал для кибервойны (независимо от того, наступательный ли или оборонительный характер этого потенциала), обязаны оценить, является ли использование кибероружия, средств и методов ведения войны согласно международному праву запрещенным в некоторых или во всех обстоятельствах. В более широком смысле, государствам важно проводить юридический анализ для обеспечения соблюдения МГП, что означает, что вооруженные силы могут разрабатывать и использовать киберсредства и методы ведения войны только в соответствии с обязательствами государства по МГП.

Такой анализ должен включать в себя многопрофильную команду, включая соответствующих юридических, военных и технических экспертов. Эти юридические обзоры необходимо проводить для более глубокого анализа законности средств, фактически используемых для совершения конкретных атак. Правовой анализ кибероружия, средств и методов ведения войны может столкнуться с множеством проблем. Во-первых, страна, проводящая юридическую экспертизу, должна определить, какой правовой стандарт применять к конкретному киберсредству. Другими словами, государствам-участникам необходимо ответить на некоторые из вопросов, обсуждаемых ранее, такие как, является ли использование киберсредства

атакой и, следовательно, требует ли оно соблюдения определенных норм международного гуманитарного права.

Во-вторых, оружие необходимо оценивать не отдельно от способа его применения. При юридической экспертизе необходимо учитывать обычное и предполагаемое использование оружия. Однако, в отличие от кинетического оружия, кибервоенные возможности могут быть менее стандартизированы, особенно если они разрабатываются для конкретной операции. Это означает, что их необходимо рассматривать в контексте конкретного киберпространства, в котором они могут быть использованы.

В-третьих, государства-участники должны проводить не только юридический анализ нового оружия, которое они намереваются использовать, но и включать в анализ оружие, которое уже прошло правовую экспертизу, с учетом всех изменений. Соответствующие киберсредства могут часто адаптироваться, что может создавать проблемы для государств, включая обновления безопасности программного обеспечения, которые могут производиться потенциальными объектами. Хотя необходимость проведения новых юридических экспертиз в случае изменений типа и масштаба, возможно, нуждается в дальнейшем уточнении, было отмечено, что "оценка того, повлияет ли изменение на функционирование программы, должна быть качественной, а не количественной".

Для того чтобы юридические экспертизы были эффективными, они должны проводиться в соответствии с принципами Конвенции. Для того чтобы юридический анализ был эффективным, страны, разрабатывающие или использующие новые оружейные технологии, должны решить эти и другие сложные вопросы. Другими словами, режим тестирования должен быть адаптирован к уникальной природе кибертехнологий. Учитывая эти сложности, наилучшей практикой для обеспечения соблюдения МГП всеми государствами является обмен информацией о механизме правового анализа государства и, насколько это возможно, о существенных результатах юридического анализа. Это особенно важно, когда возникает вопрос о

несовместимости оружия с МГП, чтобы другие государства не столкнулись с той же проблемой, и чтобы другие государства были проинформированы о выводах государства, проводящего анализ, относительно того, что такие средства запрещены МГП.

Для защиты гражданского населения и гражданской инфраструктуры в вооруженном конфликте важно признать, что кибервойна не является правовой пустотой и регулируется международным правом, включая МГП. Однако, как утверждается в данной работе, признание применимости МГП – это еще не конец дискуссии. Необходимо дальше обсуждать (особенно между государствами) вопрос о том, как следует интерпретировать МГП в киберпространстве. Любое такое обсуждение должно базироваться на понимании развития кибернетического военного потенциала.

3.3. Информационные войны в контексте глобальных трансформаций и реконфигурации Мир-Системы

Мир переживает фундаментальные трансформации, и это продолжится в ближайшем и среднесрочном будущем. Прежде всего, речь идет здесь о политических трансформациях, в особенности о трансформациях глобального управления. Выступая на форму БРИКС в Казани в 2024 году председатель КНР Си Цзиньпин подчеркнул важность «совершенствования системы глобального управления. Темпы реформ глобального управления долгое время не соответствуют глубоким изменениям баланса международных сил. Следует придерживаться принципа подлинного мультилатерализма и концепции совместного обсуждения, совместного строительства и совместного использования, возглавить реформирование системы глобального управления на основе концепций равенства, справедливости, открытости и инклюзивности»[194].

Китай и Россия выступают плечом к плечу в задаче становления нового, справедливого и многополярного порядка. Президент России Владимир Путин многократно подчеркивал в своих выступлениях приверженность России решению этой задачи. В своей речи на заседании пленарной сессии XX Ежегодного заседания Международного дискуссионного клуба «Валдай» в октябре 2023 года В.В. Путин выделил шесть «китов» нового справедливого многополярного мироустройства – 1) открытый мир без барьеров; 2) культурное и цивилизационное многообразие; 3) максимальная представительность и коллективные решения на глобальном уровне; 4) всеобщая безопасность и прочный мир; 5) справедливость как для развитых стран, так и для развивающихся; уважение интересов всех стран; 6) равноправие всех государств на международной арене [195] . В том же

[194] Действовать с широким кругозором и решительностью во имя высококачественного развития сотрудничества Большого БРИКС / Выступление на 16-ой встрече лидеров стран БРИКС, Председатель КНР Си Цзиньпин (23.10.2024, г. Казань). URL: https://by.china-embassy.gov.cn/rus/zgxx/202410/t20241024_11514992.htm (дата обращения 16.11.2024).

[195] Владимир Путин принял участие в пленарной сессии юбилейного, XX заседания Международного

выступлении В.В. Путин подчеркнул наличие большого числа совместных проектов с КНР, а также общность миссии двух стран по содействию установлению нового справедливого многополярного мироустройства. На саммите БРИКС в Казани Президент России вновь подчеркнул, что «в мире происходят поистине кардинальные изменения, идёт процесс формирования многополярного мира»[196]. Ранее В.В. Путин неоднократно отмечал также, что эти изменения наталкиваются на ожесточенное сопротивление со стороны стран «золотого миллиарда»[197].

Столь масштабные глобальные изменения, разумеется, привлекают значительное внимание представителей научного сообщества. В науке имеются различные подходы к пониманию феномена текущих и предстоящих трансформаций. Так, часть ученых рассматривает их в контексте происходящей смены пятого технологического уклада шестым. Среди ведущих российских исследователей этой темы можно назвать

дискуссионного клуба «Валдай» / Официальный сайт Президента России. 05.10.2023. URL: http://kremlin.ru/events/president/news/72444 (дата обращения 16.11.2024).

[196] Заседание саммита БРИКС в узком составе / Официальный сайт Президента России. 23.10.2024. URL: http://kremlin.ru/events/president/transcripts/75374 (дата обращения 16.11.2024).

[197] Герейханова А., Гончарук Д. Путин назвал БРИКС одним из ключевых элементов формирующегося многополярного миропорядка / Российская газета. 11.07.2024. URL: https://rg.ru/2024/07/11/vazhno-byt-vmeste.html (дата обращения 16.11.2024).

академиков В.А. Садовничего [198], А.А. Акаева [199], С.Ю. Глазьева [200], профессоров Л.Е. Гринина, А.В. Коротаева[201] и ряд других ученых.

Так, С.Ю. Глазьев разработал концепцию технологических укладов – они представляют собой «группы совокупностей технологически сопряженных производств, выделяемых в технологической структуре экономики, связанные друг с другом однотипными технологическими цепями и образующие воспроизводящиеся целостности. Каждый такой уклад представляет собой целостное и устойчивое образование, в рамках которого осуществляется полный макропроизводственный цикл, включающий добычу и получение первичных ресурсов, все стадии их переработки и выпуск набора конечных продуктов, удовлетворяющих соответствующему типу общественного потребления» [202]. Применительно к изучению глобальных трансформаций эта концепция важна тем, что переход от одного уклада к другому, как правило, сопровождается глобальной политической турбулентностью. Именно такой переход – от пятого уклада, ядро которого

---

[198] Акаев А. А., Садовничий В. А. Замкнутая динамическая модель для описания и расчёта длинной волны экономического развития Кондратьева // Вестник Российской академии наук. 2016. Т. 86, №10. С. 883-896.

[199] Акаев А. А. Эпохальные открытия Николая Кондратьева и их место в современной экономической науке // AlterEconomics. 2022. Т.19, №1. С. 11-39. Акаев А. А. Математические основы инновационно-циклической теории экономического развития Шумпетера – Кондратьева // Кондратьевские волны: аспекты и перспективы / Акаев А. А., Гринберг Р. С., Гринин Л. Е., Коротаев А. В., Малков С. Ю. (ред.). Волгоград: Учитель, 2012. С. 110-135. Акаев А. А. Большие циклы конъюнктуры и инновационно-циклическая теория экономического развития Шумпетера-Кондратьева // Экономическая наука современной России. 2013. №2 (61). С. 7-29. Акаев А. А. Анализ состояния и перспектив мирового экономического роста на основе теории Шумпетера-Кондратьева // Экономика и управление. 2011. №2. С. 9-15. Акаев А. А. Стратегическое управление устойчивым развитием на основе теории инновационно-циклического экономического роста Шумпетера-Кондратьева // Экономика и управление. 2011. №3 (65). С. 4-10.

[200] Глазьев С. Ю. Современная теория длинных волн в развитии экономики // Экономическая наука современной России. 2012. №2 (57). С. 27-42. Глазьев С. Ю. Мирохозяйственные уклады в глобальном экономическом развитии // Экономика и математические методы. 2016. Т. 52, №2. С. 3-29. Глазьев С. Ю. Перспективы становления в мире нового VI технологического уклада // МИР (Модернизация. Инновации. Развитие). 2010. №2. С. 4-10. Глазьев С. Ю., Айвазов А. Э., Беликов В. А. (2019). Циклически-волновые теории экономического развития и перспективы мировой экономики. Предсказуемо ли среднесрочное и долгосрочное развитие мировой экономики // Научные труды Вольного экономического общества России. 2019. Т. 219, №5. С. 177-211. Глазьев С. Ю. Приоритеты опережающего развития российской экономики в условиях смены технологических укладов // Экономическое возрождение России. 2019. №2 (60). С. 12-16.

[201] Коротаев А. В., Гринин, Л. Е. Кондратьевские волны в мир-системной перспективе // Кондратьевские волны. Аспекты и перспективы. Волгоград: Учитель, 2012. С. 58-109. Гринин Л. Е., Гринин А. Л., Коротаев А. В. Кибернетическая революция, шестой длинный цикл Кондратьева и глобальное старение // AlterEconomics. 2022. Т.19, №1. С. 147-165. Grinin L. E., Korotayev A. V. Global Population Ageing, The Sixth Kondratieff Wave, And The Global Financial System // Journal of Globalization Studies. 2016. Т.7, №2. С. 11-31. Grinin L. E., Grinin A. L., Korotayev A. Forthcoming Kondratieff wave, Cybernetic Revolution, and global ageing // Technological Forecasting & Social Change. 2017. Vol. 115. P. 52–68.

[202] Глазьев С. Ю. Рывок в будущее. Россия в новых технологическом и мирохозяйственном укладах. М.: Книжный мир, 2018. 768 с.

составляли информационные технологии и электронная промышленность, к шестому укладу, в основу которого, по мнению академика Глазьева, ляжет конвергенция нано-, био-, инфо- и когнитивных технологий (так называемая НБИКС-конвергенция, NBIC), а также социогуманитарные технологии – происходит в настоящее время, и академик Глазьев справедливо указывает на то, что «происходящая одновременно с технологической социально-политическая революция – переход от имперского к интегральному мирохозяйственному укладу – обуславливает смену американского цикла накопления капитала азиатским. Управление экономикой, позволившее, прежде всего, американской экономике расти высокими темпами, более не обеспечивает развития ее производительных сил. В то же время система институтов нового азиатского уклада, народившегося на периферии американоцентричного имперского мирохозяйственного уклада, напротив, обеспечивает гармонизацию разнонаправленных экономических интересов и направляет их на цели повышения общественного благосостояния»[203]. Таким образом, по его мнению, наблюдаемая сегодня глобальная турбулентность непосредственно связана и во многом вызвана замещением доминирующих технологических и мирохозяйственных укладов, которые происходят одновременно и потому усиливают друг друга (эффект резонанса)[204]. На этом фоне дополнительным мощным усилителем этого резонанса, расшатывающего мировую стабильность, стала развернутая коллективным Западом – в первую очередь, США, отчаянно пытающимися удержать статус глобального гегемона – гибридная война против России. С.Ю. Глазьев верно подмечает, что «в стремлении нанести России максимально возможный ущерб Вашингтон, Лондон и Брюссель разыграли свои главные козыри: монополию на эмиссию мировых валют, имидж образцового правового

[203] Глазьев С. Ю. Глобальная трансформация через призму смены технологических и мирохозяйственных укладов // AlterEconomics. 2022. Т. 19. № 1. С. 93-115. С. 93. См. также: Глазьев С. Ю. Ноономика как стержень формирования нового технологического и мирохозяйственного укладов // Экономическое возрождение России. 2020. № 2(64). С. 15-32.

[204] Глазьев С. Ю., Косакян Д. Л. Состояние и перспективы формирования 6-го технологического уклада в Российской экономике // Экономика науки. 2024. Т.10, №2. С. 11-29. Глазьев С. Ю. Адаптация российской экономики к смене технологических и мирохозяйственных укладов // Научные труды Вольного экономического общества России. 2023. Т. 244, №6. С. 95-102.

демократического государства, веру в «священное» право частной собственности. Тем самым они поставили все независимые от них страны перед необходимостью поиска новых мировых валютных инструментов, механизмов страхования рисков, восстановления норм международного права и создания собственных систем экономической безопасности» [205]; однако антироссийские санкции не усилили, а наоборот, подорвали глобальное доминирование США и ЕС и резко ускорили переход к новому мирохозяйственному укладу и перемещение центра мировой экономики в Юго-Восточную Азию.

Профессор Л.Е. Гринин обращает внимание на связь концепции технологических укладов (или парадигм) с концепцией длинных волн, разработанной в 1920-х гг. российским ученым Н.Д. Кондратьевым [206]. В основе этой концепции лежит наблюдение о том, что «в долгосрочной динамике некоторых экономических индикаторов (начиная по крайней мере с конца XVIII в.) наблюдается определенная циклическая регулярность. Она заключалась в том, что на смену фазам ускоренного роста соответствующих показателей приходят фазы их относительного спада или более медленного роста. Длительность одной волны составляет в среднем от 40 до 60 лет»[207]. В настоящее время происходит переход от пятой к шестой волне, а именно такие периоды перехода являются наиболее опасными с точки зрения возникновения глобальной политической нестабильности.

Для объяснения происходящих глобальных трансформаций также весьма полезен мир-системный подход, у истоков которого стояли Ф. Бродель и И.Валлерстайн[208]. В России его активно развивают профессора

---

[205] Глазьев С. Ю. О текущем положении России в мировой гибридной войне и создании необходимых условий для нашей победы // Глобальный конфликт и контуры нового мирового порядка: XX Международные Лихачевские научные чтения, 9–10 июня 2022 г. Санкт-Петербург: СПбГУП, 2022. С. 55-58. С. 56.

[206] Гринин Л. Е. Кондратьевские волны, технологические уклады и теория производственных революций // Кондратьевские волны. 2012. №1. С. 222-262.

[207] Гринин Л. Е., Гринин А. Л. Кибернетическая революция и шестой технологический уклад // Историческая психология и социология истории. 2015. Т.8, №1. С. 172-197. С. 172-173.

[208] Braudel F. Capitalism and material life, 1400–1800. Harper and Row, 1973. Braudel F. Civilization and capitalism, 15th – 18th century. Harper and Row, 1982. Wallerstein I. The modern world-system I: Capitalist agriculture and the origins of the European world-economy in the sixteenth century. Vol. 1. University of California

Л.Е. Гринин и А.В. Коротаев[209]. По их мнению, в настоящее время имеет место реконфигурация Мир-Системы – напомним, что, согласно мир-системному подходу, структура Мир-Системы включает ядро и периферию (позднее была добавлена также такая категория, как полупериферия). При этом начало этой реконфигурации было положено событиями Арабской весны 2011 года, а ее завершение займет еще какое-то время, в представлении этих ученых – до 20 лет. Основная причина этой реконфигурации, по их мнению, «связана с заметным отставанием политической составляющей глобализации от ее экономической составляющей. … быстрое экономическое развитие, так или иначе, требует своего рода подтягивания политической системы до соответствующего уровня. В противном случае внутренние напряжения и противоречия в обществе усиливаются. … Однако изменению политических и социальных институтов во многих обществах препятствуют их жесткость, а также интересы элиты»[210]. Значительная часть политических потрясений и кризисов последних лет, включая украинский кризис, рассматривается учеными как «реконфигуративные» кризисы, которые одновременно являются и геополитическими, требующими изменения мирового порядка. По Л.Е, Гринину и А.Л. Гринину, «главный вектор этой реконфигурации – ослабление центра Мир-Системы, то есть США и Запада, и одновременное усиление позиций целого ряда периферийных стран, в целом усиление

Press, 2011. Wallerstein I. World-systems analysis: An introduction. Duke University Press, 2020. Wallerstein, I. 1974. The Modern World-System: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century. NY: Academic. 410 p. Wallerstein I. 1979. The Capitalist World-Economy. Cambridge: Cambridge University Press. 305 pp. Wallerstein I. 1980. The Modern World-System II. Mercantilism and the Consolidation of the European World Economy, 1600-1750. NY: Academic. 370 p.

[209] Гринин Л. Е., Коротаев А. В. Циклы, кризисы, ловушки современной Мир-Системы: исследование кондратьевских, жюгляровских и вековых циклов, глобальных кризисов, мальтузианских и постмальтузианских ловушек. М.: URSS, 2019. Коротаев А. В., Гринин Л. Е. Кондратьевские волны в мир-системной перспективе // Кондратьевские волны. Аспекты и перспективы. Волгоград: Учитель, 2012. С. 58-109. Гринин Л. Е., Коротаев А. В., Цирель С. В. Циклы развития современной Мир-Системы. М.: ЛИБРОКОМ/URSS, 2011. Коротаев А. В., Малков А. С., Халтурина Д. А. 2019. Законы истории: Математическое моделирование развития Мир-Системы. Демография, экономика, культура. М.: ЛЕНАНД/URSS, 2019. Гринин Л. Е., Коротаев А. В. Социальная макроэволюция. Генезис и трансформации Мир-Системы. М.: Либроком/URSS, 2009.

[210] Гринин Л. Е., Гринин А. Л. Новая волна революционных процессов в афразийской макрозоне нестабильности и ее влияние на смежные мир-системные зоны // История и современность. 2022. №3(45). С. 3-22. С. 10.

развивающихся стран»[211]. Экономическое усиление многих развивающихся стран, их успехи в сокращении отставания от экономических лидеров получили название Великой конвергенции[212]. Сейчас речь идет о сокращении соответствующего отставания в глобальном политическом влиянии, которое «подтягивается» за бурным экономическим ростом и развитием. Авторы отмечают, что действия США, пытающихся любой ценой удержать ускользающую позицию гегемона, способствуют в последние годы росту «беспорядка», хаотизации Мир-Системы[213].

Таким образом, в ближайшие годы можно ожидать усиления геополитической турбулентности – а значит, и межгосударственных конфликтов различной интенсивности. С учетом того, что одной из ключевых фундаментальных технологий наступающего шестого экономического уклада ученые полагают информационные технологии, есть основания предполагать и нарастание интенсивности информационных войн, а также быстрого развития их социально-гуманитарного инструментария.

Социально-гуманитарные технологии в информационной войне относятся к использованию психологических, социологических и культурных факторов при разработке и реализации кампаний по пропаганде, дезинформации и влиянию. Основные тенденции развития этих технологий включают:

1. **Персонализация:** Собирая и анализируя больше данных о конкретных людях, можно настраивать сообщения и контент под конкретных пользователей или группы. Это может повысить эффективность пропагандистских и дезинформационных кампаний. Технологии персонализации используются в информационной войне для адаптации контента под конкретные аудитории, влияя на их убеждения и поведение.

---

[211] Там же.

[212] Grinin L., Korotayev A. Great divergence and great convergence. A Global Perspective. Cham: Springer International Publishing, 2015. Korotayev A., Goldstone J. A., Zinkina J. Phases of global demographic transition correlate with phases of the Great Divergence and Great Convergence // Technological Forecasting and Social Change. 2015. Vol. 95. P. 163-169. Korotayev A., Zinkina J. On the structure of the present-day convergence // Campus-Wide Information Systems. 2014. Vol. 31, No 2/3. P. 139-152.

[213] Гринин Л. Е. Размышления о трансформациях мирового порядка* Часть 1. Мировой порядок в прошлом и настоящем // Credo New. 2017. №1. С. 93-119.

Это может иметь как положительное, так и отрицательное воздействие, в зависимости от целей и достоверности предоставленной информации. Персонализация в информационной войне включает создание сообщений и контента, учитывая личные данные и интересы целевой аудитории. Этот подход делает информацию более убедительной и влиятельной. В информационной войне персонализация может использоваться для манипуляции общественным мнением и доверием. Например, собирая информацию о предпочтениях, политических взглядах и потребностях пользователей в сети Интернет, можно создавать сообщения, которые близки к их собственным убеждениям. Персонализированный контент в социальных сетях, блогах и новостных сайтах может оказывать большое влияние на общество, поскольку пользователи готовы изменить свои взгляды, основываясь на информации из определенных источников. Однако использование персонализации, особенно в информационной войне, может создать угрозы для общественной безопасности, такие как манипуляции общественным мнением, фальсификация выборов и распространение фейковых новостей. Поэтому важно соблюдать этические стандарты и обеспечивать контролируемость и объективность при использовании персонализации.

2. **Манипулирование социальными сетями:** Платформы социальных сетей все чаще используются для распространения пропаганды и дезинформации. Это включает в себя использование ботов, фейковых аккаунтов и таргетированной рекламы для воздействия на общественное мнение. Манипулирование социальными сетями в информационной войне включает в себя действия, направленные на манипуляцию общественным мнением и формирование желаемых взглядов и убеждений. Эти действия могут быть проведены как государственными структурами, так и частными лицами, группами и организациями. Один из методов манипулирования социальными сетями – это использование ботов. Боты – это программы, которые автоматически создают и публикуют информационные сообщения и

комментарии в социальных сетях. Использование ботов может увеличить количество сообщений в определенной теме, создать искусственную поддержку или противодействие определенным мнениям. Другим методом манипулирования социальными сетями является использование фейковых аккаунтов. Фейковый аккаунт – это профиль пользователя, созданный с целью манипуляции, который может использоваться для распространения ложной информации, провокации или создания искусственных сообществ. Кроме того, в информационной войне могут использоваться и другие технологии, такие как малвар и вирусы, хакерские атаки и др. Манипулирование социальными сетями в информационной войне представляет серьезную угрозу свободе мнения и демократии и может вызвать проблемы в общественной, политической и экономической сферах. Поэтому важно обучать пользователей различным инструментам и технологиям, улучшать системы защиты и выявления фейковой информации, а также содействовать разработке свободных и независимых социальных платформ. В целом, важно использовать социально-гуманитарные технологии с соблюдением этических норм и с акцентом на достижение положительных результатов как для отдельных лиц, так и для общества в целом.

3. **Психологические операции** (ПО): Психологические операции включают использование психологических методов для воздействия или манипулирования поведением противника. Это может включать в себя использование таких элементов, как страх, неуверенность, сомнение, а также положительное усиление и обращение к эмоциональным аспектам. Психологические операции (ПО) представляют собой способ воздействия на психические процессы целевой аудитории с целью достижения определенных целей. В рамках информационных войн ПО являются одними из наиболее эффективных и опасных инструментов, используемых для манипуляции общественным мнением и дезинформации.

Психологические операции могут быть направлены на создание или усиление негативных или позитивных эмоций, формирование стереотипов и предубеждений, а также создание ложных убеждений и ценностей. Они могут также включать в себя создание негативного или положительного образа определенного человека, группы или страны.

Например, использование фейковых новостей и видеоматериалов, специально созданных с целью ввода в заблуждение, может привести к формированию ложных убеждений и предубеждений у целевой аудитории. Использование образов и символов для создания положительного или отрицательного образа определенного человека или группы людей также может привести к серьезным последствиям и манипулированию общественным мнением.

Для противодействия ПО важно повышать информационную грамотность и критическое мышление общества. Люди должны уметь анализировать информацию, идентифицировать фейковые новости и их источники, а также уметь распознавать манипулятивные методы, которые могут быть использованы для широкомасштабного воздействия на общественное мнение. Также важно, чтобы правительственные и международные структуры улучшали системы защиты и распознавания ПО, а также работали над предотвращением и пресечением использования ПО в информационных войнах.

Понимание культуры играет важную роль в информационных войнах, так как культура определяет менталитет и поведение людей, и может быть ключевым фактором в формировании и управлении общественным мнением.

В рамках информационных войн, понимание культуры может помочь более эффективно справляться с манипуляциями и распространением дезинформации в различных культурах и регионах. Различные культуры имеют свои уникальные традиции, ценности и обычаи, которые могут влиять на то, как люди воспринимают информацию и реагируют на нее.

Например, в некоторых культурах сильнее преобладают стереотипы, предубеждения и мифы, которые могут быть использованы в информационных войнах с целью манипуляции общественным мнением. Понимание этих культурных особенностей может помочь противостоять таким методам и более эффективно защищать свою аудиторию.

Кроме того, понимание культуры позволяет более эффективно создавать и распространять информацию, которая привлекает внимание и поддержку целевой аудитории. Знание о местных традициях, ценностях и потребностях может помочь создать сообщение, более соответствующее психологическим особенностям целевой аудитории, что значительно увеличивает вероятность успеха информационной кампании.

Таким образом, понимание культуры является важным аспектом в информационных войнах, поскольку оно позволяет лучше понимать менталитет и поведение людей, противостоять манипуляциям и дезинформации, а также создавать более эффективные и целенаправленные информационные кампании.

Понимание культурных ценностей и верований целевой аудитории играет решающую роль в эффективных пропагандистских кампаниях и кампаниях по дезинформации. Это включает использование культурных символов и ассоциаций, а также призывы к национальной гордости или особенностям.

В ответ на пропаганду и дезинформацию разрабатываются контрнарративы, которые представляют собой информационные сообщения, направленные на опровержение негативных или ложных нарративов. Они могут включать в себя фактическую проверку, альтернативные нарративы и развитие навыков критического мышления. Целью контрнарративов является изменение общественных взглядов и убеждений, вызванных негативными или ложными нарративами. Они могут использоваться для предоставления доказательств и подтверждений, а также противостоять аргументам и утверждениям, которые поддерживают исходные нарративы.

Контрнарративы могут также способствовать созданию новых ценностей и вербальных фреймов с целью изменения и укрепления позиции. Важно отметить, что создание контрнарративов требует квалифицированных команд, специализирующихся на информационной борьбе. Они должны учитывать местные культурные особенности и поведенческие особенности целевой аудитории, чтобы контрнарративы были наиболее эффективными в изменении восприятия. Создатели контрнарративов также должны быть готовы реагировать на любые опровержения и атаки нарратива. В современном информационном мире реакция на негативный или ложный нарратив может быть необходима в течение нескольких часов, поэтому команды должны быть готовыми к быстрому реагированию и взаимодействию с соответствующей аудиторией. Таким образом, контрнарративы представляют собой важный инструмент в информационных войнах и могут быть эффективным средством противодействия негативным и ложным нарративам. Они должны быть организованы и созданы с учетом местной культуры и поведения целевой аудитории, а также готовыми к быстрому реагированию на любые опровержения нарратива.

Другое важное направление — развитие международного сотрудничества. Необходимо активно содействовать международному сотрудничеству в области информационной безопасности, чтобы эффективно бороться с угрозами информационной войны. Это включает в себя создание новых международных механизмов и платформ для обмена информацией и сотрудничества с другими государствами и международными организациями.

Также важно развивать международные стандарты и законодательство в области информационной безопасности, что позволит создать единую систему принципов и правил, регулирующую деятельность государств и предотвращающую конфликты и потенциальные угрозы.

Кроме того, следует усилить сотрудничество между правительствами, компаниями и экспертами в области кибербезопасности. Совместное

проведение тренингов и обучающих программ поможет повысить компетентность специалистов и качество реагирования на угрозы.

Укрепление сотрудничества между специализированными службами, ответственными за национальную безопасность и борьбу с киберпреступностью, также является важным шагом. Обмен информацией между ними может помочь в идентификации и задержании злонамеренных актеров и предотвращении кибератак.

Все эти меры способствуют созданию более устойчивой и безопасной информационной среды на международном уровне. Развитие международного сотрудничества является ключевым фактором в борьбе против угроз информационной безопасности и способствует укреплению сотрудничества между государствами в этой области.

Среди прочих мер противодействия информационным войнам наиболее перспективным представляется программное повышение медиаграмотности населения. Данный вопрос можно рассмотреть на примере рекомендаций для России. Медиаграмотное поведение основано на умении проверять информацию. В этой связи – для России предлагается создание специальных специализированных «фактчегинговых» платформ, обеспечивающих оценку источника информации и ее проверку. При этом специальные курсы, тренинги, интегрированные с систему основного и дополнительного образования, должны быть повсеместными. При этом наилучший способ противостояния информационной агрессии – наличие собственной, глобально-мировоззренческой и национально-ориентированной идеологии, известной и принимаемой большинством граждан как руководство к социально-политическому поведению, в том числе – в области информационного взаимодействия.

Кроме того, важно развивать средства разведки. В настоящее время, средства разведки и слежения играют огромную роль в информационной войне. Увеличение финансирования и усовершенствование таких средств позволяют государствам своевременно реагировать на угрозы

информационной безопасности. Средства разведки включают в себя множество различных инструментов, начиная от аналитических систем, способных мониторировать социальные сети, и заканчивая спутниковой разведкой и персональными дронами. В настоящее время усовершенствование происходит в почти всех областях, связанных со средствами разведки, включая новейшие технологии детектирования, преодоления препятствий и выявления скрывающихся объектов. Важным аспектом развития средств разведки является увеличение их скорости и точности. Необходимо, чтобы средства разведки были нацелены на минимизацию времени, затрачиваемого на поиск информации, и действовали максимально точно в условиях нарушенной информационной среды. Кроме того, чрезвычайно важно не забывать о человеческом факторе при использовании средств разведки. Без должной подготовки и компетентности людей, использующих эти средства, необходимая информация может быть утеряна или использована неправильно.

В итоге можно сказать, что развитие средств разведки является неотъемлемой частью обеспечения защиты государства в информационной войне. Улучшение технологий и компетенции кадров разведки позволит эффективно справляться с угрозами информационной безопасности и защищать интересы государства и граждан.

Усиление правовой базы является необходимым условием для эффективной защиты информационной безопасности, поскольку это позволяет правильно распределить ресурсы и определить ответственность за нарушения закона. Разработка и усиление правовой базы в области информационной безопасности должны быть направлены на решение следующих задач:

1. Определение понятий и терминологии. Это позволяет унифицировать понимание определенных терминов и снижает вероятность ошибок в правовом регулировании.

2. Установление основных прав и свобод, касающихся информационной безопасности, и ограничений на их использование.

3. Определение обязанностей и ответственности за невыполнение требований законодательства в области информационной безопасности.

4. Разработка и утверждение процедур мониторинга и контроля за соответствием организаций и граждан требованиям заранее утвержденного законодательства.

5. Определение мер пресечения нарушений закона в области информационной безопасности, включая административные, гражданские и уголовные.

Таким образом, усиление правовой базы является необходимым условием для эффективной борьбы с угрозами информационной безопасности и важным фактором обеспечения прав и свобод граждан в цифровой эпохе.

Исследователи полагают, что формирование нового мирового порядка неизбежно, но период распада современного американского порядка может затянуться, при этом сопровождаясь многочисленными «гибридными» войнами, которые могут перейти и в войны «традиционные». Это обусловливает важность перечисленных выше инструментов по противодействию информационным войнам, являющимся неотъемлемым компонентом «гибридных» войн (и вполне вероятным спутником войн «традиционных»). Новый порядок должен основываться на консенсусе, и новый гегемон, абсолютный лидер в Мир-Системе, подобный США, в нем вряд ли возможен[214]. В этом свете некорректно выставлять КНР конкурентом США в борьбе за глобальное господство и доминирование. Сторонники мир-системного подхода корректно отмечают, что Китай уже был частью центра Мир-Системы в течение значительного промежутка времени вплоть до начала XIX века[215]. Однако современная КНР не имеет стремления стать

[214] Гринин Л.Е., Гринин А.Л., Коротаев А.В. Глобальные трансформации Мир-Системы и контуры нового мирового порядка // Политическая наука. 2024. № 2. С. 124-150.
[215] Frank A. G. 1998. ReOrient: Global economy in the Asian age. Berkeley: University of California Press, 1998. P.

мировым гегемоном. Действительно, председатель Си Цзиньпин избрал путь инициативы в качестве основного направления, а мирное развитие и взаимовыигрышное сотрудничество – в качестве основной цели. Он неоднократно подчеркивал, что Китай «выступает как за установление нового порядка международных отношений в соответствии со строгим соблюдением Устава ООН, так и за создание нового типа междержавных отношений с учетом интересов средних и небольших государств; поддерживает как развитие роли уже существующих международных организаций, так и создание новых площадок; подчеркивает необходимость прислушиваться и к требованиям других стран, и к голосу Китая; делать упор и на глобальное, и на национальное управление; поддерживает создание «китайского проекта» глобального управления» [216] . Председатель Си неоднократно подчеркивал также, что в мире постепенно формируется ряд центров развития, расстановка сил изменилась в пользу глобального мира и развития[217]. Национальную идеологию Китая отражают два ключевых слова речей Си Цзиньпина: мир и общее процветание[218], его цель – построение «китайской мечты», которая позволит Китаю реализовать следующее: «...Достичь целей всеобъемлющего построения среднезажиточного общества; стать социалистической страной, процветающей, демократической, цивилизованной и гармоничной; реализовать великое возрождение китайского национального сознания. Именно осуществить мечты превращения Китая в богатое и сильное государство, энергичное развитие китайской нации и создание счастливой жизни для народа»[219].

---

xxiv. Франк А.Г. Азия проходит полный круг – с Китаем как «Срединным государством» // Цивилизации. Вып. 5. Проблемы глобалистики и глобальной истории / ред. А.О. Чубарьян. М.: Наука, 2002. С. 192-203.

[216] Ли Янь. Концепция глобального управления Си Цзиньпина. Теоретическое содержание и практическая руководящая значимость // Свободная мысль. 2019. №2 (1674). С. 65-80.

[217] Си Цзиньпин. О государственном управлении. Пекин: Издательство литературы на иностранных языках, 2014. Т. 1. С. 368.

[218] Ван Циньи, Тао Ин Имидж Китая в политических текстах Си Цзиньпина // Политическая лингвистика. 2018. №4. С. 147-154.

[219] 习近平在十二届全国人大一次会议闭幕会上发表重要讲话 / 人民网people [Китайская мечта, мечта народа. Выступление Си Цзиньпина на заключительном заседании ВСНП 12-го созыва] [Электронный ресурс] / People.com.cn. URL: http://lianghui.people.com.cn/2013npc/n/2013/0317/c357183-20816399.html (дата обращения: 22.09.2024).

Активная внешнеполитическая и внешнеэкономическая деятельность КНР вызывает далеко не однозначные оценки в зарубежных СМИ. Постоянно тиражируется идея о «китайской угрозе», что не соответствует действительности, потому что в современной внешней политике для КНР остается приоритетом обеспечение мирной международной обстановки. Конкретные проявления этого — многосторонняя дипломатия и дипломатия развития. Прагматичная миролюбивая внешняя политика КНР, определяемая моделью преемственности идей, Дэн Сяопина, направлена прежде всего на обеспечение благосостояния китайского народа [220] . При этом Китай продолжает открываться внешнему миру, «стремится к созданию нового типа международных отношений, основанных на взаимном уважении, беспристрастности, справедливости и беспроигрышном сотрудничестве, а также к формированию так называемого Сообщества человеческой судьбы» [221] . Китай стремится участвовать в глобальном управлении, развиваются и расширяются гуманитарное сотрудничество и культурный взаимообмен КНР с другими странами [222] . Китай позиционируется «как глобальная сверхдержава, что соотносится с идентичностью «китаецентризма», только уже совершенно в другом ракурсе – не закрытой для внешнего мира страны, которая не нуждается в активном взаимодействии с другими государствами, а наоборот, страны, сделавшей огромный рывок в развитии собственной экономики, страны с устойчивой политической системой, основанной на понятных народу ценностях, страны, которая не

[220] Ю Хань. Развитие современной внешней политики КНР // Terra Linguistica. 2016. №1 (239). С. 84-91.
[221] У До. Особенности внешнеполитической стратегии Си Цзиньпина // Общество: политика, экономика, право. 2018. №12 (65). С. 31-34.
[221] 胡锦涛在第十次驻外使节会议上的讲话 / People.com.cn. 30.08.2004. [Выступление Ху Цзиньтао на X совещании дипломатических посланников] [Электронный ресурс] / People.com.cn. 30.08.2004. URL: http://www.people.com.cn/GB/shizheng/1024/2748201.html (дата обращения: 25.10.2024).
[222] 聚焦十九大 专家解读：中国的大国外交彰显哪些理念? / CCTV.com. [Экспертная интерпретация: каковы концепции великой дипломатии Китая?] [Электронный ресурс] / CCTV.com. URL: http://news.cctv.com/2017/10/22/ARTIyWPLzxmXX971DmC7wpyc171022.shtml (дата обращения 15.11.2024). URL: https://english.news.cn/20240925/f090570040244339999dddcb92aaa6beb/c.html (дата обращения 15.11.2024).

только готова быть вовлеченной в глобальные мировые процессы, но и стоять в их авангарде»[223].

28 сентября 2024 года член Политбюро ЦК КПК, министр иностранных дел Ван И. принял участие в общих дебатах 79-й сессии Генеральной Ассамблеи ООН в штаб-квартире ООН в Нью-Йорке и изложил позиции Китая по совершенствованию глобального управления. Он отметил, «что перед лицом все более серьезных глобальных вызовов Китай никогда не остается в стороне, а наоборот принимает участие в глобальном управлении с беспрецедентной активностью. Председатель Си Цзиньпин последовательно выдвинул Инициативу по глобальному развитию, Инициативу по глобальной безопасности и Инициативу глобальной цивилизации, внося интеллектуальный вклад в решение различных непростых проблем, стоящих перед человечеством, и придавая импульс Китая совершенствованию глобального управления. Перед лицом односторонней травли, в частности санкций и блокад, Китай решительно поддерживает все страны в защите их законных прав, сохранении справедливости и открытости международной системы, укреплении общедоступности и согласованности глобального развития, совместном противодействии технологическим блокадам и совместном сопротивлении разъединению и разрыву цепочек» [224].

Анализ дискурса международной составляющей докладов Генеральных секретарей Компартии Китая на XV-XIX съездов показывает: «- преемственность «мирной» риторики; – следование принципам концепции «мирного возвышения», несмотря на смену формулировки на «мирное развитие»; – эволюционную, а не революционную тенденцию во внешней политике; – стремление не к копированию какой-либо существующей дипломатической модели, а к ее адаптации (как и политического строя) к реалиям китайского менталитета («дипломатия с китайской спецификой»); …

---

[223] Full text of Xi Jinping's report at 19th CPC National Congress / Xinhua.net. 03.11.2017. URL: http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm (дата обращения 15.11.2024).

[224] Ван И: Вносить вклад Китая в совершенствование глобального управления / Ministry of Foreign Affairs of the People’s Republic of China. 29.09.2024. URL: https://www.fmprc.gov.cn/rus/zxxx/202410/t20241003_11502535.html (дата обращения 15.11.2024).

– готовность предложить миру новую модель взаимодействия между странами»[225].

Эти принципы явственно проявляются и в недавних выступлениях Председателя Си[226,227]. В своем выступлении на форуме БРИКС в Казани он отметил: «Сегодня, когда мир вступает в новый период турбулентности и трансформации, мы стоим перед судьбоносным выбором. Пусть будет таким турбулентным, или вернуть его в русло мирного развития? Кстати, насколько помнится, русский писатель Чернышевский в романе «Что делать» делает героя человеком с исключительно твердой волей и решительностью в достижении своих целей. Вот сила духа таковая сегодня нам очень нужна. Чем сложнее эпоха, тем важнее вести упорную борьбу, проявляя непоколебимую волю, авангардную смелость и способность реагировать на изменения … для укрепления единства и взаимодействия стран «Глобального Юга» и авангарда в трансформации глобального управления»[228].

Выводы по главе 3

По мере распространения информационных войн и их интенсификации они привлекают все большее внимание не только политиков и представителей СМИ, но и научного и экспертного сообщества. Изучаются и разрабатываются не только тактики и инструменты ведения информационных войн, но и противодействия им, ограничения недружественного информационного воздействия на население страны,

---

[225] Помозова Н. Б. Отражение внешнеполитического вектора в дискурсе докладов на XV – XIX съездах Коммунистической партии Китая // Государственное и муниципальное управление. Ученые записки. 2018. №4. С. 156-161.

[226] Flash: Xi Calls For Building Brics Into Global South's Major Venue Of Cooperation And Vanguard For Global Governance Reform / Xinhua. 23.10.2024. URL: https://english.news.cn/20241023/95b3fdb38c7847918c07ee6b681972ef/c.html (дата обращения 15.11.2024).

[227] Xinhua Headlines: "Greater BRICS cooperation" contributes vitality, wisdom to global governance / Xinhua. 22.10.2024. URL: https://english.news.cn/20241022/bedf79fd9f354a72831c0bcbfc6e8fe2/c.html (дата обращения 15.11.2024).

[228] Действовать с широким кругозором и решительностью во имя высококачественного развития сотрудничества Большого БРИКС / Выступление на 16-ой встрече лидеров стран БРИКС, Председатель КНР Си Цзиньпин (23 октября 2024 г., Казань). URL: https://by.china-embassy.gov.cn/rus/zgxx/202410/t20241024_11514992.htm (дата обращения 15.11.2024).

участвующей (или оказавшейся вынужденной участвовать, т.е. втянутой) в информационной войне. Если кибервойны исследуются преимущественно с точки зрения кибернетических технологий, в информационных войнах значительно более сложным объектом исследований оказываются социогуманитарные технологии, в том числе психологические.

Актуальность изучения информационных войн существенно возросла в 21 веке, особенно после финансово-экономического кризиса 2008–2009 годов, когда гегемония США пошатнулась, мировой гегемон оказался не в состоянии справиться с распространением кризиса и его последствиями, и развивающиеся страны пришли на помощь, что вызвало у них закономерное стремление обеспечить больший учет своих интересов на мировой политической и экономической арене, содействовать реконфигурации мирового порядка в направлении выстраивания его на более равных и справедливых основаниях. Однако США (и страны коллективного Запада), не желая уступать свое привилегированное положение, обратились к широкому спектру инструментов ведения информационных войн, выбрав основными мишенями Китай и Россию, и эта ситуация вряд ли изменится в ближайшем будущем. С одной стороны, информационная война представляется более «гуманной», поскольку большинство ее инструментов не подразумевает человеческих жертв (хотя использование кибертехнологий может иметь гуманитарные последствия, особенно в случаях, когда кибератаки направлены на медицинский сектор или другие критически важные объекты гражданской инфраструктуры, такие как электроснабжение, водоснабжение и санитарные системы). Однако при этом войны «нового поколения» стали значительно более сложными, непредсказуемыми, и не регулируются международным гуманитарным законодательством. Это обусловливает необходимость дальнейшего изучения данного явления, выработку научно обоснованных социогуманитарных технологий, направленных на защиту населения страны от информационных кампаний страны-противника, и осознания того, что рост «беспорядка», хаотизации

Мир-Системы является «новой нормальностью» в период глобальных трансформаций и перехода к многополярному мировому порядку.

В контексте глобальных социальных трансформаций, связанных в том числе с естественным социально-политическим процессом реконфигурации Мир-Системы и сопровождающимся в его ходе глобальным геополитическим обострением и усилением значимости идеолого-мировоззренческой составляющей информационного противоборства, не приходится ожидать ослабевания интенсивности развязываемых Западом информационных войн в ближайшие 10–20 лет. Усиление идеолого-мировоззренческого аспекта информационных войн находит отражение в интенсивности соответствующих научных публикаций. В целом потенциальные угрозы национальной безопасности, связанные с внешним информационно-психологическим воздействием, могут стать критическими только в случае наличия серьезных факторов, способствующих социально-экономической и/или социально-политической нестабильности в целевых странах, подвергшихся таким атакам. Важно отметить, что ни Россия, ни Китай не имеют таких фундаментальных оснований для такой дестабилизации. Однако следует учитывать, что угрозы, связанные с разрушительными атаками в цифровой и технологической сфере, создают для России все больше рисков в области обеспечения безопасности критической инфраструктуры.

Важно, что перспективным для России и Китая направлением информационных войн является наступательный вектор идеолого-мировоззренческой войны, реализуемой путем формирования и продвижения нарративов справедливого мироустройства и партнерства цивилизаций как для интеллектуально-элитной, так и массовой аудитории коллективного Запада. Вместе с тем, данное направление представляется наиболее наукоемким в информационно-психологической сфере, поскольку связано не столько с социотехническими вопросами формирования самих нарративов, сколько с научным обеспечением их идеологической основы.

ЗАКЛЮЧЕНИЕ

Показана комплексность явления информационных войн, неизменность их природы даже в условиях наимасштабнейших социальных трансформаций последних десятилетий, но при этом выявлено изменение направленности их информационно-психологической составляющей в сторону фундаментальных, когнитивно-мировоззренческих основ социального поведения и целеполагания жизни человека, что тем более важно в условиях релятивизации базовых духовно-нравственных ценностей и патриотизма.

В этой связи технологическое развитие, прежде всего, в сфере цифровизации, резко расширяет пространство возможностей информационных войн, однако, слабо влияет на их содержание.

Показано, что многосферность явления информационных войн создает трудности для их регулирования при том, что информационные войны могут не сопровождать конкретные военные действия. Они реализуются в значительной мере в глобальном цифровом пространстве, которое в настоящее время практически не регулируется.

Выявлен наиболее перспективный подход к рассмотрению данного явления с точки зрения современных процессов глобального развития и повестки борьбы за обновленный, более справедливый мировой порядок, который продвигается Россией, Китаем и другими странами БРИКС. Это мир-системный подход для включения информационных войн в более широкий контекст современных глобальных социальных трансформаций.

В работе впервые проведена системная классификация процессов глобальных социальных трансформаций и соответствующие им изменения в характере информационных войн.

Сформулированы рекомендации для практического применения Китаем, Россией и странами Глобального Юга в противостоянии информационным войнам и ведению их против неоимпериалистических сил коллективного Запада, включающими не только и не столько ограничения

собственного информационного пространства, сколько формирование и продвижение собственной идеологии глобального развития.

Показано, что многообразие современной терминологии информационных войн, а также их частую «мимикрию» под социокультурный обмен стран и цивилизаций и иные проявления позитивной мягкой силы заставляют предложить уточняющую их классификацию. Информационные войны целесообразно разделять по направленности на информационно-психологические, то есть направленные на сознание человека и информационно-технологические, направленные на информационную инфраструктуру. Первые включают 1) военную пропаганду, 2) информационно-экстремистские или террористические действия, 3) информационно-мировоззренческие войны, (включающие, в свою очередь, а) социокультурные войны, б) «войны памяти» или войны исторических нарративов, в) информационно-политические войны); 4) информационно-экономические войны, ведущиеся против хозяйствующих субъектов или экономического потенциала в целом стран-конкурентов; 5) информационно-экологические войны, направленные на дискредитацию природного потенциала. Круг ключевых технологий, используемых для подготовки и ведения информационных войн, определяется прежде всего глобальным технологическим прогрессом в цифровизации и расширяющимся доступом широких слоев населения разных стран к информационной среде.

Во второй половине XX века становление информационного общества, а в XXI веке – цифрового общества, что является ключевой глобальной трансформацией современности, цифровизация промышленности и управления, а также научные достижения в области психологии и социологии создали условия для появления как новых объектов для информационных атак (цифровая инфраструктура экономики и, особенно, промышленности, финансов, госуправления, социальные сети, базы личных данных и т.д.), так и для технологизации информационно-психологического воздействия вплоть для использования технологий искусственного

интеллекта для пропаганды или создания ложных нарративов. При этом круг объектов направленности информационно-психологических войн практически не со времен Второй мировой войны и даже с более раннего периода активизации противостояния России с коллективным Западом в XIX веке. В то же время с усилением значимости экологической составляющей жизни человечества, новыми трендами декарбонизации и экологизация появилась новая сфера информационного воздействия – осознание природно-экологической защищенности и комфорта населения противоборствующих и конкурирующих стран.

Очевидно, что к концу 2024 года США и их союзники достигли пика интенсивности информационных войн с Россией, Китаем и другими государствами, которые идеологически противостоят западным странам. США, Россия и Китай, будучи крупнейшими военно-политическими акторами, следуют различным стратегиям в ведении информационных войн, основывающиеся на их идеолого-мировоззренческой базе и технологических возможностях. Данные стратегии следующим образом: 1) Наступательно-гегемонистская стратегия США, исходящая из стремления к глобальному доминированию; 2) Оборонительно-технологическая стратегия Китая, исходящая из принципа не навязывания другим странам своих нарративов, возможности для защиту внутреннего киберпространства и концентрации на информационно-технологических аспектах военного противостояния; 3) Оборонительно-наступательная стратегия современной России, связанная прежде всего, в стремлении защитить внутреннее информационное пространство, а также продвигать нарративы и контр-нарративы во всем мире, используя прежде всего цифровые площадки. Начавшийся в 2025 году позитивный диалог российского руководства с администрацией США пока не имеет стабильности, необходимой для стратегической смены ситуации. Руководство Китая строго контролирует информационное пространство в стране с помощью цензуры, блокировки новостных сайтов и социальных сетей. Эти меры ограничивают доступ к нежелательной информации, что

делает Китай более защищенным от информационных атак со стороны Запада. В то же время, и России, и Китаю, в условиях консолидации Глобального Большинства, не хватает наступательных информационно-психологических действий для повышения успешности своего лидерства в борьбе за новый, более справедливый миропорядок. Вместе с тем, США и коллективный Запад также подвержен информационно-психологическим и информационно-технологическим атакам ввиду как развитости и открытости своего киберпространства, так и его идеолого-мировоззренческого кризиса. Ввиду этого, секьюритизация и суверенизация киберпространства, повышение уровня цензуры и контроля охватывает как Россию, Китай и ряд других стран Глобального Большинства, так и страны коллективного Запада, особенно Европейского Союза.

Показано, что в контексте глобальных социальных трансформаций, связанных в том числе с естественным социально-политическим процессом реконфигурации Мир-Системы и сопровождающимся в его ходе глобальным геополитическим обострением и усилением значимости идеолого-мировоззренческой составляющей информационного противоборства, не приходится ожидать ослабевания интенсивности развязываемых Западом информационных войн в ближайшие 10-20 лет. Усиление идеолого-мировоззренческого аспекта информационных войн находит отражение в интенсивности соответствующих научных публикаций. В целом потенциальные угрозы национальной безопасности, связанные с внешним информационно-психологическим воздействием, могут стать критическими только в случае наличия серьезных факторов, способствующих социально-экономической и/или социально-политической нестабильности в целевых странах, подвергшихся таким атакам. Важно отметить, что ни Россия, ни Китай не имеют таких фундаментальных оснований для такой дестабилизации. Однако следует учитывать, что угрозы, связанные с разрушительными атаками в цифровой и технологической сфере, создают

для России все больше рисков в области обеспечения безопасности критической инфраструктуры.

В связи с вышеизложенным, весьма перспективным для России и Китая направлением информационных войн является наступательный вектор идеолого-мировоззренческой войны, реализуемой путем формирования и продвижения нарративов справедливого мироустройства и партнерства цивилизаций как для интеллектуально-элитной, так и массовой аудитории коллективного Запада. Вместе с тем, данное направление представляется наиболее наукоемким в информационно-психологической сфере, поскольку связано не столько с социотехническими вопросами формирования самих нарративов, сколько с научным обеспечением их идеологической основы.

Наиболее перспективными и эффективными способами борьбы с угрозами, связанными с информационными войнами, и обеспечения национальной безопасности, являются:

– Повышение критического мышления и медиа-грамотности среди населения, чтобы люди могли легче выявлять фейки, дезинформацию и пропаганду.

– Регулирование использования информационных технологий и социальных медиа с целью предотвращения распространения ложной информации и негативного воздействия на общественное мнение.

– Разработка и применение систем фильтрации контента, анализа данных и алгоритмов искусственного интеллекта.

– Сотрудничество между правительством, научным сообществом и предприятиями для разработки и внедрения комплексных стратегий по защите от информационных войн.

– Обучение и подготовка специалистов в области информационной безопасности и киберзащиты.

– Ключевым элементом противодействия информационным войнам будет разработка и принятие международных норм регулирования конкуренции между странами в информационном пространстве.

БИБЛИОГРАФИЯ

Нормативные правовые акты, стратегические документы, официальные выступления национальных лидеров и высших должностных лиц

1. Ван И: Вносить вклад Китая в совершенствование глобального управления / Ministry of Foreign Affairs of the People's Republic of China. 29.09.2024. URL: https://www.fmprc.gov.cn/rus/zxxx/202410/t20241003_11502535.html (дата обращения 15.11.2024).
2. Владимир Путин принял участие в пленарной сессии юбилейного, XX заседания Международного дискуссионного клуба «Валдай» / Официальный сайт Президента России. 05.10.2023. URL: http://kremlin.ru/events/president/news/72444 (дата обращения 16.11.2024).
3. 胡锦涛在第十次驻外使节会议上的讲话 / People.com.cn. 30.08.2004. [Выступление Ху Цзиньтао на X совещании дипломатических посланников] [Электронный ресурс] / People.com.cn. 30.08.2004. URL: http://www.people.com.cn/GB/shizheng/1024/2748201.html (дата обращения: 25.10.2024).
4. Действовать с широким кругозором и решительностью во имя высококачественного развития сотрудничества Большого БРИКС / Выступление на 16-ой встрече лидеров стран БРИКС, Председатель КНР Си Цзиньпин (23.10.2024, г. Казань). URL: https://by.china-embassy.gov.cn/rus/zgxx/202410/t20241024_11514992.htm (дата обращения 16.11.2024).
5. Заседание саммита БРИКС в узком составе / Официальный сайт Президента России. 23.10.2024. URL: http://kremlin.ru/events/president/transcripts/75374 (дата обращения 16.11.2024).

6. 习近平在十二届全国人大一次会议闭幕会上发表重要讲话 / 人民网 people [Китайская мечта, мечта народа. Выступление Си Цзиньпина на заключительном заседании ВСНП 12-го созыва] [Электронный ресурс] / People.com.cn. URL: http://lianghui.people.com.cn/2013npc/n/2013/0317/c357183-20816399.html (дата обращения: 22.09.2024).
7. Письмо постоянных представителей Казахстана, Китая, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 9 января 2015 года на имя Генерального секретаря / ГА ООН. Шестьдесят девятая сессия. Пункт 91 повестки дня Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности. URL: https://www.mid.ru/ru/foreign_policy/un/organs/1582262/ (дата обращения 06.11.2024).
8. 习近平. 习近平谈治国理政. 北京.: 外语教学与研究出版社 [Си Цзиньпин. О государственном управлении. Пекин: Издательство литературы на иностранных языках]. - 2014. - Т.1. – p. 646
9. Соглашение между правительствами государств—членов ШОС о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 года / Бюллетень международных договоров». 2012. № 1. С. 13—21.
10. Указ Президента Российской Федерации № 24 от 10.01.2000 «О Концепции национальной безопасности Российской Федерации» URL: https://docs.cntd.ru/document/901751578 (дата обращения 14.11.2024)
11. Указ Президента Российской Федерации № 400 от 02.07.2021 «О Стратегии национальной безопасности Российской Федерации» URL: https://docs.cntd.ru/document/420327289#6520IM (дата обращения 14.11.2024)
12. Указ Президента Российской Федерации № 537 от 12.05.2009 «О Стратегии национальной безопасности Российской Федерации до 2020

года» URL: https://docs.cntd.ru/document/902156214 (дата обращения 14.11.2024)

13. Указ Президента Российской Федерации № 683 от 31.12.2015 «О Стратегии национальной безопасности Российской Федерации» URL: https://docs.cntd.ru/document/420327289#6520IM (дата обращения 14.11.2024)
14. Указ Президента Российской Федерации от 05.12.2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения 31.10.2024).
15. Федеральный закон от 26.07.2017 N 187-ФЗ (ред. от 10.07.2023) «О безопасности критической информационной инфраструктуры Российской Федерации»
16. Указ Президента Российской Федерации от 30.11.2016 г. N 640 "Об утверждении Концепции внешней политики Российской Федерации". URL: http://kremlin.ru/acts/bank/41451 (дата обращения: 1.10.2025).
17. Послание Президента РФ Федеральному Собранию от 01.12.2016 "Послание Президента Российской Федерации Федеральному Собранию" URL: https://www.consultant.ru/document/cons_doc_LAW_207978/ (дата обращения: 1.09.2025).
18. Указ Президента Российской Федерации от 09.05.2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы». URL: http://kremlin.ru/acts/bank/41919 (дата обращения: 1.09.2025).
19. Указ Президента РФ от 12.04.2021 г. № 213 "Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности". URL: http://kremlin.ru/acts/news/65350 (дата обращения: 1.10.2025).

20. Указ Президента РФ от 02.07.2021 г. N 400 "О Стратегии национальной безопасности Российской Федерации" URL: http://www.kremlin.ru/acts/bank/47046 (дата обращения: 11.10.2025).
21. Flash: Xi Calls For Building Brics Into Global South's Major Venue Of Cooperation And Vanguard For Global Governance Reform / Xinhua. 23.10.2024. URL: https://english.news.cn/20241023/95b3fdb38c7847918c07ee6b681972ef/c.html (дата обращения 15.11.2024).
22. Full text of Xi Jinping's report at 19th CPC National Congress / Xinhua.net. 03.11.2017. URL: http://www.xinhuanet.com/english/special/2017-11/03/c_136725942.htm (дата обращения 15.11.2024).
23. National Security Strategy// White House, Washington. October 12, 2022. URL: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf (дата обращения: 20.10.2025).
24. Regulation (eu) 2022/2065 of the european parliament and of the council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng (дата обращения: 1.10.2025)
25. U.S. Department of Defense. 2023 Cyber Strategy of the Department of Defense. Summary. Washington, D.C.: U.S. Department of Defense, 2023. URL: https://media.defense.gov/2023/Sep/12/2003299076/-1/-1/1/2023_DOD_Cyber_Strategy_Summary.PDF
26. U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2023. P. 1. URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-Department-Of-Defense-Strategy-For-Operations-In-The-Information-Environment.Pdf
27. U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2023.

URL: https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-Department-Of-Defense-Strategy-For-Operations-In-The-Information-Environment.Pdf

28. U.S. Department of Defense. Strategy for Operations in the Information Environment. Washington, D.C.: Pentagon, 2016. URL: https://dod.defense.gov/portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf

Статьи в журналах и сборниках, монографии

29. Акаев А. А. Большие циклы конъюнктуры и инновационно-циклическая теория экономического развития Шумпетера-Кондратьева // Экономическая наука современной России. 2013. №2 (61). С. 7-29.
30. Акаев А. А. Математические основы инновационно-циклической теории экономического развития Шумпетера – Кондратьева // Кондратьевские волны: аспекты и перспективы / Акаев А. А., Гринберг Р. С., Гринин Л. Е., Коротаев А. В., Малков С. Ю. (ред.). Волгоград: Учитель, 2012. С. 110-135.
31. Акаев А. А. Стратегическое управление устойчивым развитием на основе теории инновационно-циклического экономического роста Шумпетера-Кондратьева // Экономика и управление. 2011. №3 (65). С. 4-10.
32. Акаев А. А. Эпохальные открытия Николая Кондратьева и их место в современной экономической науке // AlterEconomics. 2022. Т.19, №1. С. 11-39.
33. Акаев А. А., Садовничий В. А. Замкнутая динамическая модель для описания и расчёта длинной волны экономического развития Кондратьева // Вестник Российской академии наук. 2016. Т. 86, №10. С. 883-896.

34. Акаев А. А. Анализ состояния и перспектив мирового экономического роста на основе теории Шумпетера-Кондратьева // Экономика и управление. 2011. №2. С. 9-15.
35. Алаудинов А.А., Манойло А.В. Когнитивная и ментальная составляющие современной гибридной войны// Вопросы политологии. 2024. Т. 14. № 2 (102). С. 583-591;
36. Алексеев А. П., Алексеева И. Ю. Информационная война в информационном обществе // Вопросы философии. 2016. №11.
37. Алексеев А.П. Общество в условиях информационной войны: вопрос интеллектуального суверенитета // Философия и общество. 2017. № 2 (83). С. 18–27.
38. Алексеев А.П., Алексеева И.Ю. Цифровизация и когнитивные войны // Философия и общество. 2021. №4 (101). С. 39–51.
39. Ананьева Е. В. Сумеют ли США и Британия сделать из России страну-изгой? // Научно-аналитический вестник Института Европы РАН. 2018. №2. С. 5–12.
40. Ананьева Е. В., Годованюк К. А. Матрёшка “дела Скрипалей” // Современная Европа. 2018. №3(82). С. 16–26.
41. Аникин В. И., Сурма И. В. Национальная безопасность России: новые подходы в меняющемся мире // Вопросы безопасности. — 2016. — № 3. — С. 1–18.
42. Аникин В.И. О некоторых практических аспектах философии информационной цивилизации в международных отношениях // Человечество на границе тысячелетий: диалог цивилизаций: сборник материалов научно-практической конференции. Киев. 2003. С. 42–46.
43. Аникин В.И., Абдеев Р.Ф., Сурма И.В. Философские аспекты информационной цивилизации и современные проблемы управления в ракурсе глобальной безопасности // Вопросы безопасности. 2017. № 2. С. 44–54.

44. Аникин В.И., Моисеев А.В., Сурма И.В., Семенова О.В. Современные подходы в принятии внешнеполитических решений в Российской Федерации. М.: Русайс, 2021. 240 с.
45. Антонович П. И. (2011). О современном понимании термина «кибервойна» // Вестник Академии военных наук. 2011. № 2. С. 89–96.
46. Арон Р. Опиум интеллектуалов // Логос. 2005. № 6. С. 182–205.
47. Бажанов Е.П. Россия между Западом и Востоком // Современный мир и геополитика. М.: Канон+, 2015. С. 9–47.
48. Бажанов Е.П., Бажанова Н.Е. Диалог и столкновение цивилизаций. М.: Весь мир, 2013. 272 с.
49. Бажанов Е.П., Бажанова Н.Е. Международные отношения в XXI веке. М.: «Восток-Запад», 2011.
50. Бажанов Е.П., Бажанова Н.Е. Мир и война. М.: Восток-Запад, 2011. 335 с.
51. Барабаш В. В., Котеленец Е. А. (2016). Информационные войны и медийное пространство: теоретические аспекты новейших изменений // Известия высших учебных заведений. Поволжский регион. Гуманитарные науки. 2016. №3(39). С. 150–158.
52. Барабаш В. В., Котеленец Е. А., Лаврентьева М. Ю. Информационная война: к генезису термина // Знак: проблемное поле медиаобразования. 2019. № 3(33). С. 76–89.
53. Баранов Е.Г. Информационно-психологическое воздействие: сущность и психологическое содержание // Национальный психологический журнал. 2017. № 1 (25). С. 25–31.
54. Баришполец В.А. Информационно-психологическая безопасность: основные положения // Информационные технологии. 2013. №5. С. 62–107.
55. Бартош А. А. Стратегическая культура как инструмент «мягкой силы» российской дипломатии // Вестник Московского университета. Серия 12. Политические науки. 2019. № 4. С. 19–31.

56. Бедрань В. В. Механизмы информационной войны США против Ирака в начале XXI в. // Вестник РГГУ. Серия: Политология. История. Международные отношения. 2012. №7 (87). С. 186–195.
57. *Бедрицкий А.В.* Информационная война: концепции и их реализация в США. М.: РИСИ, 2008. 187 с.
58. Белл Д. Социальные рамки информационного общества // Новая технократическая волна на Западе. Москва: Прогресс, 1986. С. 330-342.
59. Бжезинский З. Великая шахматная доска: господство Америки и его геостратегические императивы. М.: Международные отношения, 1999. 256 с.
60. Бирюков С.В., Чирун С.Н., Андреев А.В. Информационно-пропагандистские стратегии и технологии украинской элиты в информационной войне с Россией// PolitBook. 2023. № 2. С. 66-86.
61. Богатуров А.Д. «Украинский вызов» и альтернативы внешней политики России // Научно-образовательный форум по международным отношениям. 2014. Т. 12. № 39. С. 6–16.
62. Богатуров А.Д., Аверков В.В. История международных отношений 1945-2017. М.: Аспект Пресс, 2017.
63. Бутусов А. В. Политический характер информационных войн в сфере спорта // Вестник Тамбовского университета. Серия: Общественные науки. 2018. №4(14). С. 76–79.
64. Бухарин С.Н., Глушков А.Г., Ермолаев И.Д. Информационное противоборство. Кн. 2. М.: Полиори, 2004. 501 с.
65. Валлерстайн И. Анализ мировых систем и ситуация в современном мире. СПб.: Университетская книга, 2001. 416 с.
66. Валлерстайн И. Есть ли будущее у капитализма? М.: Ин-т Гайдара, 2015. 320 с.
67. Ван Циньи, Тао Ин Имидж Китая в политических текстах Си Цзиньпина // Политическая лингвистика. 2018. №4. С. 147-154.

68. Воинов Д. Е. «Мягкая сила» Игр «Сочи-2014» и зарубежные медиа: анализ политико-информационного фона российской Олимпиады // Вестник Московского университета. Серия 25. Международные отношения и мировая политика. 2015. № 7(2). С. 155–181.
69. Володин А.Г. Становление полицентрического мироустройства как продолжение геополитических процессов XX века // Контуры глобальных трансформаций: политика, экономика, право. 2019. Т. 12. № 4. С. 6–31.
70. Выходец Р. С., Панцерев К. А. Сравнительный анализ современных концепций информационного противоборства // Евразийская интеграция: экономика, право, политика. 2022. Т. 16, № 4. С. 139–148.
71. Выходец Р.С. «Информационные доминанты» как инструмент информационно-психологических войн // Общественные науки и современность. 2022. № 4. С. 93–104.
72. Гавра Д.П. Информационное противоборство: современное понимание, характеристики, подходы к междисциплинарному познанию// Российская школа связей с общественностью. 2023. № 29. С. 10-26.
73. Гаврилов Л.А., Зарипов Р.И. Язык массовой коммуникации и информационная война// Москва, 2023.
74. Гаврилова С.М., Закаурцева Т.А. Италия: опыт автономий как пример национально-государственного устройства // Вестник Дипломатической академии МИД России. Россия и Мир. 2017. № 2 (12). С. 71–80.
75. Гадзацев К. В. Политическое давление и информационная война США против России на европейском газовом рынке: состояние и перспективы // Информационные войны. 2020. №1. С. 11–17.
76. Галаганова С.Г. Лингвистическое программирование в информационной войне// Вестник Академии военных наук. 2024. № 1 (86). С. 43-46.
77. Глазьев С. Ю. Адаптация российской экономики к смене технологических и мирохозяйственных укладов // Научные труды Вольного экономического общества России. 2023. Т. 244, №6. С. 95-102.

78. Глазьев С. Ю. Глобальная трансформация через призму смены технологических и мирохозяйственных укладов // AlterEconomics. 2022. Т. 19. № 1. С. 93-115.
79. Глазьев С. Ю. Мирохозяйственные уклады в глобальном экономическом развитии // Экономика и математические методы. 2016. Т. 52, №2. С. 3-29.
80. Глазьев С. Ю. Ноономика как стержень формирования нового технологического и мирохозяйственного укладов // Экономическое возрождение России. 2020. № 2(64). С. 15-32.
81. Глазьев С. Ю. О текущем положении России в мировой гибридной войне и создании необходимых условий для нашей победы // Глобальный конфликт и контуры нового мирового порядка: XX Международные Лихачевские научные чтения, 9–10 июня 2022 г. Санкт-Петербург: СПбГУП, 2022. С. 55-58.
82. Глазьев С. Ю. Перспективы становления в мире нового VI технологического уклада // МИР (Модернизация. Инновации. Развитие). 2010. №2. С. 4-10.
83. Глазьев С. Ю. Приоритеты опережающего развития российской экономики в условиях смены технологических укладов // Экономическое возрождение России. 2019. №2 (60). С. 12-16.
84. Глазьев С. Ю. Рывок в будущее. Россия в новых технологическом и мирохозяйственном укладах. М.: Книжный мир, 2018. 768 с.
85. Глазьев С. Ю. Современная теория длинных волн в развитии экономики // Экономическая наука современной России. 2012. №2 (57). С. 27-42.
86. Глазьев С. Ю., Айвазов А. Э., Беликов В. А. (2019). Циклически-волновые теории экономического развития и перспективы мировой экономики. Предсказуемо ли среднесрочное и долгосрочное развитие мировой экономики // Научные труды Вольного экономического общества России. 2019. Т. 219, №5. С. 177-211.

87. Глазьев С. Ю., Косакян Д. Л. Состояние и перспективы формирования 6-го технологического уклада в Российской экономике // Экономика науки. 2024. Т.10, №2. С. 11-29.

88. Годованюк К. А. Кибербезопасность и борьба с дезинформацией: опыт Великобритании // Научно-аналитический вестник Института Европы РАН. 2019. №4. С. 87–92.

89. Гончарова И. В., Ницевич В. Ф., Судоргин О. А. Информационная война как инструмент политического противостояния в современном многополярном мире // Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление. 2024. Т. 11. №1. С. 19–31.

90. Гринин Л. Е. Кондратьевские волны, технологические уклады и теория производственных революций // Кондратьевские волны. 2012. №1. С. 222-262.

91. Гринин Л. Е. Размышления о трансформациях мирового порядка* Часть 1. Мировой порядок в прошлом и настоящем // Credo New. 2017. №1. С. 93-119.

92. Гринин Л. Е., Гринин А. Л. Кибернетическая революция и шестой технологический уклад // Историческая психология и социология истории. 2015. Т.8, №1. С. 172-197. С. 172-173.

93. Гринин Л. Е., Гринин А. Л. Новая волна революционных процессов в афразийской макрозоне нестабильности и ее влияние на смежные мир-системные зоны // История и современность. 2022. №3(45). С. 3-22.

94. Гринин Л. Е., Гринин А. Л. От рубил до нанороботов. Мир на пути к эпохе самоуправляемых систем: История технологий и описание их будущего. ООО «Издательство "Учитель"», 2015.

95. Гринин Л. Е., Гринин А. Л., Коротаев А. В. Кибернетическая революция, шестой длинный цикл Кондратьева и глобальное старение // AlterEconomics. 2022. Т.19, №1. С. 147-165.

96. Гринин Л. Е., Коротаев А. В. Социальная макроэволюция. Генезис и трансформации Мир-Системы. М.: Либроком/URSS, 2009.

97. Гринин Л. Е., Коротаев А. В. Циклы, кризисы, ловушки современной Мир-Системы: исследование кондратьевских, жюгляровских и вековых циклов, глобальных кризисов, мальтузианских и постмальтузианских ловушек. М.: URSS, 2019.

98. Гринин Л. Е., Коротаев А. В., Цирель С. В. Циклы развития современной Мир-Системы. М.: ЛИБРОКОМ/URSS, 2011.

99. Гринин Л.Е., Гринин А.Л., Коротаев А.В. Глобальные трансформации Мир-Системы и контуры нового мирового порядка // Политическая наука. 2024. № 2. С. 124-150.

100. Гришаева Л.Е. Устав ООН и новое мироустройство // Вестник РУДН. Серия: политология. 2015. Т.15. № 4. С. 92–102.

101. Громыко А.А. Глобальный мир: риски и возможности // Современная Европа. 2018. № 1. С. 137–147.

102. Громыко А.А. Дилеммы Европейского оборонного союза // Контуры глобальных трансформаций: политика, экономика, право. 2019. Т. 12. № 2. С. 6–28.

103. Грызлов В.М., Перцев А.Б. Информационное противоборство. История и современность // Вестник Академии военных наук. 2015. № 2. С. 124–128.

104. Демин К. А., Пушкарева И. Н., Тагильцева Ю. Р. Компьютерные игры военного жанра как элемент пропаганды в информационной войне России и США // Политическая лингвистика. 2016. № 5. С. 110–116.

105. Добреньков В. И. Система и стратегии национальной безопасности России в XXI в. // Вестник Московского университета. Серия 18. Социология и политология. 2013. №4. С. 5–36.

106. Довгань Е. Ф., Мороз Н.О. ОДКБ и информационная безопасность // Организация Договора о коллективной безопасности и планирование на случай чрезвычайных обстоятельств после 2014 г. / Е. Ф. Довгань, А. В.

Русакович (ред.). Женева – Минск: Женевский центр демократического контроля над вооруженными силами, Центр изучения внешней политики и безопасности, 2015. С. 207–236.

107. Дугин А.Г. Концептуальные подходы к понятию «цивилизация» // Вестник Московского университета. Сер. 18: Социология и политология. 2013. № 1. С. 33–41.
108. Егорова М.Р. Информационная война как угроза национальной безопасности страны в современном мире на примере конфликтов xxi века// Евразийский Союз: вопросы международных отношений. 2023. Т. 12. № 7 (53). С. 991-999.
109. Егорченков Д. А., Данюк Н. С. Теоретико-идеологические подходы к исследованию феномена" гибридных войн" и" гибридных угроз": взгляд из России // Вестник Московского университета. Серия 12. Политические науки. 2018. № 1. С. 26–48.
110. Емалетдинов Е.О., Дубровский Г.Д. Когнитивная война: сущность, понятие, особенности // Культура и природа политической власти: теория и практика. Екатеринбург, 2023. С. 236–241.
111. Жильцов С.С. Истоки украинского национализма // Вестник РУДН. Сер. Политические науки. 2014. № 4. С. 21–36.
112. Жильцов С.С. Технологии и механизмы борьбы за власть на Украине // Россия и современный мир. М.: Канон+, 2016. С. 451-470.
113. Задохин А.Г., Чиджиев Б. Геополитика симбиоза «периферия-центр» и перспективы многополярного мира // Мировая политика. 2016. № 1 (13). С. 55–63.
114. Закария Ф. Постамериканский мир будущего. М.: Европа, 2009. 280 с.
115. Зимбардо Ф., Ляйппе М. Социальное влияние. СПБ: «ПИТЕР», 2001. 448 с.
116. Зиновьева Е. Что не так с Глобальным цифровым договором?// РСМД, 31 октября 2024 URL:https://russiancouncil.ru/analytics-and-

comments/analytics/chto-ne-tak-s-globalnym-tsifrovym-dogovorom/ (дата обращения: 1.10.2025).

117. Иванов О.П. Россия и НАТО: новая парадигма отношений // Россия и современный мир, М.: Канон+, 2016. С. 44-59.
118. Иванов О.П. Россия и НАТО: точка невозврата // Обозреватель-Observer. 2015. № 1. С. 5–16.
119. Калинин О.И., Приходько М.В. Информационная война: коммуникативный, дискурсивный, когнитивный и культурно-идеологический аспекты// Военно-филологический журнал. 2023. № 1. С. 23-36.
120. Кандалов В. И., Карташова Д. А. Особенности реализации современных военных информационно-коммуникативных операций // Социально-гуманитарные знания. 2023. №9. С 69–72.
121. Капто А. С. Кибервойна: генезис и доктринальные очертания // Вестник Российской академии наук. 2013. Т. 83. №7. С. 616–616.
122. Караяни А.Г., Зинченко Ю.П. Информационно-психологическое противоборство в войне: история, методология, практика. М.: МГУ, 2007. 172 с.
123. Карпович О.Г. Роль США в украинском кризисе (2013–2014-е гг.) // Международные отношения. 2016. № 2. С. 179–188.
124. Карпович О.Г. Украинский кризис в контексте противостояния России и Запада // Вестник российской нации. 2016. № 6 (52). С. 197–205.
125. Карпович О.Г. Практика проведения США операций информационной войны в сфере внешней политики // Национальная безопасность / nota bene. 2017. № 1. С. 112–126.
126. Кастельс М. Информационная эпоха: экономика, общество и культура; пер. с англ. под науч. ред. Шкаратана О.И. М.: ГУВШЭ, 2000. 608 с.
127. Каткова Е. Ю., Юнюшкина А. С. Китайские концепции и возможности в информационной войне: соперничество КНР и США в киберпространстве

// Вестник Российского университета дружбы народов. Серия: Всеобщая история. 2022. Т. 14. № 2. С. 197–210.

128. Кафтан В. В., Погорелый А. П. Роль идеологии в современной информационной войне // Гуманитарные науки. Вестник Финансового университета. 2023. Т. 13, №6. С. 46–53.
129. Кириченко А. В. Информационно-психологические войны: современные тенденции и технологические возможности //Акмеология. 2015. №.4(56). С. 209–214.
130. Кондаков И.В., Соколов К.Б., Хренов Н.А. Цивилизационная идентичность в переходную эпоху: культурологический, социологический и искусствоведческий аспекты. М.: Прогресс-Традиция, 2011. 1024 с.
131. Коротаев А. В., Гринин Л. Е. Кондратьевские волны в мир-системной перспективе // Кондратьевские волны. Аспекты и перспективы. Волгоград: Учитель, 2012. С. 58-109.
132. Коротаев А. В., Гринин, Л. Е. Кондратьевские волны в мир-системной перспективе // Кондратьевские волны. Аспекты и перспективы. Волгоград: Учитель, 2012. С. 58-109.
133. Коротаев А. В., Малков А. С., Халтурина Д. А. 2019. Законы истории: Математическое моделирование развития Мир-Системы. Демография, экономика, культура. М.: ЛЕНАНД/URSS, 2019.
134. Коцюбинская Л.В. Понятие «Информационная война» в современной лингвистике: новые подходы // Политическая лингвистика. 2015. №4. С. 93–96.
135. Кочетков В. В. Глобализация в образовании: информационная война и "промывание мозгов" или доступ к мировым знаниям и благам цивилизации? // Вестник Московского университета. Серия 18: Социология и политология. — М.: Издательство Московского государственного университета, 2005. — № 1. — С. 144—159.

136. Кочетков В.В. Роль чемпионата мира по футболу 2018 г. в формировании имиджа России // Социологические исследования, 2020, № 7, С. 82-92.
137. Красовская Н. Р., Гуляев А. А. К вопросу классификации информационных войн // Социология науки и технологий. 2019. Т. 10. №. 2. С. 44–55.
138. Красовская Н. Р., Гуляев А. А., Лахтин А. Ю., Вакуленко А. Н. Технологии информационных войн против России // Власть. 2019. № 3. С. 42–47.
139. Крылова И. А. Информационно-психологические войны как фактор дезинтеграционных процессов в современном мире //Большая Евразия: развитие, безопасность, сотрудничество. 2021. №. 4-1. С. 106–110.
140. Крылова И. А. Информационные войны и безопасность России // Россия: тенденции и перспективы развития. 2016.Т. 11, №2. С. 116–121.
141. Крылова И. А. Новые виды войн и безопасность России // Знание. Понимание. Умение. 2016. №3. С. 58–71.
142. Кугушева А. От информационных войн к поведенческим // Информационные войны. 2016. №1. С. 11–22.
143. Кукарцева М.А. Политический нарратив – инструмент «формирования себя» в мировой политике // Обозреватель-Observer. 2013. № 4 (279). С. 100–109.
144. Кургинова Д.Ю. К вопросу о том, что такое русофобия// Каспийский регион: политика, экономика, культура. 2024. № 1 (78). С. 104-110.
145. Лаврентьева М. Ю. Особенности технологий и методов информационно-психологических войн СССР с Великобританией и США в период 1939–1953 гг. Автореф. … кандидата филологических наук. М., 2020. – 26 с.
146. Лайнбарджер П. Психологическая война. М.: Воениздат, 1962.
147. Лебедева М.М., Кузнецов Д.А. Трансрегионализм – новый феномен мировой политики // Полис. Политические исследования. 2019. № 5. С. 71–84.

148. Леонова О.Г. Кибервойна и противоборство в цифровом информационном пространстве // Информационное общество. 2018. №2. С. 43–46.
149. Лепский В.Е. Информационно-психологическая безопасность субъектов дипломатической деятельности // Дипломатический ежегодник – 2002. Сб. статей. – М.: Научная книга, 2003. С. 233–248.
150. Лепский В.Е. Технологии управления в информационных войнах (часть 1: от классической к постнеклассической рациональности) // Информационные войны. 2016. № 2 (38). С. 57–64.
151. Ли Янь. Концепция глобального управления Си Цзиньпина. Теоретическое содержание и практическая руководящая значимость // Свободная мысль. 2019. №2 (1674). С. 65-80.
152. Лукушин В.А. Внешнее информационное давление на российскую молодежь как инструмент глобального противоборства// Общественные науки и современность. 2023. № 3. С. 68-82.
153. Люлина А. Г., Ефименко Е. С. Интернет-цензура в современном Китае: жесткий контроль и гибкая система урегулирования // Вестник РУДН. Серия: Всеобщая история. 2022. Т. 14. №2. С. 175–188.
154. Манойло А. В. "Дело Скрипалей" как операция информационной войны // Российский социально-гуманитарный журнал. 2019. №1. С. 72–97.
155. Манойло А. В. Государственная информационная политика в особых условиях. М.: МИФИ, 2003.
156. Манойло А. В. Информационная война и новая политическая реальность (I) // Российский социально-гуманитарный журнал. 2021. №1. С. 100–132.
157. Манойло А. В. Информационная война как угроза российской нации // Вестник российской нации. 2016. №6. С 174–184.
158. Манойло А. В. К вопросу о содержании понятия «информационная война» // Дневник АШПИ. 2012. №28. С. 19–20.
159. Манойло А. В. К вопросу о содержании понятия «информационная война» // Современная Россия и мир: альтернативы развития

(Информационные войны в международных отношениях): сборник научных статей / под ред. Ю.Г. Чернышова. Барнаул: Изд-во Алт. ун-та, 2012. С. 18–19.

160. Манойло А. В. Технологии современных информационных войн // Политическая наука. 2017. № Спецвыпуск. С. 306–325.
161. Манойло А.В. "Киев за три дня" и "новая искренность Хёрша" как пример "управления ожиданиями" в операциях информационной войны// Российский социально-гуманитарный журнал. 2023. № 3.
162. Мартыненко Е. В. Характер информационной войны между Россией и США в Сирии // Общество: политика, экономика, право. 2016. №9. С. 9–12.
163. Меньшиков П.В., Михина Л.К. Система противодействия угрозам информационной безопасности КНР // Вестник ЗабГУ. 2022. Т. 28. №1. С. 124–139.
164. Мехтиева Н. Р. К. (2017). Информационные войны как" цифровой" аспект глобализации // Век глобализации. 2017. №3(23). С. 77–89.
165. Миронова Н.Г. О проблеме обеспечения когнитивной безопасности. On the Problem of Ensuring Cognitive Security // Экономика и управление: научно-практический журнал. 2021. № 1. С. 119–125.
166. Монина Л. В. Проблема обеспечения информационной безопасности России // Современная Россия и мир: альтернативы развития (Информационные войны в международных отношениях): сборник научных статей / под ред. Ю.Г. Чернышова. Барнаул: Изд-во Алт. ун-та, 2012. С. 29–34.
167. Мороз Н.О. Международно-правовые основы обеспечения международной информационной безопасности // Труд. Профсоюзы. Общество. 2016. № 1 (51). С. 77–81.
168. Мчедлова М.М. Модернизация: политическая реинтерпретация концептуальных оснований и российский цивилизационный контекст // Россия реформирующаяся. 2013. № 12. С. 80–110.

169. Назаретян А.П. Психология стихийного массового поведения. Лекции. М.: ПЕР СЭ, 2001. 112 с.
170. Найденкова К. В., Чугунов, В. В. Институциональные аспекты обеспечения кибербезопасности в РФ и за рубежом // Финансовая безопасность. Современное состояние и перспективы развития. Материалы VIII Международной научно-практической конференции Международного сетевого института в сфере ПОД/ФТ. Том 1. – М.: НИЯУ МИФИ, 2022. С. 240–252.
171. Неймарк М.А. «Мягкая сила» в мировой политике. Уточнение проблемного поля. Часть 1. // Обозреватель-Observer. 2016. № 1 (312). С. 31–42.
172. Неймарк М.А. «Умная сила»: к перспективам в мировой политике. Часть 2. // Обозреватель-Observer. 2016. № 2 (312). С. 67–77.
173. Ольшанский Д.В. Политическая психология. Екатеринбург: Деловая книга, 2001. 496 с.
174. Орехов В. В. " Партизанская тактика" информационной войны. Часть II: Информационная безопасность в эпоху Николая I // Ученые записки Крымского федерального университета имени В.И. Вернадского. Филологические науки. 2021. Т. 7. №3. С. 131–167.
175. Павловский А. А. Некоторые аспекты угроз информационной безопасности в международной сфере // Информационная безопасность как составляющая национальной безопасности государства: материалы Междунар. науч.-практ. конф., Минск, 11–13 июля 2013 г. : в 3 т. / Ин-т нац. безопасности Респ. Беларусь; редкол. С. Н. Князев (гл. ред.) [и др.]. Минск, 2013. Т. 2. С. 105–109.
176. Панарин И.Н. СМИ, пропаганда и информационные войны. М.: Поколение, 2012.
177. Помозова Н. Б. Отражение внешнеполитического вектора в дискурсе докладов на XV – XIX съездах Коммунистической партии Китая //

Государственное и муниципальное управление. Ученые записки. 2018. №4. С. 156-161.

178. Пономарева Е.Г. Вывихнутый век. Кто его вправит? М.: Книжный мир, 2016. 352 с.
179. Пономарева Е.Г., Рудов Г.А. «Принцип домино»: мировая политика на рубеже веков. М.: Канон+, 2016. 309 с.
180. Пономарева Е.Г., Рудов Г.А. «Цветные революции»: природа, символы, технологии // Обозреватель-Observer. 2012. № 3 (266). С. 36–48.
181. Почепцов Г.Г. Информационно-психологическая война. М.: СИНТЕГ, 2000. 179 с.
182. Почепцов Г.Г. Информационные войны. М.: Refl-buk; 2001. 574 с.
183. Сергеев И. В. Информационно-психологическая война как форма эскалации межгосударственных конфликтов //Информационные войны. 2015. №.2. С. 38–41.
184. Силков С.В. Информационная война // Социология: Энциклопедия. – Минск: Общество с ограниченной ответственностью «Книжный дом», 2003. – С. 385.
185. Сковородников А. П., Копнина Г. А. Лингвистика информационно-психологической войны: к обоснованию и определению понятия //Политическая лингвистика. 2016. №. 1. С. 42–50.
186. Сковородников А. П., Королькова Э. А. Речевые тактики и языковые средства политической информационно-психологической войны в России: этико-прагматический аспект (на материале «Новой газеты») // Политическая лингвистика. 2015. № 3 (53). С. 160–172.
187. Смакотина Н.Л. Глобальные социальные трансформации в контексте демографических изменений и урбанизации // Acta Biomedica Scientifica. 2022. Т. 7. № 3. С. 47–56.
188. Смирнов А. Информационно-психологическая война //Свободная мысль. 2013. №. 6. С. 81–96.

189. Современные международные отношения: учебник / под ред. Торкунова А.В., Мальгина А.В. М.: Аспект-Пресс, 2012. 688 с.
190. Соколов Д. В. Способы защиты российских национальных интересов от информационных угроз извне, спровоцированных в результате обострения восточно-украинского политического конфликта // Общество: политика, экономика, право. 2016. №3. С. 53–58.
191. Соловьёв А. В. Информационная война: понятие, содержание, проспектива // Пространство и время. 2010. №2. С. 75–81.
192. Степин В.С. Эпоха цивилизационных перемен и диалог культур. М.: ИНИОН РАН, 2009.
193. Сурмин Ю. П., Туленков Н. В. Теория социальных технологий: учебное пособие. Киев: МАУП, 2004. 605 с.
194. Суходолов А. П. Идеологическая функция средств массовой информации в условиях информационных войн // Вопросы теории и практики журналистики. 2015. Т. 4. №2. С. 117–126.
195. Тагильцева Ю. Р. Стратегии и тактики информационно-психологической войны в контексте российско-британских отношений // Экология языка и коммуникативная практика. 2018. №4. С. 92–104.
196. Тоффлер Э. Метаморфозы власти. – М.: АСТ, 2004. – 672 с.
197. Тоффлер Э. Третья волна. – М.: АСТ, 2010. – 784 с.
198. У До. Особенности внешнеполитической стратегии Си Цзиньпина // Общество: политика, экономика, право. 2018. №12 (65). С. 31-34.
199. Фарина А.Я. Анализ современных форм, методов и приемов информационного воздействия по каналам СМИ // Вестник МГЛУ. Серия: Исторические науки. 2010. № 2 (581). С. 247–266.
200. Феофанов К. А. Цивилизационная теория модернизации. М.: Издательские решения, 2016. 248 с.
201. Франк А.Г. Азия проходит полный круг – с Китаем как «Срединным государством» // Цивилизации. Вып. 5. Проблемы глобалистики и глобальной истории / ред. А.О. Чубарьян. М.: Наука, 2002. С. 192-203.

202. Хантингтон С. Столкновение цивилизаций. М.; СПб.: АСТ, 2003. 603 с.
203. Хьелл Л., Зиглер Д. Теории личности. Основные положения, исследования и применение. 3-е изд. СПб.: Питер, 2008. 609 с.
204. Цыганков П. А. “Гибридная война”: политический дискурс и международная практика // Вестник Московского университета. Серия 18. Социология и политология. 2015. №4. С. 253–258.
205. Цыганков П.А. «Гибридные войны»: понятие, интерпретации и реальность // «Гибридные войны» в хаотизирующемся мире XXI века / Под ред. П.А. Цыганкова. М.: Издательство Московского университета, 2015. С. 32–42.
206. Цыганков П.А. Системный подход в теории международных отношений // Вестник МГУ. Сер.12: Политические науки. 2013. № 5. С. 3–25.
207. Чумаков А.Н. Актуальный инструментарий информационного противоборства в "холодной", "горячей" и "гибридной" войне// Наука. Общество. Оборона. 2023. Т. 11. № 2 (35). С. 19.
208. Шаклеина Т. А. Лидерство и современный мировой порядок // Международная жизнь. 2015. Т. 13. № 43. С. 6–19.
209. Шарп Дж. От диктатуры к демократии. Концептуальные основы освобождения; пер. Козловской Н.М.: Новое издательство, 2012.
210. Шатило Я. С., Черкасов В. Н. Информационные войны // Информационная безопасность регионов. 2009. №2 (5). С. 44–51.
211. Шевченко О. М., Штофер Л. Л. Ксенофобия как эффективная технология современных информационных войн // Гуманитарий Юга России. 2015. №1 С. 98–108.
212. Штоль В.В. Холодная война как элемент системы противостояния Запада и России // Обозреватель-Observer. 2016. №10 (321). С. 1–29.
213. Шутов А.Д. Теория и практика современной мировой политики // Вестник Дипломатической академии МИД России. Россия и мир. 2018. № 1 (15). С. 153–159.

214. Ю Хань. Развитие современной внешней политики КНР // Terra Linguistica. 2016. №1 (239). С. 84-91.
215. Ярмак О.В., Бакулин А.В., Бакулин Д.В. Феномен сетецентризма в условиях современного когнитивного противостояния: на примере анализа херсонского кейса// Вестник Института социологии. 2023. Т. 14. № 2. С. 114-135.Аватков В.А., Каширина Т.В. Тенденции развития современных международных отношений // Обозреватель-Observer. 2017. № 11 (334). С. 5-15.
216. Akaev A. A., Sadovnichiy V. A. A closed dynamic model to describe and calculate the Kondratiev long wave of economic development // Herald of the Russian Academy of Sciences. 2016. Vol. 86, No 5. P. 371–383.
217. Akaev A., Korotayev A., Issaev L., Zinkina J. Technological development and protest waves: Arab spring as a trigger of the global phase transition? // Technological Forecasting and Social Change. 2017. Vol. 116. P. 316–321.
218. Akaev A., Sadovnichy V., Korotayev A. On the dynamics of the world demographic transition and financial-economic crises forecasts // The European Physical Journal Special Topics. 2012. Vol. 205, No 1. P. 355–373.
219. Andersen M.S., Wohlforth W.C. Balance of power: a key concept in historical perspective. In: de Carvalho B., Costa Lopez J., Leira H. (eds). Routledge handbook of historical international relations. London: Routledge, 2021. P. 289-301.
220. Arrighi G. The long twentieth century: money, power, and the origins of our times. London: Verso, 1994. 400 p.
221. Arrighi G., Silver B. J. Chaos and governance in the modern world system. University of Minnesota Press, 1999.
222. Bodrožić Z., Adler P. S. The evolution of management models: A neo-Schumpeterian theory // Administrative Science Quarterly. 2018. Vol. 63. №. 1. P. 85–129.
223. Braudel F. Capitalism and material life, 1400–1800. Harper and Row, 1973.

224. Braudel F. Civilization and capitalism, 15th – 18th century. Harper and Row, 1982.
225. Chase-Dunn C., Anderson E. (Eds.). The historical evolution of world-systems. Cham: Springer, 2005. https://doi.org/10.1057/9781403980526
226. Chase-Dunn C., Hall T. D. Rise and demise: Comparing world-systems. Westview Press, 1997.
227. Chase-Dunn C., Lerro B. Social change: Globalization from the Stone Age to the present. London: Routledge, 2016.
228. Chase-Dunn C., Niemeyer R., Alvarez A., Inoue H., Love J. Cycles of rise and fall, upsweeps and collapses: Changes in the scale of settlements and polities since the Bronze Age. In L. Grinin, P. Herrmann, A. Korotayev, & A. Tausch (Eds.), History and mathematics: Processes and models of global dynamics. Volgograd: Uchitel, 2010. P. 64–91.
229. Cheng D. Cyber dragon: Inside China's information warfare and cyber operations. Bloomsbury Publishing USA, 2016.
230. Denemark R. A., Friedman J., Gills B. K., Modelski G. World system history: The social science of long-term change. London: Routledge, 2000.
231. Diakonoff I. The paths of history. Cambridge: Cambridge University Press, 1999.
232. Dossi S. On the asymmetric advantages of cyberwarfare. Western literature and the Chinese journal Guofang Keji // Journal of Strategic Studies. 2020. Vol.43, No 2. P. 281–308.
233. Frank A. G. 1998. ReOrient: Global economy in the Asian age. Berkeley: University of California Press, 1998.
234. Frank A. G., Gills B. K. (Eds.). The world system: Five hundred years, or five thousand. London: Routledge, 1993.
235. Fredericks Brian E. Information Warfare at the Crossroads. Joint Force Quarterly. 1997. Vol. 17. Pp. 97–103.
236. Gellner E. Plough, sword and book. The structure of human history. Chicago: University of Chicago Press, 1988.

237. Gills B. K., Thompson W. (Eds.). Globalization and global history. London: Routledge, 2012.
238. Glenn J.C., Florescu E., The Millennium Project Team. State of the Future 19.1. Washington, DC: The Millennium Project, 2018.
239. Grinin L. E., Grinin A. L., Korotayev A. Forthcoming Kondratieff wave, Cybernetic Revolution, and global ageing // Technological Forecasting & Social Change. 2017. Vol. 115. P. 52–68.
240. Grinin L. E., Korotayev A. V. Global Population Ageing, The Sixth Kondratieff Wave, And The Global Financial System // Journal of Globalization Studies. 2016. T.7, №2. C. 11-31.
241. Grinin L. Macrohistory and globalization. Volgograd: Uchitel, 2012.
242. Grinin L. On revolutionary waves since the 16th century. In J. A. Goldstone, L. Grinin, & A. Korotayev (Eds.), Handbook of revolutions in the 21st century: The new waves of revolutions, and the causes and effects of disruptive political change. Cham: Springer, 2022. P. 389–411. https://doi.org/10.1007/978-3-030-86468-2_13
243. Grinin L., Grinin A. Historical materialism: Does the concept have a future? // Social Evolution & History. 2023. Vol. 22. No 1. P. 143–178.
244. Grinin L., Grinin A. The cybernetic revolution and the forthcoming epoch of selfregulating systems. Volgograd: Uchitel, 2016.
245. Grinin L., Korotayev A. Great divergence and great convergence. A global perspective. Cham: Springer, 2015.
246. Grinin L., Korotayev A. Great divergence and great convergence. A Global Perspective. Cham: Springer International Publishing, 2015.
247. Grinin L., Korotayev A. Origins of globalization in the framework of the Afroeurasian world-system history. In T. D. Hall (Ed.) Comparing globalizations. Historical and worldsystems approaches. Cham: Springer, 2018. P. 37–70.
248. Grinin L., Korotayev A. Social macroevolution. Genesis and transformations of the world system. Moscow: Librocom/URSS, 2009.

249. Hampson F. O., Jardine E. Look Who's Watching: Surveillance, Treachery and Trust Online. Waterloo, ON, Canada: Centre for International Governance Innovation, 2016. 364 p.
250. Hjelle L., Ziegler D. Personality Theories: Basic Assumptions, Research, and Applications. McGraw-Hill Book Company, 1992.
251. Ilyin I., Ursul A. Globalistics: New investigative trends in science // Globalistics and Globalization Studies. 2012. Vol. 1. P. 107–118.
252. Joint Vision 2020. America's Military – Preparing for Tomorrow / National Defense University, Institute for National Strategic Studies. Washington, D.C., 2000.
253. Kennedy P. The rise and fall of great powers: economic change and military conflict from 1500 to 2000. New York, NY: Random House, 1987. 677 p.
254. Korotayev A. Compact mathematical models of world system development, and how they can help us to clarify our understanding of globalization processes. In G. Modelski, T. Devezas, & W. R. Thompson (Eds.) Globalization as evolutionary process: Modeling global change. London: Routledge, 2008. P. 133–160.
255. Korotayev A. The 21st century singularity in the big history perspective. A re-analysis. In A. Korotayev & D. LePoire (Eds.) The 21st century singularity and global futures. A big history perspective (pp.). Cham: Springer, 2020. P. 19–75.
256. Korotayev A. World religions and social evolution of the old world Oikumene civilizations: A cross-cultural perspective. Edwin Mellen Press, 2004.
257. Korotayev A., Goldstone J. A., Zinkina J. Phases of global demographic transition correlate with phases of the Great Divergence and Great Convergence // Technological Forecasting and Social Change. 2015. Vol. 95. P. 163-169.
258. Korotayev A., Malkov A., Khaltourina D. Introduction to social macrodynamics: Compact macromodels of the World System growth. Moscow: KomKniga/URSS, 2006.

259. Korotayev A., Malkov S. Mathematical models of the world-system development. In S. Babones & C. Chase-Dunn (Eds.) Routledge handbook of world-systems analysis. Routledge, 2012. P. 158–161.
260. Korotayev A., Zinkina J. On the structure of the present-day convergence // Campus-Wide Information Systems. 2014. Vol. 31, No 2/3. P. 139-152.
261. Libicki M. What is information warfare? Washington: GPG, 1995. 280 p.
262. Little R. The balance of power in international relations: metaphors, myths and models. Cambridge: Cambridge university press, 2007. 317 p.
263. Malkov S., Davydova O. Modernization as a global process: The experience of mathematical modeling // Computer Research and Modeling. 2021. Vol. 13, No 4. P. 859–873.
264. Maslow A. H. Motivation and Personality. New York: Harper & Row, 1954.
265. McNeill W. H. The pursuit of power: Technology, armed force, and society since AD 1000. Chicago: University of Chicago Press, 2013.
266. Mearsheimer J.J. The tragedy of great power politics. New York: W.W. Norton, 2001. 555 p.
267. Modelski G., Devezas T., Thompson W. R. (Eds.). Globalization as evolutionary process: Modeling global change. London: Routledge, 2007.
268. Modelski G., Thompson W. R. Leading sectors and world powers: The coevolution of global politics and economics. University of South Carolina Press, 1996.
269. Modelski G., Thompson W.R. Leading sectors and world powers: the coevolution of global politics and economics. Columbia, SC: University of South Carolina press, 1996. 263 p.
270. Molander R.C., Riddile A., Wilson P.A. Strategic Information Warfare: A new face of war. RAND Corporation, 1996.
271. Müller T., Albert M. Whose balance? A constructivist approach to balance of power politics // European journal of international security. 2021. Vol. 6, No 1. P. 109-128. DOI: https://doi.org/10.1017/eis.2020.19

272. Murray D., Brown D. (eds). Multipolarity in the 21st century: a new world order. New York: Routledge, 2012. 224 p.
273. Nexon D.H. The balance of power in the balance // World Politics. 2009. Vol. 61, No 2. P. 330-359. DOI: https://doi.org/10.1017/s0043887109000124
274. Nichiporuk B. US Military opportunities: Information-warfare concepts of operation. In: Z. Khalilzad & J. Shapiro (eds). Strategic appraisal: United States air and space power in the 21st century. Rand Corporation, 2002. Pp. 187-219.
275. Paul T.V., Wirtz J.J., Fortmann M. Balance of power: theory and practice in the 21st century. Stanford, CA: Stanford University Press, 2004. 384 p.
276. Rodrigue B. H. Disaster's offspring: Catastrophe, narrative, and survival in global history // Journal of Globalization Studies. 2021. Vol. 12, No 1. P. 159–171.
277. Schmitt M. (ed.), Tallinn Manual on the International Law Applicable to Cyber Warfare. Cambridge: Cambridge University Press, 2013. 300 p.
278. Schwab K. The Fourth Industrial Revolution. Crown Currency, 2017. 192 p.
279. Spykman N.J. America's strategy in world politics: the United States and the balance of power. London: Routledge, 2017. 525 p.
280. Sunstein C. R. The Law of Group Polarization // Journal of Political Philosophy. 2002. Vol. 10. № 2. Pp. 175–195.
281. Turchin P. Historical dynamics: Why states rise and fall (2nd ed.). Princeton, NJ: Princeton University Press, 2018.
282. Vuletić, D. V., & Stanojević, P. Concepts of information warfare (operations) of the United States of America, China and Russia // Review of International Affairs. 2022. Vol. 73, No 1185. P. 51–70.
283. Wallerstein I. 1979. The Capitalist World-Economy. Cambridge: Cambridge University Press. 305 p.
284. Wallerstein I. 1980. The Modern World-System II. Mercantilism and the Consolidation of the European World Economy, 1600-1750. NY: Academic. 370 p.

285. Wallerstein I. The modern world-system I: Capitalist agriculture and the origins of the European world-economy in the sixteenth century. Vol. 1. University of California Press, 2011.
286. Wallerstein I. World-systems analysis: An introduction. Duke University Press, 2020.
287. Wallerstein, I. 1974. The Modern World-System: Capitalist Agriculture and the Origins of the European World-Economy in the Sixteenth Century. NY: Academic. 410 p.
288. Wendt A. Social Theory of International Politics. Cambridge: Cambridge University Press. 1999.
289. Zhang F. Reconceiving the balance of power: a review essay //Review of international studies. 2011. Vol. 37, No 2. P. 641-651.
290. Zinkina J., Christian D., Grinin L., Ilyin I., Andreev A., Aleshkovski I., Shulgin S., Korotayev A. A big history of globalization: The emergence of a global world system. Cham: Springer, 2019.

Интернет источники

291. Встреча с Президентом США Джозефом Байденом// Официальный Интернет-сайт Президента России. 7.12.2021. URL: http://www.kremlin.ru/events/president/news/67315 (дата обращения: 1.09.2022).
292. Встреча с Президентом США Джозефом Байденом// Официальный Интернет-сайт Президента России. 7.12.2021. URL: http://www.kremlin.ru/events/president/news/67315 (дата обращения: 1.09.2022).
293. Герейханова А., Гончарук Д. Путин назвал БРИКС одним из ключевых элементов формирующегося многополярного миропорядка / Российская газета. 11.07.2024. URL: https://rg.ru/2024/07/11/vazhno-byt-vmeste.html (дата обращения 16.11.2024).

294. Институты Конфуция. Уральский федеральный университет. URL:https://ci.urfu.ru/ru/about/ (дата обращения:1.04.2025).

295. Интервью директора Департамента международной информационной безопасности МИД России А.В.Крутских «Глобальная киберповестка: дипломатическая победа» журналу «Международная жизнь», 7 июня 2021 года / Сайт Министерства иностранных дел Российской Федерации. 08.06.2022. URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1752094/ (дата обращения: 1.08.2025).

296. Исследователи установили, какой контент чаще всего блокируется в Китае / SecurityLab.ru. 12.07.2021. URL: https://www.securitylab.ru/news/522101.php (дата обращения 16.10.2024)

297. Китай вводит обязательную идентификацию интернет-пользователей / Digital.Report. 29.08.2017. URL: https://digital.report/kitay-vvodit-obyazatelnuyu-identifikatsiyu-internet-polzovateley/ (дата обращения 16.10.2024).

298. Китай готовится к усилению кибервойн. Создана особая армейская структура для ИТ-поддержки войск// СиНьюс, 22 Апреля 2024 года. URL: https://gov.cnews.ru/news/top/2024-04-22_kitaj_sozdal_novuyu_voennuyu (дата обращения: 1.04.2025)

299. Китайцы создали высокоэффективного ИИ-цензора / SecurityLab.ru. 15.04.2021. URL: https://www.securitylab.ru/news/518922.php (дата обращения 16.10.2024)

300. Количество кибератак на сервисы и структуры России в 2022 году выросло в семь раз// ТАСС. 21 марта 2023 года. URL: https://tass.ru/ekonomika/17327093 (дата обращения: 1.09.2025).

301. Лукин Е.В. Психологические основы информационной войны// Центр стратегических оценок и прогнозов. URL:https://csef.ru/ru/oborona-i-

bezopasnost/265/psihologicheskie-osnovy-informaczionnoj-vojny-3725 (дата обращения: 1.09.2025).

302. Мельникова О. Опыт Китая в защите национального киберсуверенитета / Международная жизнь. 13.12.2022. URL: https://interaffairs.ru/news/show/38218 (дата обращения 16.10.2024)
303. Мушта А., Баранов А. Информационная война / Большая российская энциклопедия / [Электронный ресурс] – URL: https://bigenc.ru/c/informatsionnaia-voina-2b7815 (дата обращения: 1.09.2025).
304. О первой сессии Спецкомитета ООН по разработке всеобъемлющей конвенции по противодействию информационной преступности / Сайт Министерства иностранных дел Российской Федерации. 12.03.2022 URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1803908/ (дата обращения: 1.09.2025).
305. Об инициативе стран-членов ШОС «Правила поведения в области обеспечения международной информационной безопасности» / МИД РФ. 29.01.2015. URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1582268/ (дата обращения 06.11.2024).
306. Об итогах деятельности Группы правительственных экспертов ООН по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности / Сайт Министерства иностранных дел Российской Федерации 02.06.2021 URL: https://www.mid.ru/ru/foreign_policy/international_safety/mezdunarodnaa-informacionnaa-bezopasnost/1423809/ (дата обращения: 1.09.2025).
307. ООН пересматривает принципы интернет-управления через 20 лет// DIGITAL-REPORT, 26.05.2025. URL:https://digital-report.ru/oon-peresmotrit-printsipy-internet-upravleniya/ (дата обращения: 1.10.2025).

308. Песков: РФ находится в состоянии информационной войны с англосаксами [Электронный ресурс]. URL: http://rg.ru/ 2016/03/26/peskov-rf-nahoditsia-v-sostoianii-informacionnoj-vojny-s-anglosaksami.html
309. Тренин Д. Конфликт уникальностей. Как будут складываться отношения России и США после послания Путина / Российский совет по международным делам. 05.03.2018. URL: http://russiancouncil.ru/analytics-and-comments/comments/konfl ikt-unikalnostey-kak-budut-skladyvatsya-otnosheniya-rossii-i-ssha-posleposlaniya-putina/#detail
310. Тренин Д. Смягчение конфликта в условиях гибридной войны / Московский центр Карнеги. 25.01.2018. URL: http://carnegie.ru/2018/01/25/ru-pub-75296
311. Щекоян И. Поднебесная правда: кто и зачем ведет информационную войну с КНР// Известия. 28 ноября 2019 года. URL: https://iz.ru/947921/irena-shekoian/podnebesnaia-pravda-kto-i-zachem-vedet-informatcionnuiu-voinu-s-knr (дата обращения: 1.09.2025).
312. Betting big on quantum / McKinsey. 13.09.2022. URL: https://www.mckinsey.com/featured-insights/sustainable-inclusive-growth/charts/betting-big-on-quantum (дата обращения 16.10.2024).
313. China calls for joint efforts to advance global governance / Xinhua 25.09.2024. URL: https://english.news.cn/20240925/f09057004024433999dddcb92aaa6beb/c.html (дата обращения 15.11.2024).
314. China closes more than 13,000 websites in past three years / Reuters. 24.12.2017. URL: https://www.reuters.com/article/us-china-internet/china-closes-more-than-13000-websites-in-past-three-years-idUSKBN1EI05M/?feedType=RSS&feedName=technologyNews (дата обращения 16.10.2024).
315. China invests $47 billion in largest ever chip fund / Techxplore. 27.05.2024. URL: https://techxplore.com/news/2024-05-china-invests-billion-largest-chip.html (дата обращения 16.10.2024).

316. China invests US$6.1 billion in data centre infrastructure amid surge in demand for AI chips / South China Morning Post. 29.08.2024. URL: https://www.scmp.com/tech/tech-trends/article/3276455/china-invests-us61-billion-data-centre-infrastructure-amid-surge-demand-ai-chips (дата обращения 18.10.2024).
317. Chinese Quantum Companies and National Strategy 2023 / The Quantum Insider. 13.04.2023. URL: https://thequantuminsider.com/2023/04/13/chinese-quantum-companies-and-national-strategy-2023/ (дата обращения 16.10.2024).
318. Cimpanu C. Oracle: China's internet is designed more like an intranet / ZDNet. 23.07.2019. URL: https://www.zdnet.com/article/oracle-chinas-internet-is-designed-more-like-an-intranet/ (дата обращения 16.10.2024).
319. Closing Digital Divide Critical to Social, Economic Development, Delegates Say at Second Committee Debate on Information and Communications Technologies: Meetings Coverage / UN. 2015. URL: https://www.un.org/press/en/2015/gaef3432.doc.htm (дата обращения 1.10.2025).
320. Digital Divide / Stanford University. URL: https://cs.stanford.edu/people/eroberts/cs201/projects/digital-divide/start.html (дата обращения 1.10.2025).
321. Dotterer G., Hedges A. Parker H. The Digital Divide in the Age of the Connected Classroom / NetRef. 14.01.2016. URL: https://net-ref.com/wp-content/uploads/2016/01/Bridging-the-Digital-Divide-NetRef-White-Paper-FINAL.pdf (дата обращения 1.10.2025).
322. Elliott L. Spread of internet has not conquered 'digital divide' between rich and poor: report / The Guardian. 13.01.2016. URL: https://www.theguardian.com/technology/2016/jan/13/internet-not-conquered-digital-divide-rich-poor-world-bank-report#:~:text=6%20years%20old-,Spread%20of%20internet%20has%20not%20conquered%20'digital%20divide,between%20rich%20and%20poor%20%E2%80%93%20report&text=The%20

rapid%20spread%20of%20the,divide%20between%20rich%20and%20poor (дата обращения 1.10.2025)

323. Green S. Cognitive Warfare. The Augean Stables. Joint Military Intelligence College. July 2008 [Электронный ресурс]. URL: www.theaugeanstables.com/wp-content/uploads/2014/04/Green-Cognitive-Warfare. pdf (дата обращения: 29.10.2022).
324. Information warfare / NATO. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf (дата обращения 15.10.2024).
325. John Hopkins University & Imperial College London. Countering Cognitive Warfare: Awareness and Resilience [Электронный ресурс] : NATO Review. 2021. May 20. URL: https://www.nato.int/docu/review/articles/2021/05/20/ countering-cognitive-warfare-awareness-and-resilience/index.html (дата обращения: 19.10.2024).
326. Lewis B.C. Information Warfare / Federation of American Scientists. Intelligence Resource Program. URL https://irp.fas.org/eprint/snyder/infowarfare.htm (дата обращения 15.10.2024).
327. McKendrick J. Lack Of Digital, Cloud Opportunities Is Actually Embarrassing For Employees, Survey Suggests / Forbes. 16.07.2016. URL: https://www.forbes.com/sites/joemckendrick/2016/07/16/lack-of-digital-cloud-opportunities-is-actually-embarrassing-for-employees-survey-suggests/?sh=6e2394ab6aab (дата обращения 1.10.2025).
328. McLaughlin C. The Homework Gap: The 'Cruelest Part of the Digital Divide' / NEA Today. 20.04.2016. URL: https://www.nea.org/advocating-for-change/new-from-nea/homework-gap-cruelest-part-digital-divide (дата обращения 1.10.2025).
329. Peterson, R., Oxnevad I., Yan F. After Confucius Institutes// National Association of Scholars, 15 June 2022 URL: https://www.nas.org/reports/after-confucius-institutes/full-report (дата обращения: 1.04.2025).

330. Spafford, Eugene H., "The Internet Worm Incident" (1989). Department of Computer Science Technical Reports. Paper 793. https://docs.lib.purdue.edu/cstech/793.

331. U.S. Cyber Command. Our History / U.S. Cyber Command. URL: https://www.cybercom.mil/About/History/ (дата обращения 10/10/2024).

332. Xinhua Headlines: "Greater BRICS cooperation" contributes vitality, wisdom to global governance / Xinhua. 22.10.2024. URL: https://english.news.cn/20241022/bedf79fd9f354a72831c0bcbfc6e8fe2/c.html (дата обращения 15.11.2024).

333. 聚焦十九大 专家解读：中国的大国外交彰显哪些理念？/ CCTV.com. [Экспертная интерпретация: каковы концепции великой дипломатии Китая?] [Электронный ресурс] / CCTV.com. URL: http://news.cctv.com/2017/10/22/ARTIyWPLzxmXX971DmC7wpyc171022.shtml (дата обращения 15.11.2024).