

Научная статья

УДК 323.21

doi: 10.47598/2078-9025-2024-3-64-17-23

АКТУАЛЬНЫЕ ТЕХНОЛОГИИ ИНФОРМАЦИОННОЙ ВОЙНЫ И СТРАТЕГИЧЕСКИХ КОММУНИКАЦИЙ

Данил Андреевич Блишун¹, Сергей Николаевич Чирун²✉

^{1,2}Кемеровский государственный университет, Кемерово, Россия

¹blishunov19@mail.ru

²Sergii-Tsch@mail.ru✉, <https://orcid.org/0000-0001-7422-8030>

Аннотация. Актуальность представленной статьи объясняется тем, что в условиях обострения отношений России со странами коллективного Запада эффективная защита стратегических интересов страны является приоритетной функцией государства. Целью исследовательской работы является анализ основных технологий информационной войны, а также анализ близкого информационной войне феномена стратегических коммуникаций. Сегодня термины «информационная война» и «стратегические коммуникации» прочно вошли в научный и деловой оборот, а сам XXI век ознаменовался активацией применения инновационных технологий информационного противоборства.

Авторы рассматривают известные подходы к пониманию феномена информационной войны, рассматривают особенности применения, преимущества и ограничения, технологий информационной войны. Приходят к заключению о том, что информационная война является неотъемлемым элементом динамики современного международного конфликта, ввиду этого умение ориентироваться в особенностях современного кризисного информационно-коммуникационного взаимодействия, знание технологии ведения информационных войн помогут осуществить контроль над собственным информационным полем и информационными ресурсами противника.

Ключевые слова: информационная война, стратегические коммуникации, сеть «Интернет», противоборство, преступления в сети «Интернет», фейки

Для цитирования: Блишун Д. А., Чирун С. Н. Актуальные технологии информационной войны и стратегических коммуникаций // Вестник БИСТ (Башкирского института социальных технологий). 2024. № 3(64). С. 17–23. <https://doi.org/10.47598/2078-9025-2024-3-64-17-23>.

Research article

CURRENT TECHNOLOGIES OF INFORMATION WARFARE AND STRATEGIC COMMUNICATIONS

Danil A. Blishunov¹, Sergey N. Chirun²✉

^{1,2}Kemerovo State University, Kemerovo, Russia

¹blishunov19@mail.ru

²Sergii-Tsch@mail.ru✉, <https://orcid.org/0000-0001-7422-8030>

Abstract. The relevance of the presented article is explained by the fact that in the conditions of aggravation of relations between Russia and the countries of the collective West, effective protection of the country's strategic interests is a priority function of the state. The purpose of the research work is to analyze the main technologies of information warfare, as well as the analysis of the phenomenon of strategic communications close to information warfare. Today, the terms "information warfare" and "strategic communications" have firmly entered into scientific and business circulation, and the 21st century itself has been marked by the activation of the use of innovative technologies of information confrontation. The authors consider

known approaches to understanding the phenomenon of information warfare, consider the features of application, advantages and limitations of information warfare technologies. They come to the conclusion that information warfare is an integral element of the dynamics of a modern international conflict, in view of this, the ability to navigate the features of modern crisis information and communication interaction, knowledge of the technology of conducting information wars will help to exercise control over its own information field and the enemy's information resources.

Keywords: information warfare, strategic communications, Internet, confrontation, crimes on the Internet, fakes

For citation: Blishunov D. A., Chirun S. N. Current technologies of information warfare and strategic communications. *Vestnik BIST (Bashkirskogo instituta social'nykh tekhnologij) = Vestnik BIST (Bashkir Institute of Social Technologies)*. 2024;(3(64)):17–23. (In Russ.). <https://doi.org/10.47598/2078-9025-2024-3-64-17-23>.

В современных условиях, характеризующихся ситуацией перманентного обострения международных отношений, особую актуальность в изучении информационных войн представляет геополитический подход, ярким представителем которого является И. Н. Панарин. По мнению доктора политических наук, профессора И. Н. Панарина творцами первой мировой информационной войны (между Востоком и Западом) являются У. Черчилль, Дж. Кеннан и А. Далес, деструктивным усилиям которых на информационном фронте успешно противостоял И. В. Сталин, после ухода из жизни которого поражение СССР в информационной войне, по мнению И. Н. Панарина, стало практически неизбежно [1, с. 13–122].

Отметим, что не все политологи (как российские, так и зарубежные) считают уместным использование термина «информационная война». Многие пытаются искать и находить ему альтернативу в иной близкой по значению терминологии [2].

В конце XX в. в США оформились ряд научных школ, исследующих феномен информационной войны. Среди них нужно отметить структуры Национального оборонного университета США, лаборатории корпорации РЭНД, а также исследования специалистов университета ВВС США. Именно идеи этих структур оказали влияние на высшее военно-политическое руководство США.

Сотрудниками РЭНД Дж. Арквиллой и Д. Ронфельдтом была выдвинута футурологическая концепция, прогнозирующая достижение успеха в будущих войнах на основе информационного превосходства [3, с. 88–89].

По мнению ученых университета ВВС США Дж. Стейна и Р. Шафрански война будет вестись на уровне сознания, а любые действия

противника будут работать на пользу США [4–5].

Концепция «стратегического паралича», была сформулирована О. Йенсенем. Суть ее в том, чтобы сделать невозможным эффективное сопротивление противника [6].

В рамках анализа военной стратегии рассматривает информационную войну Дж. Дерриан. Победа обеспечивается за счет технологизации вооруженных сил государства. Кроме того, им утверждается необходимость разрушения информационных систем противника [7, с. 771–788].

Исследователь М. Либики связывал успех информационной войны с развитием системы глобального слежения, что даст возможность заблаговременно предупредить любые деструктивные намерения противника и одержать победу даже без начала военных действий [8].

Концепция сетевой войны является одним из направлений теории информационной войны. Автором этой концепции является А. Цебровски. Концепция базируется на использовании информационных технологий и в первую очередь означает тотальную интеграцию компьютерных и коммуникационных систем [9].

В современной науке известно большое количество подходов к интерпретации феномена информационной войны. Например, что «информационная война — противоборство сторон, возникающее из-за конфликта интересов и/или идеологий и осуществляемое путем целенаправленного информационного воздействия друг на друга с использованием специальных технологий для получения определенного преимущества в материальной или идеологической сфере и защиты собственной

безопасности» [10, с. 11]. В исследованиях Г. Г. Почепцова понятие информационной войны определяется как «коммуникативная технология по воздействию на массовое сознание с кратковременными и долговременными целями» [11, с. 121].

Е. В. Каблуков, придерживаясь конструктивистского подхода, отмечает, что информационная война «представляет собой последовательное и систематическое конструирование реальности, причиняющей вред какому-либо объекту и/или его образу в медиадискурсе» [12, с. 235–238].

Согласно Л. В. Коцюбинской, информационная война представляет собой «информационное воздействие на общественное (массовое) сознание с целью внесения изменений в когнитивную структуру, с тем чтобы в дальнейшем получить изменения в поведенческой структуре» [13, с. 93–96].

Однако отметим, что, по нашему мнению, в указанном определении понятие «информационная война» пересекается с категорией стратегической коммуникации [14, с. 229–233]. Поскольку стратегические коммуникации представляет собой «скоординированные действия, сообщения, образы и другие виды оповещения и вовлеченности, направленные на информирование, влияние и убеждение определенных целевых аудиторий в поддержку целей государства» [15, с. 52–76].

На наш взгляд, основное отличие информационной войны от стратегических коммуникаций заключается в методах и отчасти технологиях реализации.

Информационная война — это, прежде всего, дестабилизация и разрушение стратегических структур оппонента, что нередко сопровождается большими рисками перехода войны в горячую стадию. Тогда как стратегические коммуникации направлены в первую очередь на формирование, поддержание и оптимизацию собственных управленческих структур и интересов, укрепление имиджа и поддержание долгосрочных позитивных отношений с партнерами. В следствие чего в случае стратегических коммуникаций речь идет об использовании более прозрачных и этичных методов, чем в классической ситуации информационной войны.

Стратегическая коммуникация — ровесница человеческой цивилизации. Социолог и специалист по массовым коммуникациям Г. Иннис утверждал, что любая работа с информацией преследует цель контроля пространства и времени, так в средневековых монастырях тексты переписывались с папируса на пергамент. При этом тексты корректировались в соответствии с актуальной на тот момент научной парадигмой, а первоисточники уничтожались [16].

Ведение информационной войны предполагает распространение ложной или вводящей в заблуждение информации для дестабилизации общества, подрыва доверия к власти и политическим институтам. Информационная война носит агрессивный, наступательный характер и часто направлена на создание конфликта или разрушение институтов и социальной стабильности. С этим связаны ее специфические методы и технологии: пропаганда, кибератаки, распространение фейковых сообщений, манипуляции, а также использование психологических операций для деморализации противника. Все это может предшествовать реализации традиционных военных операций или же быть частью гибридной войны. При этом технологии и методы информационной войны могут иметь как прикладную, так и стратегическую направленность.

Перефразируя идеи М. Фуко, можно сказать, что политика — это информационная война, продолженная иными средствами [17, с. 148–151].

Стратегические коммуникации носят более созидательный и конвенциональный характер, направлены на построение позитивного имиджа политического актора, формирование общественного мнения, поддержание долгосрочных устойчивых отношений и продвижение стратегических интересов. Поэтому методы стратегических коммуникаций включают публичную дипломатию, общественные связи (PR), маркетинговые кампании, официальные заявления и речевые мероприятия, а также использование медиаплатформ для донесения месседжа.

Назовем некоторые, на наш взгляд наиболее актуальные в современных условиях технологии информационной войны и стратегических коммуникаций.

1) Стратегическое управление фобиями. Технология заключается в управляемом переносе восприятия информации из рациональной в эмоциональную сферу. В результате использования данной технологии реципиенты становятся менее критичными в восприятии поступающей информации и более удобными для манипулирования.

2) Технология нормализации. Призвана обеспечить принятие того, что в обыденном сознании нормальным человеком воспринимается как совершенно недопустимое (убийство, насилие, предательство и т. п.). Разновидностью этой технологии является «Окно Овертона».

3) Операции влияния. Целевые рекламные кампании, предполагающие создание вирусного контента, который быстро распространяется и влияет на массовое сознание. Использование данных о пользователях для осуществления таргетированной рекламы, направленной на изменение их политических взглядов и поведения.

4) Создание образа тотального (сакрального) врага. Эта технология предполагает эффективное противопоставление нежелательным социальным группам и меньшинствам, а также государствам-изгоям. В реализации этой технологии используются различные приемы, обычно связанные с управлением интерпретациями религиозно-сакральных, культурных, идеологических или геополитических смыслов.

5) Дезинформация. Создание и распространение фейковых или искаженных новостей. Сюда же относится введение в заблуждение путем частичной или полной замены истинной информации ложной. Здесь возможны определенные варианты. Например, это может быть фабрикация фактов, что может использоваться для обвинения противника в каких-либо действиях, которые в действительности им не совершались. Или это может быть «ложное объяснение», когда фабрикуются не сами факты, а элементы их интерпретации.

6) Технология фреймов. Речь идет о конструировании рамочного восприятия. Например, мы видим, что в контексте арабо-израильского конфликта на Ближнем Востоке, одной из сторон конфликта постоянно и совершенно

некорректно применяется термин «антисемитизм». Этот термин часто используется одной группой семитов в качестве инструмента стигматизации своих политических и идеологических противников, представленных другой группой семитов. Причем большинство реципиентов — потребителей политической информации, к сожалению, демонстрируют высокую толерантность к восприятию некорректности указанного фрейма.

7) Историческое ре-конструирование. Существует мнение, согласно которому человеческой истории как объективной реальности вовсе не существует, поскольку история всегда является продуктом перманентного политического конструирования, осуществляемого в интересах элит и выражающих их интересы политических акторов, что имеет место как на национальном, так и на глобальном уровнях стратегического управления. Поэтому переписывание или ре-конструирование истории — это перманентный процесс, мало зависящий от научной составляющей, но всегда синхронизированный с процессами динамики правящих элит. Соответственно, эффективное управление указанным процессом повышает надежность и управляемость долгосрочных стратегических коммуникаций.

8) Возвеличивание своего народа и формирование шаблона национально-культурного превосходства. Такая технология основана на постулировании цивилизационного превосходства над государством (народом, нацией) противника. Эта технология формирования особой гордости по факту принадлежности к определенной, якобы исключительной общности. Она позволяет создавать образ мнимой непобедимости и превосходства, условной «богоизбранности», духовной, интеллектуальной, волевой или физической мощи определенного народа или нации. В реализации указанной технологии властью активно привлекаются представители национальной культуры и кинематографа.

9) Перераспределение информационного веса. Эту технологию нередко применяют историки, «вспоминая», вводя в научный оборот имена тех или иных «незаслуженно» забытых политических либо общественных деятелей. Указанная технология может быть реализована

на через присуждение политическому диссиденту, реформатору, или просто непопулярному в своей стране политику высокой зарубежной (международной) награды. Так, например, президент М. С. Горбачев получил Нобелевскую премию мира за год до распада СССР.

10) Формирование негативного образа. Технология связана с созданием долговременного негативного образа определенного народа или общности, что может быть связано с утверждением представлений о его, якобы «нецивилизованности», «негуманности», нечистоплотности, неадекватности.

11) Технологии медиа-манипуляции. Эта группа технологий информационной войны предполагает как работу с контекстом (изменение контекста реальных событий, включая манипуляцию статистикой) для создания ложного впечатления), так и прямую фальсификацию данных. Это может касаться как подделки документов, в том числе исторического содержания, так и монтаж изображений и видео с целью коррекции визуального контента для сознательного искажения реальности.

Современная информационная война основывается на стратегическом подходе, гибко сочетающем применение комплекса традиционных методов с инновационными технологиями и платформами. Это предполагает опору на комплексную модель стратегических

коммуникаций, включающую в себя четкое определение целей, задач и ключевых месседжей, позволяющую эффективно воздействовать как на внутренние, так и на внешние аудитории.

Такая модель предполагает формирование и продвижение единого стратегического нарратива, адаптированного к различным аудиториям и учитывающего их социо-культурные особенности, способного укреплять идентичность и продвигать национальные интересы.

Государство в ситуации угрозы информационной войны должно обеспечить эффективный мониторинг медийного и интернет-пространства для выявления угроз и попыток информационного вмешательства со стороны враждебных международных акторов, используя эффективные аналитические инструменты, такие как Big Data и искусственный интеллект, для прогнозирования и превенции информационных угроз, защиты информационных систем от кибератак, а также поддержания готовности к проведению собственных наступательных операций в информационном пространстве противника. При этом стратегия должна быть адаптивной, способной оперативно реагировать на высоко динамичную ситуацию современного информационного противоборства.

Список источников

1. Панарин И. Н. Первая мировая информационная война. Развал СССР. Санкт-Петербург : Питер, 2010. 256 с.
2. Гриняев С. Н. Взгляды военных экспертов США на ведение информационного противоборства // Зарубежное военное обозрение. 2001. № 8. С. 19–27.
3. Arquilla J., Ronfeldt D., Zanini M. Networks, Netwar, and Information — Age Terrorism // The Changing Role of Information in Warfare. Rand Corporation, 1999. P. 78–89.
4. Stein G. J. Information Attack: Information Warfare In 2025 // Research paper presented to Air Force 2025. 1996. August. 37 p.
5. Szafranski R. Harnessing Battlefield Technology: Neocortical Warfare // The Acme of Skill, Military Review. 1994. November. P. 48–53.
6. Colonel Owen E. Jensen. Information Warfare: Principles of Third-Wave War // Airpower Journal. 1994. Vol. VIII, No. 4. P. 35–43.
7. Der Derian J. Virtuous War / Virtual Theory // Royal Institute of International Affairs. 2000. Vol. 76, No. 4. P. 771–788.
8. Libicki M. C. What is Information Warfare. Washington, D. C. : Center for Advanced Concepts and Technology, Institute for National Strategic Studies, 1995. 4 p.; Ill. (Series «Strategic forum» ; No. 28).
9. Cebrowski A. K., Navy U.S., Garstka J. J. Network — Centric Warfare: Its Origin and Future // Proceedings. 1998. January. P. 76–84.
10. Колмогорова А. В., Сквородников А. П., Копнина Г. А. Лингвистика информационно-психологической войны : В 2 кн. Кн. 1. Красноярск : Сибирский федеральный университет, 2017. 212 с.

11. Почепцов Г. Г. Информационные войны. Новый инструмент политики. Москва : Алгоритм, 2015. 256 с.
12. Каблуков Е. В. К вопросу об актуализации дискурсивных практик идентификации в условиях информационной войны // Профессиональная культура журналиста цифровой эпохи : материалы Всероссийской научно-практической конференции с международным участием (Екатеринбург, 19 мая 2017 г.). Екатеринбург : Уральский ун-т, 2017. С. 235–238.
13. Коцюбинская Л. В. Понятие «информационная война» в современной лингвистике: новые подходы // Политическая лингвистика. 2015. № 4 (54). С. 93–96.
14. Гавра Д. П. Категория стратегической коммуникации: современное состояние и базовые характеристики // Век информации. 2015. № 3 (4). С. 229–233.
15. Минаева Л. В. Стратегическая коммуникация как инструмент продвижения национальных интересов страны // Российская школа связей с общественностью. 2021. № 20. С. 52–76.
16. Tremblay G. From Marshall McLuhan to Harold Innis, or From the global village to the world empire // Canadian Journal of Communication. 2014. Vol. 37, No 4. P. 561–575.
17. Фуко М. Политика — это продолжение войны другими средствами // Интеллектуалы и власть: избранные политические статьи, выступления и интервью. Москва : Праксис, 2002. С. 148–151.

References

1. Panarin I. N. The First World Information War. The Collapse of the USSR. Saint Petersburg: Piter; 2010. 256 p. (In Russ.).
2. Grinyaev S. N. The Views of US Military Experts on Conducting Information Warfare. *Zarubezhnoe voennoe obozrenie = Foreign Military Review*. 2001;(8):19–27. (In Russ.).
3. Arquilla J., Ronfeldt D., Zanini M. Networks, Netwar, and Infonnation — Age Terrorism. The Changing Role of Information in Warfare. Rand Corporation; 1999. P. 78–89.
4. Stein G. J. Information Attack: Information Warfare In 2025. Research paper presented to Air Force 2025. 1996;(August);37.
5. Szafranski R. Harnessing Battlefield Technology: Neocortical Warfare. The Acme of Skill, *Military Review*. 1994;(November);48–53.
6. Colonel Owen E. Jensen. Information Warfare: Principles of Third-Wave War. *Airpower Journal*. 1994;VIII(4):35–43.
7. Der Derian J. Virtuous War / Virtual Theory. *Royal Institute of International Affairs*. 2000;76(4):771–788.
8. Libicki M. C. What is Information Warfare. Washington, D. C.: Center for Advanced Concepts and Technology, Institute for National Strategic Studies; 1995. 4 p.; ill. (Series “Strategic forum”; No. 28).
9. Cebrowski A. K., Navy U. S., Garstka J. J. Network — Centric Warfare: Its Origin and Future. *Proceedings*. 1998;(January):76–84.
10. Kolmogorova A. V., Skovorodnikov A. P., Kopnina G. A. Linguistics of Information and Psychological Warfare: In 2 books. Book 1. Krasnoyarsk: Siberian Federal University; 2017. 212 p. (In Russ.).
11. Pocheptsov G. G. Information Wars. A New Policy Instrument. Moscow: Algorithm; 2015. 256 p. (In Russ.).
12. Kablukov E. V. On the issue of updating discursive practices of identification in the context of information warfare. *Professional`naya kul`tura zhurnalista cifrovoy e`poxi : materialy` Vserossijskoj nauchno-prakticheskoy konferencii s mezhdunarodny`m uchastiem (Ekaterinburk, 19 maya 2017 g.) = Professional culture of a journalist in the digital era: materials of the All-Russian scientific and practical conference with international participation (Ekaterinburg, May 19, 2017)*. Ekaterinburg: Ural University; 2017. P. 235–238. (In Russ.).
13. Kotsyubinskaya L. V. The concept of “information warfare” in modern linguistics: new approaches. *Politicheskaya lingvistika = Political linguistics*. 2015;(4(54)):93–96. (In Russ.).
14. Gavra D. P. The category of strategic communication: current state and basic characteristics. *Vek informacii = Information Age*. 2015;(3(4)):229–233. (In Russ.).
15. Minaeva L. V. Strategic communication as a tool for promoting the country's national interests. *Rossijskaya shkola svyazej s obshhestvennost`yu = Russian School of Public Relations*. 2021;(20):52–76. (In Russ.).
16. Tremblay G. From Marshall McLuhan to Harold Innis, or From the global village to the world empire. *Canadian Journal of Communication*. 2014;37(4):561–575. (In Russ.).
17. Foucault M. Politics is a continuation of war by other means. Intellectuals and power: selected political articles, speeches and interviews. Moscow: Praxis; 2002. P. 148–151. (In Russ.).

Информация об авторах

Д. А. Блишун — аспирант;

С. Н. Чирун — доктор политических наук, доцент, профессор кафедры философии и общественно-политических наук.

Information about the authors

D. A. Blishunov — a graduate student;

S. N. Chirun — Doctor of Science (Political), Associate Professor, Professor of the Department of Philosophy and Social and Political Sciences.

Статья поступила в редакцию 05.09.2024; одобрена после рецензирования 19.09.2024; принята к публикации 23.09.2024.

The article was submitted 05.09.2024; approved after reviewing 19.09.2024; accepted for publication 23.09.2024.