Научная статья
https://doi.org/10.24412/3034-3364-2024-4-5
УДК 32

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, МЕДИА И IT-ПЛАТФОРМЫ КАК ИНСТРУМЕНТЫ ВЕДЕНИЯ «ИНФОГИБРИДНЫХ ВОЙН»

Ермаков К.А.
Центр политических исследований «АПЕК-КОНСАЛТИНГ»

Аннотация. *В работе рассматривается использование концепций «Effects-Based Approach to Joint Operations» - совместных операций, нацеленных на конечный эффект (СОНКЭ), служащей основой для реализации Soft Power, сочетающей в себе элементы Hard Power и Soft Power, приводятся этапы реализации СОНКЭ в отношении «враг-систем»; дается характеристика концепции NCW (Network Centric Warfare)- «сетецентрического способа ведения войны» как ведущего способа реализации Hard Power; проводится параллель между разработанными RAND corporation способами осуществления стратегического информационного противоборства и «инфогибридной» войной. С использованием методов системного и структурно-функционального анализа исследуется применение информационных технологий, медиа и IT-платформ в ходе ведения «инфогибридных» войн, делаются выводы: о возможности рассмотрения медиа и IT-платформ как глобальных акторов, непосредственно влияющих на международные отношения; о превращении информационных технологий в инструмент ведения информационно-психологических и «инфогибридных» войн; о «сетецентрическом характере» использования информационных технологий, медиа и IT-платформ в качестве компонентов Smart Power.*

Ключевые слова: *информационно-коммуникационные технологии, «сетецентрическая война», глобальные акторы, медиа и IT-платформы, «инфогибридная» война, стратегическое информационное противоборство, Smart Power, международные отношения, мегатренды.*

INFORMATION TECHNOLOGIES, MEDIA AND IT PLATFORMS AS TOOLS FOR WARRIING "INFO-HYBRID WARS"

Kirill A. Ermakov
Center for Political Studies "APEK-CONSULTING"

Abstract. *The paper considers the use of the concepts of the "Effects-Based Approach to Joint Operations" - joint operations aimed at the final effect (SONKE), serving as the basis for the implementation of Soft Power, combining elements of Hard Power and Soft Power, provides the stages of SONKE implementation in relation to "enemy systems"; provides a description of the NCW (Network Centric Warfare) concept - "network-centric method of waging war" as the leading method of implementing Hard Power; draws a parallel between the methods of implementing strategic information confrontation developed by the RAND corporation and "infohybrid" warfare. Using the methods of system and structural-functional analysis, the use of information technologies, media and IT platforms in the course of waging "infohybrid" wars is studied, conclusions are made: on the possibility of considering media and IT platforms as global actors directly influencing international relations; on the transformation of information technologies into a tool for waging information-psychological and "infohybrid" wars; on the "network-centric nature" of using information technologies, media and IT platforms as components of Smart Power.*

Keywords: *Information and communication technologies, "network-centric warfare", global actors, media and IT platforms, "infohybrid" warfare, strategic information confrontation, Smart Power, international relations, megatrends.*

Введение. События последнего десятилетия XX века оказали очень серьезное влияние на последующее мироустройство, систему международных отношений и архитектуру международной безопасности. Крах Организации стран Варшавского договора, последовавший вскоре распад СССР, выполнявшего роль второго полюса сформировавшейся на тот момент биполярной системы, дали возможность истеблишменту США сделать вывод о победе в Холодной войне [1], и руководствуясь ранее раз-

работанными положениями «гегемонистической стабильности [2], приступить к реализации, описанной З. Бжезинским возможности стать единственным мировым лидером с учетом роста их мощи и влияния [3]. Происходившее, в то же время, опережающее развитие информационно-коммуникационных технологий оказало влияние не только на скорость общественных коммуникаций и возможности доступа к медиа и информационному контенту, проникнув во все сферы жизни общества, но и не осталось без внимания военных аналитиков и инженеров. Последовавшие вслед за этим новые разработки в сфере вооружений, средств управления подразделениями, создание новых средств связи и коммуникации, совершенствование средств, методов и способов разведки, широкое использование автоматизации привели к необходимости создания новых концепций ведения войн в условиях глобального проникновения ИКТ.

Обсуждение. Политика, проводимая США и его сателлитами, непосредственно нацелена на получение односторонних преимуществ как в экономической, в политической сфере и всегда ставит своей задачей достижение определенного конечного эффекта. Достижение намеченных целей происходит с использованием концепции «Effects-Based Approach to Joint Operations» - совместные операции, нацеленных на конечный эффект (СОНКЭ). Концепция СОНКЭ не ограничивается чисто военными составляющими, а представляет из себя определенную совокупность действий, сочетающую в себе элементы Hard Power и Soft Power. Страна, на которую будет оказано воздействие, схематично рассматривается как «враг-система». «Враг-система» при этом изображается в виде сферы, внутри которой в качестве концентрических слоев расположены все компоненты государственной мощи. При этом политическое руководство образует внутреннее ядро, а наружный слой образован непосредственно вооруженными силам, предназначенными для непосредственного отражения внешней агрессии. Этапы осуществления СОНКЭ можно представить следующим образом:

- определение характера и способов наиболее эффективного воздействия на «враг-систему» и при необходимости её окружение;
- перевод её в категорию «система -мишень»;
- определение точек критической уязвимости;
- создание условий по необратимому нарушению стабильности и связей внутри системы;
- достижение синергического эффекта, приводящего к невозможности нормального функционирования;
- разрушение «системы-мишени» под воздействием совокупного кумулятивного эффекта.

В качестве способа реализации Hard Power был предложен NCW (Network Centric Warfare)- «сетецентрический способ ведения войны» [4]. По своей сути концепция «сетецентрической войны» представляет способ координации действий войск с использованием достижений информационно-компьютерных технологий и информационного превосходства в области прогнозирования, осуществления управления, связи, коммуникации по коррекции действий в том числе в режиме реального времени. Её использование также позволяет обеспечить эффективность, непрерывность и адаптивность управления подразделениями на основе анализа (в том числе с использованием ИКТ) всего комплекса поступающей о действиях противника информации. Использование информационных технологий и интернет пространства в военных целях является субтрендом мирового развития. В 2020 г. Министерство обороны США и Илон Маск заключили соглашение о тестовом использовании спутниковой системы интернет Starlink в военных целях. По состоянию на декабрь 2023 года по заявлениям украинских военных, ВСУ использовали около 47 тыс. пользовательских терминалов сети Starlink, которые использовались как для обмена информацией и управления подразделениями, так и для управления БПЛА (беспилотными летательными аппаратами) [5]. 7 декабря агентство Bloomberg сообщило, что Пентагон и компания SpaceX заключили контакт о расширении доступа ВСУ к спутниковой группировке Starshield, обеспечивающей в том числе и защищенный стабильный интернет сигнал для использования в военных целях [6]. 14 декабря 2024 г. Министерство обороны США объявило о запуске программы «Rapid Capability Cell» - четырех пилотных проектов по использованию искусственного интеллекта как на поле боя, так и в управлении предприятиями ВПК [7].

Базовые концепции реализации Soft Power были представлены Дж. Наем еще в 2004 г. [8]. Осуществляемые операции «мягкой силы» всегда отличал ярко выраженный «сетецентрический» характер. Весьма интересным примером совокупного использования информационных технологий и деятельности медиа и IT-платформ в качестве Soft Power является их использование в ходе противоправных действий

при попытке свержения конституционного строя в Республике Беларусь в 2020 г. Исследование, указанных событий, которое провел К. Нагорняк [9], позволило сделать выводы:

- о целенаправленном формировании цикличной протестной активности;

- о наличии двух разработанных в одном координирующем центре сценариев организации свержения конституционного строя: в первом случае предполагалось создание постоянно действующего ядра протестной активности в столице и постепенная изоляция органов государственной власти и управления; во втором - формирование «сетевого протеста» путем организации непрерывной цепи децентрализованных акций с целью последующей организацией постоянных протестов в центре Минска и других крупных городов.

Для достижения указанных целей была запланирована постепенная изоляция так называемых «столпов поддержки режима» -органов государственной и муниципальной власти, институтов внутренней безопасности (МВД, КГБ), банковской системы, промышленности и экономики. Координация и управление протестами, получение обратной связи осуществлялось с использованием информационных технологий, включало в себя создание и использование крупных Telegram-каналов, таких как «Nexta Live», «Nexta TV», «Беларусь головного мозга», «TUT. BY новости», «Радио Свобода Беларусь», «Мая Краіна Беларусь», «Хартия–97%», «Наша Ніва». Указанные ресурсы распространяли методические рекомендации по организации забастовок на предприятиях, анонсировали проведение антиправительственных акций и места их проведения, сообщали о местонахождении и приближении представителей силовых структур, публиковали персональные данные сотрудников силовых структур и органов государственной власти, распространяли специального программное обеспечение по анонимизации пользователей и пр. Также, использовались ИКТ фильтрации для селектирования выдачи информации. При любых поисковых запросах в Google первыми появлялись карты протестов и информация «Euronews» [10]. В этом состоял один из способов поддержки протестующих и предпринималась попытка привлечь большее количество участников и расширить его географию. Особенность протеста в Беларуси в 2020 году состоит в том, что он изначально был задуман как «сетецентрический протест», и для его генерации, управления, получения обратной связи предполагалось использовать в том числе и специально созданные Telegram-каналы для проведения последующего анализа следует отметить, что события августа-сентября 2020 г. в Беларуси, презентованные западными медиа как исключительно мирные действия таковыми не являлись. Только за 10 августа 2020 г. по данным МВД Республики Беларусь пострадали 39 силовиков и более 50 гражданских лиц [11].

События в 2022 г. в Республике Казахстан, в ходе которых для координации действий агрессивно-настроенных жителей, мародеров, заранее организованных и спонтанных преступных группировок, деструктивных элементов и террористических групп широко использовались информационные технологии, также повлекли многочисленные жертвы.

По заявлению Президента РК Касым-Жомарта Токаева, январская трагедия 2022 г. представляла собой «попытку государственного переворота» и «террористическую атаку» на Казахстан [12].

Казахстанский исследователь Р. Сысоева полагает, что хотя «методология организации» этого неудавшегося переворота отличается от уже реализованных сценариев «цветных революций» на постсоветском пространстве и в ряде других регионов, но, несомненно, вбирает их основные технологии [13].

В ходе расследования январских событий по статьям, относящимся к убийствам, похищению оружия, мятежу, мародерствам, было возбуждено более четырех тысяч уголовных дел имущества, пострадало около 5 тыс. человек и погибло более 200 человек [14].

Достижение предусмотренного Smart Power совокупного кумулятивного эффекта, реализуется в том числе на основе разработок по осуществлению стратегического информационного противоборства второго поколения, разработанного RAND corporation. Для данного вида противоборства характерно длительное использование в информационном пространстве новейших достижений ИКТ, направленных как на нанесения максимального вреда «системам-мишеням», так и на обеспечение проекции всех видов мощи США на территорию других стран. М. Лебедева определила современное состояние мира как транснационализацию [15]. Транспарентность государственность границ, частичная утрата суверенитета привели к повсеместному использованию информационных технологий, медиа и IT-платформ, по своей сути и характеру являющихся транснациональными. Основное

направление их деятельности - повсеместное разжигание вражды и розни, достижение определенных политических целей с использованием инструментов манипуляционно-психологического подавления, что позволяет считать их эффективными компонентами ведения информационно-психологической войны, непосредственно подчиняющимися описанным еще К. фон Клаузевицем закономерностям.

Ф. Фукуяма утверждал, что вопросы идентичности станут осью мировой политики XXI веке [16].

Одним из необходимых компонентов ведения войны, не важно используется в ходе неё Hard Power или нет, является создание атмосферы ненависти. Для разжигания вражды и ненависти используются все доступные инструменты: медиа и IT-платформы, средства рекламы и PR-технологии, социальные сети, киноиндустрия, бизнес-коммуникации [17]. В роли координатора действий по разработке, продвижению и реализации, созданных в рамках СОНКЭ стратегий выступает высший менеджмент глобальных IT-платформ («Meta», «YouTube», «WhatsApp», «WeChat», «Google» и др.), СМИ («CNN», «BBC», «Deutsche Welle», «Reuter», «FrancePresse», «The Washington Post», «Голос Америки», «Радио Свобода», «Blumberg», «Economist», «Time», и др.) [18].

С. Небренчин и А. Вьюнов полагают, что все современные войны вне зависимости от того, ведутся ли прямые военные действия или нет, являются «инфогибридными», ввиду их направленности не только на политическую систему, экономику, военное строительство, но и социальную и социокультурную сфере, религиозную и культурную идентичность [19].

С целью защиты национальных интересов Российской Федерации в условиях всеобъемлющего проникновения информационно-коммуникационных технологий, обеспечения функционирования органов государственной власти, защиты прав и свобод граждан Российской Федерации, Указом Президента Российской Федерации была принята Доктрина информационной безопасности Российской Федерации [20].

Соглашение о сотрудничестве государств - членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности также предусматривает дальнейшее развитие системы информационной безопасности государств - членов ОДКБ на основе межгосударственного сотрудничества и укрепления межведомственного взаимодействия [21].

Результаты. Используя методы системного и структурно-функционального анализа можно заключить следующее:

- медиа и IT-платформы стали глобальными акторами, непосредственно воздействующими на международные отношения, и формируют мировосприятие не только отдельных личностей и социальных групп, но и оказывают определяющее влияние на формирование внешней информационной среды;

- информационные технологии превратились в инструмент ведения информационно-психологических и «инфогибридных» войн;

- повсеместное использование ИКТ, медиа и IT-платформ в качестве инструментов СОНКЭ, скоординированный характер действий, несомненная интеграция в общую структуру ведения «инфогибридных» войн, позволяют сделать вывод об их «сетецентрическом характере» в ходе использовании в качестве компонентов Smart Power;

- мегатренд глобального политико цивилизационного противоборства в информационном пространстве оказывает существенное влияние на международные отношения и государственную политику Российской Федерации и стран ОДКБ.

Заключение. Информационные технологии, медиа и IT-платформы непосредственно участвуют в формировании государственной мощи. Их состоявшаяся интеграция в общую структуру ведения «инфогибридных» войн требует учета в ходе оценки вызовов и угроз.

Рассматривая возможные трансформации системы международных отношений, необходимо учитывать роль медиа и IT-платформ как глобальных акторов, непосредственно формирующим информационную среду и оказывающих непосредственное влияние на государственную политику.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование в формате double-blind peer review (рецензенту неизвестны имя и должность ав-

Conflict of Interest

None declared.

Review

All articles are reviewed in the double-blind peer review format (the reviewer does not know the name and position of the author, the author

тора, автору неизвестны имя и должность рецензента). Рецензия может быть предоставлена заинтересованным лицам по запросу.

does not know the name and position of the reviewer). The review can be provided to interested persons upon request.

Литература:

1. Буш Дж. О победе США над СССР в Холодной войне (прямая речь 26.01.1992) URL https://rutube.ru/video/9cbbb7ed12fdbd4742150d57fb51e592/.

2. Webb M.C., Krasner S.D. Hegemonic stability theory: an empirical assessment //Review of International Studies – № 15, 1989. 183-198 pp.

3. Бжезинский, З. Великая шахматная доска / З. Бжезинский; [пер. с англ. О. Уральской]. – М.: АСТ, 2019. – 384 с.

4. Network Centric Warfare. The RMA Debate, (http://www.comw.org/rma/fulltext/netcenterwar.html), (дата обращения 27.09.2024) «Сетецентрическая война. Дайджест по материалам открытых изданий и СМИ». – М. ВАГШ ВС РФ, 2010

5. Varenytsia I. -URL: https://tass.ru/armiya-i-opk/20589497 - (дата обращения 07.12.2024)

6. Пентагон расширит доступ Украины к системе Starshield - URL https://ria.ru/20241207/pentagon-1987867540.html -(дата обращения 16.12.2024)

7. Электронный ресурс URL https://www.defense.gov/News/News-Stories/Article/Article/3999805/dods-chief-ai-officer-launches-rapid-capability-cell-frontier-ai-pilots-to-acce /- (дата обращения 16.12.2024)

8. Nye J. Soft power: The means to success in world politics. New York. 2004.

9. Нагорняк К.И. Активность оппозиционных Telegram-каналов и поведенческий фактор пользователей Google как метод исследования протестов в Белоруссии 2020 года // Вестник Российского университета дружбы народов. Серия: Политология. 2021. Т. 23. № 1. С. 60–77.

10. Электронный ресурс URL: https://korrespondent.net/world/4261878-Google-sozdal-kartu-protestov-v-mynske-a-Telegram-vkluichyl-antytsenzuru -(дата обращения 10.12.2024)

11. Электронный ресурс URL: https://lenta.ru/news/2020/08/10/postr/ – (дата обращения 10.12.2024)

12. Выступление Главы государства Касым-Жомарта Токаева на внеочередной сессии Совета коллективной безопасности ОДКБ // Президент Республики Казахстан. URL: https://www.akorda.kz/ru/vystuplenieglavy-gosudarstva-kasym-zhomarta-kemelevicha-navneocherednoy-sessii-soveta-kollektivnoy-bezopasnostiodkb-1002245 (дата обращения: 10.12.2024)

13. Сысоева Р. В. Январские события 2022 г. и миротворческая операция ОДКБ в Казахстане // Вестник Российского университета дружбы народов. Серия: Международные отношения. 2023. Т. 23, № 2. С. 241—252.

14. Мәжілісте Қаңтар оқиғасының мән-жайы айтылды // Қазақстан Республикасы Парламенті Мәжілісінің. 05.01.2023. (На казахском языке). URL: https://www.parlam.kz/kk/mazhilis/news-details/id49908/1/15 - (дата обращения: 10.12.2024)

15. Лебедева М.М. «Система политической организации мира: «Идеальный шторм». URL: https://cyberleninka.ru/article/n/sistema-politicheskoy-organizatsii-mira-idealnyy-shtorm - (дата обращения 10.09.2024)

16. Fukuyama F. 30 Years of World Politics: What Has Changed? // Journal of Democracy. January, 2020.

17. Федор Пашин Стратегия гибридного сдерживания России. URL: https://cont.ws/@paschin-541/272120. - (дата обращения: 27.09.2024)

18. Небренчин С.М. Стратегия эскалации напряженности в гибридной войне против России. URL: http://ukros.ru/wp-content/uploads/2024/09/Небренчин.pdf. – (дата обращения 06.10.2024)

19. Небренчин С.М., Вьюнов А.С. Современная инфогибридная война против России: стратегия, нарративы, технологии // Военная мысль. -№6, июнь, 2024. – сс.17-34

20. Электронный ресурс URL http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102161033&page=1&rdk=0&link_id=0#I0 – (дата обращения 17.12.2024)

21. Электронный ресурс URL https://docs.cntd.ru/document/542645728 - (дата обращения 17.12.2024).

References:

1. Bush J. About the victory of the USA over the USSR in the Cold War (direct speech on 01/26/1992) URL https://rutube.ru/video/9cbbb7ed12fdbd4742150d57fb51e592 /.

2. Webb M.C., Krasner S.D. Hegemonic stability theory: an empirical assessment //Review of International Studies – No. 15, 1989. 183-198 pp.

3. Brzezinski, Z. The Great Chessboard / Z. Brzezinski; [trans. from the English O. Uralskaya]. – M.: AST, 2019. – 384 p.

4. Network Centric Warfare. The RMA Debate, (http://www.comw.org/rma/fulltext/netcenterwar.html), (accessed 09/27/2024) "Network-centric warfare. Digest based on materials from open publications and mass media." – M. VAGSH of the Armed Forces of the Russian Federation, 2010

5. Varenytsia I. -URL: https://tass.ru/armiya-i-opk/20589497 - (accessed 07.12.2024)

6. The Pentagon will expand Ukraine's access to the Starshield - URL system https://ria.ru/20241207/pentagon-1987867540.html -(accessed 12/16/2024)

7. Electronic resource URL https://www.defense.gov/News/News-Stories/Article/Article/3999805/dods-chief-ai-officer-launches-rapid-capability-cell-frontier-ai-pilots-to-acce /- (accessed 12/16/2024)

8. Nye J. Soft power: The means to success in world politics. New York. 2004.

9. Nagornyak K.I. Activity of oppositional Telegram channels and the behavioral factor of Google users as a method of studying protests in Belarus in 2020 // Bulletin of the Peoples' Friendship University of Russia. Series: Political Science. 2021. Vol. 23. No. 1. pp. 60-77.

10. Electronic resource URL: https://korrespondent.net/world/4261878-Google-sozdal-kartu-protestov-v-mynske-a-Telegram-vkluichyl-antytsenzuru -(accessed 10.12.2024)

11. Electronic resource URL: https://lenta.ru/news/2020/08/10/postr / – (accessed 10.12.2024)

12. Speech by Head of State Kassym-Jomart Tokayev at the extraordinary session of the CSTO Collective Security Council // President of the Republic of Kazakhstan. URL: https://www.akorda.kz/ru/vystuplenieglavy-gosudarstva-kasym-zhomarta-kemelevicha-navneocherednoy-sessii-soveta-kollektivnoy-bezopasnostiodkb-1002245 (date of application: 10.12.2024)

13. Sysoeva R. V. January events of 2022 and the CSTO peacekeeping operation in Kazakhstan // Bulletin of the Peoples' Friendship University of Russia. Series: International Relations. 2023. Vol. 23, No. 2. pp. 241-252.

14. Mazhiliste Kantar okigasynyn man-zhayy aityldy // Kazakhstan Republikasy Parliamenti Mazhilisin. 05.01.2023. (In Kazakh). URL: https://www.parlam.kz/kk/mazhilis/news-details/id49908/1/15 - (date of application: 10.12.2024)

15. Lebedeva M.M. "The system of political organization of the world: "The perfect storm". URL: https://cyberleninka.ru/article/n/sistema-politicheskoy-organizatsii-mira-idealnyy-shtorm - (accessed 09/10/2024)

16. Fukuyama F. 30 Years of World Politics: What Has Changed? // Journal of Democracy. January, 2020.

17. Fyodor Pashin Strategy of hybrid deterrence of Russia. URL: https://cont.ws/@paschin-541/272120 . - (date of access: 09/27/2024)

18. Nebrenchin S.M. Strategy of escalation of tension in the hybrid war against Russia. URL: http://ukros.ru/wp-content/uploads/2024/09/Небренчин.pdf . – (date of address 06.10.2024)

19. Nebrenchin S.M., Vyunov A.S. Modern infohybrid war against Russia: strategy, narratives, technologies // Military thought. -No.6, June, 2024. – ss.17-34

20. Electronic resource URL http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102161033&page=1&rdk=0&link_id=0#I0 – (accessed 12/17/2024)

21. Electronic resource URL https://docs.cntd.ru/document/542645728 - (accessed 12/17/2024)

Информация об авторе:

Ермаков Кирилл Александрович, научный сотрудник, Центр политических исследований «АПЕК-КОНСАЛТИНГ», Россия, Москва, e-mail: profadvmos@mail.ru

Kirill A. Ermakov, scientific fellow, APEK-CONSULTING Center for Political Studies, Russia, Moscow.