Государственное и муниципальное управление. Ученые записки. 2024. № 2. С. 178–183
State and Municipal Management. Scholar Notes. 2024;(2):178–183
Политология и этнополитика

Научная статья
УДК 32
https://doi.org/10.22394/2079-1690-2024-1-2-178-183 EDN CIRDUE

Характерные особенности современных информационных войн политической направленности

Давид Кромвелович Григорян[1],
Евгения Николаевна Кондратенко[2]

[1, 2]Южно-Российский институт управления – филиал Российской академии народного хозяйства и государственной службы при Президенте Российской Федерации, Ростов-на-Дону, Россия
[1]Ростовский юридический институт МВД России, Ростов-на-Дону, Россия
[1]davo-davo23@mail.ru, https://orcid.org/0000-0002-9411-8418
[2]zen2710@yandex.ru, https://orcid.org/0000-0003-0286-5131

Аннотация. В статье проводится анализ характерных особенностей информационных войн политической направленности. Сегодня информационные войны являются неотъемлемым элементом политической системы, выступая в качестве инструмента политического управления. Специфика информационной войны заключается прежде всего в том, что боевые действия происходят в плоскости виртуального пространства. Было выявлено, что всемирная информационная компьютерная сеть вывела информационные войны на новый уровень, став мощным инструментом для реализации информационных атак. Данная тенденция нашла свое отражение в политических конфликтах, которые происходят в границах информационного поля.

Ключевые слова: информация, коммуникация, информационная война, киберпространство, массовое сознание, манипуляция, политические технологии

***Для цитирования*:** Григорян Д. К., Кондратенко Е. Н. Характерные особенности современных информационных войн политической направленности // Государственное и муниципальное управление. Ученые записки. 2024. № 2. С. 178–183. https://doi.org/10.22394/2079-1690-2024-1-2-178-183. EDN CIRDUE

Politology and Ethnopolitics

Original article

Characteristic features of modern information wars of a political orientation

David K. Grigoryan[1],
Evgenia N. Kondratenko[2]

[1, 2]South-Russia Institute of Management – branch of Russian Presidential Academy of National Economy and Public Administration, Rostov-on-Don, Russia
[1]Rostov Law Institute of the Ministry of Internal Affairs of Russia, Rostov-on-Don, Russia
[1]davo-davo23@mail.ru, https://orcid.org/0000-0002-9411-8418
[2]zen2710@yandex.ru, https://orcid.org/0000-0003-0286-5131

Abstract. The article analyzes the characteristic features of information wars of a political orientation. Today, information wars are an integral element of the political system, acting as an instrument of political governance. The specificity of information warfare lies primarily in the fact that the fighting takes place in the plane of virtual space. It was revealed that the worldwide information computer network has brought information warfare to a new level, becoming a powerful tool for implementing information attacks. This trend is reflected in the political conflicts that occur within the boundaries of the information field.

***Keywords**:* information, communication, information warfare, cyberspace, mass consciousness, manipulation, political technologies

For citation: Grigoryan D. K., Kondratenko E. N. Characteristic features of modern information wars of a political orientation. *State and Municipal Management. Scholar Notes.* 2024;(2):178–183. (In Russ.). https://doi.org/10.22394/2079-1690-2024-1-2-178-183. EDN CIRDUE

Информационная война существенно отличается от реальных военных кампаний. Специфика информационной войны заключается прежде всего в том, что боевые действия происходят в плоскости виртуального пространства. Следовательно, ощутить происходящие в информационном поле процессы не предоставляется возможным. В большей степени информационные кампании направлены на психику человека. Манипулятивные технологии, применяемые в ходе информационных кампаний, лишают человека возможности сознательно и рационально воспринимать информацию. Как правило, моральный и этический аспекты, в ходе реализации информационной кампании, не учитываются.

В информационной войне особое внимание уделяется технологиям ведения борьбы [1, с. 111]. Первые приемы воздействия на массовое сознание были известны уже в античные времена. Развитие источников информации и средств коммуникации способствовало появлению более изощренных методов влияния. Данная тенденция сформировала новый пласт, пригодный для изучения специалистами в области психологии, менеджмента и общественных наук. Например, в конце 1930-х гг. в США Институт анализа пропаганды представил семь классических приемов ведения информационной войны [2, с. 89]:

1. «Приклеивание или навешивание ярлыков» (name calling). Ярлык представляет собой оскорбительное выражение, порочащее противника. Прием направлен на формирование негативного отношения общественности к какому-либо объекту с помощью ярлыка.

2. «Сияющие обобщения» или «блистательная неопределенность» (glittering generality). Идеи, выгодные для конкретного субъекта, лоббируются за счет слов, несущих положительную эмоциональную составляющую: «свобода», «мир», «победа» и т.д.

3. «Перенос» или «трансфер» (transfer). То, что не представляет истинной ценности навязывается обществу доступными ассоциативными связями. Используя данный метод в обратную сторону, достигается цель дискредитации.

4. «Ссылка на авторитеты», «свидетельства» или «свидетельствование» (testimonial). Манипулятивное воздействие основывается на оценочных высказываниях личностей, которые имеют в глазах общественности высокий уровень доверия и уважения.

5. «Свои ребята» или «игра в простонародность» (plain folks). Общественное доверие достигается посредством коммуникатора, состоящего в образе человека, прошедшего те же испытания, что и рядовой член общества.

6. «Перетасовка» или «подтасовка карт» (card stacking). Подача информации происходит исключительно с точки зрения, выгодной субъекту.

7. «Общий вагон», «общая платформа» или «фургон с оркестром» (band wagon). Апелляция информацией с отсылкой на большинство. Например, фраза оратора может начинаться со слов: «Каждый сознательный гражданин…».

Очевидно, что развитие информационно-коммуникационных технологий способствовало трансформации информационного пространства. Изменения претерпели все элементы информационной системы. В большей степени влияние на информационно-коммуникативные процессы оказало появление Интернета. Как следствие, всемирная информационная компьютерная сеть вывела информационные войны на новый уровень, став мощным инструментом для реализации информационных атак. Данная тенденция нашла свое отражение в политических конфликтах, которые происходят в границах информационного поля [3, с. 89].

Провокации или искусственное побуждение к ответной реакции удачно подходит для ведения информационной войн. Задача состоит в выводе противника из уравновешенного положения. Необходимо довести его до такого состояния, когда принятие им решений будет происходить бессознательно и нерационально. В политике такой эффект достигается за счет безосновательных скандалов,

обвинений, сфальсифицированных убийств и т.п. Подстрекательство может исходить как извне, так изнутри системы[1].

Современные информационные войны в контексте политики обладают рядом отличительных характеристик.

Во-первых, сегодня объектом целенаправленного информационного воздействия является молодежь [4, с. 483]. Информационные атаки относительно молодой аудитории происходят часто и намеренно. Политические акторы стремятся воспитать молодой электорат нежели изменить идейные установки представителей старшего поколения. Основным инструментом для манипуляции сознанием молодого поколения, как уже было отмечено ранее, является Интернет. В отношении молодежи эффективно работает передача информации посредством социальных сетей, видеохостинговых сайтов, мессенджеров и т.п. Однако стоит отметить, что к лоббированию политических идей посредством интернет-площадок, актуальных для молодежи, в большей степени сегодня прибегают представители оппозиции. Действующая власть в глобальной сети отдает предпочтение официальным сайтам, которые представляют меньший интерес для нового поколения.

Во-вторых, виртуальное противоборство переходит в киберпространство [5, с. 112]. В настоящее время атакам подвергается не только человек, но и устройства коммуникации. В большой политике персональные и конфиденциальные данные сегодня представляют значительную ценность. Хакеры и пранкеры, работающие на успех определенного политического актора могут покушаться на системы связи, энергетические станции, облачные хранилища, банковские информационные системы, предприятия телекоммуникационной, аэрокосмической, энергетической, ядерной, нефтегазовой и транспортной отраслей, компании, занимающиеся разработкой криптографических и нанотехнологий, а также СМИ противника.

В рамках киберпространства применяются технологии, основанные на компьютерных вирусах, кибератаках, шпионаже, троянах [6, с. 34].

Кибератаки бывают следующих видов [7, с. 6]:

a) Distributed Denial of Service (DDoS) атаки подразумевают доведение системы до абсолютного отказа в работе посредством множества запросов. В качестве примера можно привести технологию Smurfing.

b) Remote to Local Attack (R2L) атака подразумевает получение удаленного доступа к компьютеру неавторизованного пользователя. Например, на экране имитируется окно ввода пароля посредством троянского коня.

c) User to Root Attack (U2R) атака подразумевает получение прав администратора, используя уязвимость системы при наличии учетной записи у злоумышленника. В таком случае буфер может быть переполнен, и программа уже не справляется с проверкой данных на соответствие.

d) Probe атака происходит зондированием и подразумевает сканирование сети. Происходит выявление открытых портов и получение доступа к конфиденциальной информации.

Интернет-преступники сегодня становятся полноправными участниками политических процессов. Наиболее известными хакерскими группировками являются Equation Group, Stuxnet, Flame, Carbanak и Lurk. Участники Lurk регулярно совершали кражу крупных сумм со счетов коммерческих организаций, используя для атак вредоносное программное обеспечение[2].

На сайте Лаборатории Касперского представлено описание способов управления политическим процессом в интернет-пространстве. Например, контроль предвыборной кампании может осуществляться посредством следующих технологий[3]:

- политический спам;
- фальшивые опросы общественного мнения;
- тревожные сигналы.

---

[1] Баранов Н. В. Классические технологии информационно-психологической войны. [Электронный ресурс]. Режим доступа: https://nicbar.ru/politology/study/ (Дата обращения: 10.05.2024).

[2] В Екатеринбурге прошло первое заседание по делу группы хакеров Lurk. [Электронный ресурс]. Режим доступа: https://ekb.rbc.ru/ekb/freenews/5c470f329a7947132f34df4b (Дата обращения: 17.05.2024).

[3] Технологии предвыборного обмана в киберпространстве. [Электронный ресурс: официальный сайт международной компании «Лаборатория Касперского»]. Режим доступа: https://www.kaspersky.ru/blog/russian-election-scam-2018/19895/ (Дата обращения: 17.05.2024).

В-третьих, современные информационные кампании отличаются абсолютным пренебрежением моральными и этическими нормами. Цинизм становится ориентиром при подаче информационного материала. Стремление закрепить политическое лидерство стирает все границы дозволенного. Например, конфронтация европейских стран с Россией осуществляется посредством радикальных информационных поводов. Так в Польше борьба с советским прошлым и лояльным отношением к России ведется посредством уничтожения и осквернения памятников героям Великой Отечественной войны. Политика декоммунизации предполагает снос объектов культурного наследия, содержащих в себе отсылку к советскому прошлому. Посол Российской Федерации в Республике Польша Андреев С.В. отмечал: «Если называть вещи своими именами, то против России идет идеологическая и информационная война. И важнейшая составляющая этой информационной войны – война с нашей исторической памятью, война с российской историей»[1].

Еще более ужасающим примером является деятельность террористических организаций в рамках информационного пространства. Радикалы доносят свои политические идеи и религиозные убеждения до всего мирового сообщества посредством распространения видеороликов, содержащих сцены насилия. Данная информационная атака заключает в себе мощное психологическое воздействие. Так экстремисты из группировки «Исламское государство» распространили видеоматериалы, содержащие процесс совершения массовой казни сирийских военнослужащих[2]. Благодаря слаженной работе специальных ведомств, подобный контент изымается из общего доступа.

В-четвертых, современные информационные войны характеризуются многогранностью манипулятивных технологий. Сегодня информация подается таким образом, что не удается окончательно понять ее суть и истинное предназначение. Политические деятели в процессе информационного противоборства часто прибегают к помощи PR-специалистов и политических консультантов. Эксперты в области политической рекламы, имиджмейкинга, спичрайтинга разрабатывают новые способы и приемы для эффективного информационного воздействия [8, с. 59].

Спрос на услуги политического менеджмента способствовал развитию частных коммерческих объединений по данному направлению. Например, в США набирают популярность так называемые «мозговые центры». Сотрудники исследовательских институтов и радиовещательных компаний таких как: RAND Corparation, Centr for Strategie and International Studies, the New York Times, NBC занимаются генерацией идей для результативного принятия решений [9, с. 59]. Как можно заметить, современный американский подход к манипулированию делает ставку на медийную сферу. Политические технологи в значительной степени используют речевые стратегии и языковое манипулирование. Если же говорить о конкретном способе управления сознанием, то американские технологи активно применяют прием внушения страха перед террором, который позволяет создать привлекательный образ спецслужб, расширить их сферу деятельности и повысить уровень их финансирования [10, с. 109].

В-пятых, современные информационные войны обладают диктаторскими чертами. Государства стараются максимально подчинить своему влиянию значительное количество субъектов политики посредством агрессивной информационной политики. Подача политической информации в газетах осуществляется с помощью кричащих заголовков.

В-шестых, сегодня информационные атаки носят систематический и бесперебойный характер. Реакция политических акторов на действия друг друга молниеносная.

В-седьмых, сегодня нет четкого понимания того каким образом фильтровать информационный контент. Сущность и наличие информационных конфликтов бывают скрытыми для простого обывателя. Благодаря умелой подаче политической информации СМИ, человек может неосознанно быть полноценным участником конфликта и до конца не понимать сути происходящего.

На основании вышеперечисленного следует заключить, что на сегодняшний день динамика информационного противоборства определяется развитием информационно-коммуникационных технологий. Временной промежуток между информационными атаками сократился, что привело к увеличению информационных нападений. В настоящее время Интернет является основной площадкой

[1] Польша не жалеет сил в войне с советским прошлым. [Электронный ресурс]. Режим доступа: https://www.vesti.ru/doc.html?id=2738887 (Дата обращения: 18.05.2024).
[2] Боевики ИГ опубликовали видео жестокой расправы над сирийскими военными. [Электронный ресурс]. Режим доступа: https://www.ntv.ru/novosti/1263738/ (Дата обращения: 18.05.2024).

и инструментом для манипулирования, информационное противоборство переходит в киберпространство. Изменение сознания посредством информационных сообщений достигается без учета этических и моральных норм.

Единого и системного подхода по снижению влияния информационных войн на данный момент не существует. Политические информационные атаки достаточно агрессивны и распространяют свое влияние на все сферы общественной жизни. Таким образом, от расстановки сил в информационном пространстве зависит исход политической деятельности. Необходимо основательно изучать особенности информационных войн как явление и разработать системный подход по минимизации влияния деструктивных процессов на все сферы жизни.

Список источников

1. Малик Е. Н., Шедий М. В. Информационная война против России как геополитическая деструкция государственности и политической системы / Современные тенденции развития научного сообщества в эпоху глобальных перемен. Кадырова Б.К., Ахматова А.Т., Шаршеева Б.К., Джантаева Г.А., Воронков А.Н., Елфимов О.М., Кукина Е.А., Набокова М.Б., Гнездилова Л.А., Немцева Н.В., Жемерикина Ю.И., Малик Е.Н., Шедий М.В. Уфа: ООО "Аэтерна", 2023. С. 111-127.

2. Макаров В. Е. Политические и социальные аспекты информационной безопасности: Монография Москва; Таганрог: С. А. Ступин, 2015. 352 с.

3. Кондратенко Е. Н., Григорян Д. К., Погорелов М. А. Анализ информационной конфронтации между российскими и зарубежными СМИ и роль лидерско-элитного фактора в данном процессе// Государственное и муниципальное управление. Ученые записки. 2020. № 1. С. 188–192.

4. Аюрова А. М. Клиповое мышление и информационная война: грани соприкосновения// Вестник современных исследований. 2018. № 7.1 (22). С. 483–489.

5. Информационное право: учебник для вузов/ Н.Н. Ковалева [и др.]; под редакцией Н.Н. Ковалевой. М.: Издательство Юрайт, 2024. 353 с.

6. Дунин В. С., Блинникова Л. В. Аналитический обзор кибернетических угроз инфокоммуникационным системам // Охрана, безопасность, связь. Том 2. № 3 (3). 2018. С. 34–39.

7. Емельянова Ю. Г., Талалаев А. А., Тищенко И. П., Фраленко В. П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы// Программные системы: теория и приложения. 2011. № 3(7). С. 6–10.

8. Маматказин Н. И., Ахмедов Б. Т. Информационная война как фактор реализации геополитических целей / Научный вектор. Сборник научных трудов. Под научной редакцией Е.Н. Макаренко. Ростов-на-Дону, 2022. С. 334-337.

9. Фролова О.А. Внутренняя структура американской политической элиты как субъекта мировой политики в начале XXI века // Современные исследования социальных. 2012. № 10. С. 59–65.

10.Макарова Т. Б. Политическое манипулирование как инструмент укрепления государственной власти в США // Вестник Забайкальского государственного университета. 2015. № 3 (118). С. 107–113.

References

1. Malik E. N., Shady M. V. Information war against Russia as geopolitical de-structuring of statehood and political system. In: *Modern tendencies of development of scientific community in an era of global changes.* Kadyrova B.K., Akhmatova A.T., Sharsheeva B.K., Dzhantaeva G.A., Voronkov A.N., Elfimov O.M., Kukina E.A., Nabokova M.B., Gnezdilova L.A., Nemtseva N.V., Zhemerikina Yu.I., Malik E.N., Shediy M.V. Ufa: "Aeterna"; 2023: 111–127. (In Russ.)

2. Makarov V. E. *Political and social aspects of information security*: Monograph. Moscow; Taganrog: S. A. Stupin; 2015. 352 p. (In Russ.)

3. Kondratenko E. N., Grigoryan D. K., Pogorelov M. A. Analysis of information confrontation between Russian and foreign media and the role of the leadership-elite factor in this process. *State and Municipal Management. Scholar Notes.* 2020;(1):188–192. (In Russ.). https://doi.org/10.22394/2079-1690-2024-1-1-188-192.

4. Ayurova A. M. Clip thinking and information warfare: the edges of contact. *Bulletin of Modern Research.* 2018;7.1(22):483–489. (In Russ.)

5. *Information law: textbook for universities.* N.N. Kovaleva (et al.); edited by N.N. Kovaleva. Moscow: Yurait Publishing House; 2024. 353 p. (In Russ.)

6. Dunin V. S., Blinnikova L. V. Analytical review of cybernetic threats to infocommunication systems. *Protection, security, communications*. 2018;2(3(3)):34–39. (In Russ.)

7. Yemelyanova Yu. G., Talalaev A. A., Tishchenko I. P., Fralenko V. P. Neural network technology for detecting network attacks on information resources. *Software systems: theory and applications.* 2011;3(7):6–10. (In Russ.)

8. Mamatkazin N. I., Akhmedov B. T. *And the information war as a factor in the realization of geopolitical goals.* In: *Scientific vector. Collection of scientific works*. Under the scientific editorship of E.N. Makarenko. Rostov-on-Don; 2022: 334–337. (In Russ.)

9. Frolova O. A. The internal structure of the American political elite as a subject of world politics at the beginning of the XXI century. *Modern social research.* 2012;(10):59–65. (In Russ.)

10. Makarova T. B. Political manipulation as a tool for strengthening state power in the USA. *Bulletin of the Trans-Baikal State University.* 2015;3(118):107–113.

Информация об авторах

Д. К. Григорян – кандидат политических наук, профессор кафедры политологии и этнополитики ЮРИУ РАНХиГС; начальник кафедры информационного обеспечения органов внутренних дел Ростовского юридического института МВД России.

Е. Н. Кондратенко – кандидат политических наук, доцент кафедры политологии и этнополитики ЮРИУ РАНХиГС.

Information about the authors

D. K. Grigoryan – Cand. Sci. (Polit.), Professor of the Department of Political Science and Ethnopolitics, South-Russia Institute of Management – branch of RANEPA; Head of the Department of Information Support of the Department of Internal Affairs, Rostov Law Institute of the Ministry of Internal Affairs of the Russian Federation.

E. N. Kondratenko – Cand. Sci. (Polit.), Associate Professor of the Department of Political Science and Ethnopolitics, South-Russia Institute of Management – branch of RANEPA.

Вклад авторов: все авторы сделали эквивалентный вклад в подготовку публикации. Авторы заявляют об отсутствии конфликта интересов.

Contribution of the authors: the authors contributed equally to this article. The authors declare no conflicts.

Статья поступила в редакцию 13.05.2024; одобрена после рецензирования 30.05.2023; принята к публикации 31.05.2024.
The article was submitted 13.05.2024; approved after reviewing 30.05.2024; accepted for publication 31.05.2024.