

ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2226-7867-2020-10-3-128-131
УДК 32.019.51(045)

Принципы стабильности ресурсов в условиях информационных войн

Д.Э. Ковригин

Финансовый университет, Москва, Россия
<https://orcid.org/0000-0001-9880-1137>

АННОТАЦИЯ

В наши дни многократно усилилась значимость информационных систем, ставших неотъемлемой частью жизни человечества. В современных конфликтах информационные атаки перешли из разряда вспомогательных средств в основные. Умелое управление потоками информации определяет не только специфику, но иногда и результат реальных конфликтов. При этом различные акторы непрерывно ведут между собой войны в информационном пространстве. В конфликте на уровне государств они представляют свою идеологию и образ будущего. Противостояние идет одновременно между всеми государствами, и ни одна сторона априори не может победить. В ходе подобного бесконечного противостояния особо актуальной становится проблема поддержания ресурсной стабильности. Целью данной работы является выделение базовых принципов информационной политики государства.

Ключевые слова: информационно-коммуникационные технологии; информационные атаки; кибербезопасность; гибридная война; информационные ресурсы

Для цитирования: Ковригин Д.Э. Принципы стабильности ресурсов в условиях информационных войн. *Гуманитарные науки. Вестник Финансового университета*. 2020;10(3):128-131. DOI: 10.26794/2226-7867-2020-10-3-128-131

ORIGINAL PAPER

Principles of Stability of Resources in the Conditions of Information Wars

D.E. Kovrigin

Financial University, Moscow, Russia
<https://orcid.org/0000-0001-9880-1137>

ABSTRACT

Today, the importance of information systems, which have become an integral part of human life, has increased many times. During this process, information attacks moved from the category of auxiliary tools to the category of main ones. Now skilful management of information flows determines not only the specifics but sometimes the outcome/result of wars. At the present stage, States are constantly waging wars among themselves in the information space. Each state represents its ideology and image of the future. The confrontation is going on simultaneously between all States, and no side can win a priori. In the course of such an endless confrontation, the problem of maintaining resource stability becomes particularly urgent. The purpose of this work is to highlight the basic principles of the state's information policy.

Keywords: information and communication technologies; information attacks; cybersecurity; hybrid warfare; information resources

For citation: Kovrigin D.E. Principles of stability of resources in the conditions of information wars. *Gumanitarnye Nauki. Vestnik Finasovogo Universiteta = Humanities and Social Sciences. Bulletin of the Financial University*. 2020;10(3):128-131. DOI: 10.26794/2226-7867-2020-10-3-128-131

К началу XXI в. государства стали постепенно отказываться от ведения крупномасштабных военных кампаний, так как ущерб, наносимый ими, огромен. Ставка сделана на типы силовой активности, в последнее время обобщенно называемые термином «гибридная война». Впервые об этой концепции написали Джеймс Н. Мэттис и Фрэнк Г. Хоффман в статье, опубликованной 8 ноября 2005 г., «Future Warfare: The Rise of Hybrid Wars». В ней говорится о том, что существуют как традиционные, так и нетрадиционные методы ведения войны. В классическом формате ведения войны, по заявлению авторов, «...очевидно, что Соединенные Штаты будут доминировать над обычными противниками в обозримом будущем» [1]. Но противник может использовать неожиданные сочетания технологий и тактики, — такие методы ведения войны, как организация беспорядков, терроризм, нелимитированное насилие, партизанская война, наркопреступность становятся все более изощренными и являются серьезной угрозой безопасности США в глобальном масштабе. Действия врага, полагают Д. Н. Мэттис и Ф. Г. Хоффман, направлены на аккумуляцию эффекта нескольких тактических действий, при этом они усиливают результат через СМИ, ведя информационную войну.

Таким образом, методы информационного воздействия являются неотъемлемым элементом гибридной войны. Более того: там, где возможно обмениваться информацией, можно вести информационные боевые действия [2, 3].

Представления об информационной войне в общем виде сформировались в конце XX в. и в теорию гибридных войн интегрировались в сложившемся виде. Сам термин предложил использовать еще в 1976 г. Томас Рон [4]. Информационная война определяется им как воздействие на гражданское население, власти и вооруженные силы с помощью распространения специально подготовленной информации. К ней относятся действия, направленные на достижение превосходства путем нанесения ущерба информации и информационным системам противника. Благодаря новым коммуникационным технологиям в XX и XXI вв. данный тип войны вышел на передний план [5].

Следует учитывать, что в организации внутренней связи различные страны в той или иной степени зависимы от других государств.

Например, около 45% внутреннего канадского трафика проходит через США, и лишь затем возвращаются в Канаду. С Российской Федерацией ситуация схожая: «25% потока информации покидает территорию России, проходит через Швецию, чтобы снова закончить маршрут в России» (<https://internetintel.oracle.com/blog-single.html?id=Analysis+by+Oracle+Internet+Intelligence+Highlights+China%E2%80%99s+Unique+Approach+to+Connecting+to+...>). Единственным, имеющим возможность частично функционировать в неглобальной сети (без подключения к западным сервисам), является китайский интернет. В соответствии с отчетами Oracle, в Китае очень мало точек подключения к глобальному интернету, также на территории этой страны не функционируют иностранные операторы связи. Таким образом, внутренний трафик никогда не покидает пределы КНР. Но даже это полностью не способно защитить китайский интернет от внешних угроз.

В таком контексте необходимо решать вопрос о тех ресурсах, которые могут привлечь большинство государств для ведения информационной войны. Речь не идет о таких технологических гигантах, как США, или о государствах, количественно подавляющих многие внешние проблемы, например, о Китае. Мы говорим о государствах, не контролирующих разработку технологий и производство технических средств, т.е. занимающих оборонительную позицию. И их единственный ресурс — генерирование информации в таком количестве, чтобы этого оказалось достаточно для стабилизации внутренней ситуации и оперативной закрытости коммуникационной системы от внешнего информационного давления.

Задача должна решаться как технически, так и средствами, предлагаемыми семиотическим подходом к организации и развитию массовых коммуникаций. В общем виде задача определяется как необходимость поддержания многообразия информационных потоков — то есть создание системы, которая характеризуется множественностью средств производства информации, различной ее направленностью, а также наличием совокупности информационных пространств и пространств общественных дискуссий [7].

Наиболее комфортной базовой концепцией, позволяющей описать оптимальную модель «защитного» многообразия информационных

потоков, представляется теория социальных систем Н. Лумана. Основными принципами ресурсной стабильности коммуникационных процессов в таком случае являются следующие:

1. *Стремление к информационному разнообразию.* Полная информационная изоляция населения была трудно осуществима даже в период холодной войны. На современном этапе создание изолированного информационного пространства — еще более сложная задача. Человек, получив доступ к иностранным СМИ и увидев иную медиареальность, только в силу впечатления от количественного разнообразия будет склонен воспринимать эту иную реальность как систему коммуникативных способов представлений, становящихся основанием для его действий [8]. В связи с этим, в любом полагающем себя независимым информационном пространстве необходимо стремиться к созданию системы оснований действия через поддержание количественной вариативности, разнообразия. Это особенно важно, если учесть, что количественное уменьшение в общественной коммуникации числа структурированных суждений (мнений) разрушает ее способность адаптировать управленческую систему к новым вызовам. Данная позиция логически подводит к следующему пункту.

2. *Изложение мнения в нескольких версиях (стремление к вариативному идеологическому спектру интерпретаций).* Под этим понимается создание диапазона мнений и интерпретаций, в котором официальная позиция по определенному вопросу может варьироваться. Одна жестко сформулированная позиция значительно более уязвима для критики, чем несколько различных. Для субъекта принятия решения желательно не поддерживать полностью ни одно из них, что оставляет пространство для маневров в случае изменения политической ситуации. Даже полная смена политического курса в подобном случае пройдет относительно спокойно.

3. *Институциональная разведенность каналов трансляции мнений.* Необходимо создавать специализированные информационные каналы для представителей различных социальных групп и интересов. Подобные каналы дают системный контроль за специфической информацией, получаемой социальными группами. Используя язык, актуальный для определенных сообществ, государство способно проецировать свои идеи с меньшими транзакционными издержками.

4. *Дублирование возможной позиции внешнего давления внутренними структурами.* Здесь можно воспользоваться понятием о «структурном дрейфе», разработанном по отношению к биологическим системам У. Матурано и Ф. Варела [6]. В случае межкультурных коммуникаций структурный дрейф описывает ситуацию, когда одна культура пытается заимствовать у другой что-то одно, например, технологию производства, но вместо этого мигрирует связанная группа культурных концептов, начинающая системное развитие уже неподконтрольное заимствовавшей ее культуре.

Проиллюстрируем данный процесс на условном примере времен холодной войны. Предположим, что граждане некоей страны с авторитарным политическим режимом, знакомясь с самопрезентацией американской политической системы, могли предположить, что доступность благ для жителей США связана не с долгим развитием экономики страны, а с их двухпартийной системой. Таким образом, у этих граждан возникли ассоциативные связи между благами, предоставляемыми государством и идеологическим окрасом его политики. Предположим, что отсутствие многопартийности стало поводом для длительного системного пропагандистского воздействия со стороны условных США. Естественно, что государству, желающему заполучить технологии без привязки к социальным изменениям, в этом случае выгоднее иметь на своей территории некоторое количество партий с различной политической направленностью, показывая тем самым своим гражданам отсутствие связи между социальными благами и той или иной политической доктриной. Но если сама возможность многопартийности не представлена в авторитарной культуре хотя бы в виде актуализируемого исторического экскурса, то у такого государства нет ресурсов информационного противостояния внешнему воздействию, и его общество будет «инфицировано» факторами, задающими неконтролируемое субъектами власти развитие.

Все вышеобозначенное приводит нас к признанию того, что в современных условиях конфликты не могут быть окончательно выиграны ни одной из сторон, поэтому ведутся непрерывно и являются фоном для всех политических событий. Для оборонительной позиции на первое место выходит разумный менеджмент информационных ресурсов государства.

СПИСОК ИСТОЧНИКОВ

1. Mattis J. N., Hoffman F. G. Future Warfare: The Rise of Hybrid Wars. URL: <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf>.
2. Штофер Л. Л. Информационная война как радикальная форма политической борьбы. *Гуманитарий Юга России*. 2018;7(4):158–174.
3. Юрков Д. В. Проблемы информационно-психологической безопасности общества в контексте обеспечения национальных интересов России в информационной сфере. *Вестник Российского университета дружбы народов. Серия: Государственное и муниципальное управление*. 2016;(1):39–49.
4. Кихтан В. В., Качмазова З. Н. Информационная война: понятие, содержание и основные формы проявления. *Вестник Волжского университета им. В. Н. Татищева*. 2018;2(2):228–235.
5. Гладкова Л. А. Глобальная информационная война. *Социально-гуманитарные знания*. 2016;(1):36–44.
6. Обзор монографии: Матурана У., Варела Ф. Древо познания. Пер. с англ. *Социологический журнал*. 2003;(2):168–179.
7. Мирзаев А. А. Информационное многообразие и проблемы патриотического воспитания будущих специалистов в условиях вуза. *Человек и образование*. 2018;3(56):118–122.
8. Луман Н. Реальность массмедиа. Пер. с нем. М.: Праксис; 2005. 256 с.

REFERENCES

1. Mattis J. N., Hoffman F. G. Future Warfare: The Rise of Hybrid Wars. URL: <http://milnewstbay.pbworks.com/f/MattisFourBlockWarUSNINov2005.pdf> (accessed on 17. 02. 2020).
2. Stover L. L. Information warfare as a radical form of political struggle. *Gumanitarii Yuga Rossii*. 2018;7(4):158–174. (In Russ.).
3. Yurkov D. V. Problems of information and psychological security of society in the context of ensuring national interests of Russia in the information sphere. *Vestnik Rossiiskogo universiteta druzhby narodov. Seriya: Gosudarstvennoe i munitsipal'noe upravlenie*. 2016;(1):39–49. (In Russ.).
4. Kihtan V. V., Kachmazova Z. N. Information war: concept, content and main forms of manifestation. *Vestnik Volzhskogo universiteta im. V. N. Tatishcheva*. 2018;2(2):228–235. (In Russ.).
5. Gladkova L. A. Global information war. *Sotsial'no-gumanitarnye znaniya*. 2016;(1):36–44. (In Russ.).
6. Review of the monograph: Maturana W., Varela F. Tree of knowledge. Translated from English. *Sotsiologicheskii zhurnal*. 2003;(2):168–179. (In Russ.).
7. Mirzaev A. A. Information diversity and problems of Patriotic education of future specialists in the conditions of higher education. *Chelovek i obrazovanie*. 2018;3(56):118–122. (In Russ.).
8. Luman N. The reality of mass media. Moscow: Praxis; 2005. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Дмитрий Эльдарович Ковригин — студент 4-го курса бакалавриата факультета социологии и политологии, Финансовый университет, Москва, Россия
dmitrykovr@gmail.com

ABOUT THE AUTHOR

Dmitry E. Kovrigin — 4th-year undergraduate student, Faculty of Sociology and Political Sciences, Financial University, Moscow, Russia
dmitrykovr@gmail.com

Статья поступила 25.03.2020; принята к публикации 20.04.2020.

Автор прочитал и одобрил окончательный вариант рукописи.

The article received on 25.03.2020; accepted for publication on 20.04.2020.

The author read and approved the final version of the manuscript.