ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНСТИТУТ
МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ (УНИВЕРСИТЕТ)
МИНИСТЕРСТВА ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

На правах рукописи

ЖУКОВ Артём Владимирович

СОЦИАЛЬНЫЕ СЕТИ КАК ИНСТРУМЕНТ ПОЛИТИЧЕСКОЙ ВЛАСТИ: ВЛИЯНИЕ НА МЕЖДУНАРОДНУЮ БЕЗОПАСНОСТЬ

Специальность 22.00.05 – Политическая социология

Диссертация на соискание ученой степени
кандидата социологических наук

Научный руководитель:
доктор исторических наук, профессор
Подберёзкин Алексей Иванович

Москва – 2020

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ 3

ГЛАВА 1. МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ В КИБЕРПРОСТРАНСТВЕ: СТРАТЕГИЧЕСКИЙ КОНТЕКСТ 19

1.1. Киберпространство как сфера международных отношений и национальной безопасности 19

1.2. Структура кибервласти и стратегический потенциал государства в XXI веке 35

1.3. Кибервойна как проявление сложного информационно-политического насилия 56

Выводы к главе 1 69

ГЛАВА 2. СОЦИАЛЬНЫЕ СЕТИ КАК СТРАТЕГИЧЕСКИЙ РЕСУРС КИБЕРВОЙНЫ 72

2.1. Социальные сети как фактор стратегической безопасности 72

2.2. Факторы политической мобилизации в социальных сетях 83

2.3. Травматизация сознания в социальных сетях как новая форма политического насилия: вызовы национальной безопасности 93

Выводы к главе 2 111

ЗАКЛЮЧЕНИЕ 114

СПИСОК ЛИТЕРАТУРЫ 118

ВВЕДЕНИЕ

Актуальность исследования объясняется несколькими важными обстоятельствами. Современный мир радикально изменяется: идет процесс перехода от доминирования линейного к нелинейному развитию. Его квинтэссенцию выразил лауреат Нобелевской премии И.Р. Пригожин в постулате «стрелы времени» - ускоряется и усложняется развитие живой и неживой природы, а также человеческих обществ. Из этого следует, что современные социальные структуры становятся открытыми неустойчивыми, неравновесными, саморазвивающимися. Сказанное относится и к характеру социальных сетей – они не только ускоренно развиваются, но и качественно усложняются, становятся саморазвивающимися системами, в значительной степени существующими независимо от «воли» человека, что, соответственно, формирует сложные риски и уязвимости для функционирования социума, усложняет и международные отношения и международную безопасность. В значительной степени под влиянием фактора сетевого развития общества осуществился переход от Ньютоновской к Энштейновской картине мира, что предполагает *нелинейный взгляд* на природу международных отношений и выработку новых подходов к их интерпретациям, одним из которых стал «квантовый подход»[1]. В продолжении подобного рода исследований автор считает актуальным учесть *факторы сложности и саморазвития социальных сетей,* сопровождающиеся возникновением эмерджентных реалий («соседствующих пространств», «вневременного времени», «культуры реальной виртуальности»[2]), что привело в XXI веке к *радикальным изменениям* природы международных отношений и международной безопасности – они развиваются не только под влиянием осознанных действий людей, но и в силу своей *саморефлексивной*

[1] Алексеева Т.А., Минеев А.П., Лошкарёв И.Д., Ананьев Б.И. «Квантовый подход» к международным отношениям. М.: Знание Сила, 2018.

[2] Castells M. The Information Age: Economy, Society and Culture. Vol.I: The Rise of the Network Society. 2-nd ed. Cambridge MA. Oxford UK: Blackwell Publishers, 2010.

природы – «рефлексивному творению истории»[3]. Такого фактора в истории международных отношений ранее не существовало, и на него пока не обращено должное внимание исследователей. Благодаря сложным социальным сетям появились принципиально новые политические инструменты влияния и управления акторами мирового сообщества. Фактически произошло определённое перераспределение внутри всей системы международной обстановки (МО) в пользу новых, прежде всего, информационных и цифровых средств формирования смыслов политики и международной безопасности посредством власти *кодов сигнификаций*[4] опасностей и угроз. В глобальной сети интернет, частью которой являются социальные интернет-ресурсы, осуществляется *конструирование значимых смыслов* опасности/безопасности, которые активно используются международными акторами. Как считает Дж. Александер, политические технологии, производимые ими доминирующие смыслы посредством кодов сигнификации, могут в заданном направлении формировать общественное сознание, что используется для достижения политических целей[5]. Пример тому – искусственно инсценируемая угроза России западному миру. Эта тенденция производства политически заданных смыслов со временем приобрела глобальный характер, стала новой социально-политической властью, которая изменяет реалии международной безопасности. Смыслы, производимые посредством кодов сигнификации, по существу, становятся своего рода материальной силой, задающей характер сознания и поведения как простых граждан, так и политических акторов. Как заявляет У. Бек, то, что отношения производства в капиталистическом обществе представляли для Карла Маркса, то *отношения определения* представляют сегодня: «”Отношения определения” основываются на контроле над “средствами определения”, над научными и легальными правилами. Здесь, аналогично,

[3] Giddens A.Modernity and Self-identity: Self and Society in the Late Modern Age. Cambridge: PolityPress, 1991. P. 109.

[4] Бодрийяр Ж. К критике политической экономии знака. М.: Библион-Русская книга, 2003.

[5] Alexander J. C. The Meaning of Social Life: A Cultural Sociology. New York: Oxford University Press, 2003.

существуют “собственники средств определения” – конкретно, ученые и эксперты – и граждане “лишенные средств определения”, которые имеют зависимый статус “простых людей” и которые подвержены власти определения и выбора экспертов, решающих от имени всех»[6]. Из этого следует, что «публичная дипломатия Web. 2.0», создающая *смыслы как реальных, так и мифических, инсценированных угроз*, представляет собой комплекс силовых инструментов политического влияния новой политической власти. Однако пока недостаточно показано влияние созданных в сетях *инсценированных угроз* на международную безопасность. Инсценированные угрозы по своей силе могут превосходить реальные опасности.

Таким образом, актуальность исследования определяется разработкой подхода к интерпретации социальной сети как новой политической власти, представляющей социальное взаимодействие, при котором одна сторона навязывает волю другим с помощью кодов сигнификаций, искусственно произведенных политически заданных смыслов, что изменяет характер международной безопасности вообще и, соответственно, предполагает востребованность новых подходов к национальной безопасности России

Степень разработанности проблемы. Исследование влияния социальных сетей и Веб 2.0 технологий на международную безопасность вследствие своей новизны и масштабности мало изучено в российской и зарубежной литературе. Лишь отдельные аспекты данной темы являются достаточно разработанными в науке. Материалы, использующиеся в качестве источниковедческой базы исследования, можно разделить на три группы. К *первой группе* источников относятся международные и национальные нормативно-правовые акты:

– обеспечивающие безопасность киберпространства[7];

---

[6] Beck U. World at Risk. Cambridge: Polity Press, 2010.

[7] Cyber Security Strategy of the European Union: An open, safe and secure Cyberspace. JOIN (2013). European Commission, Brusscls, 2013. URL: https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (дата обращения 13.04.2020);

– способы борьбы с преступлениями в сфере компьютерной информации[8];

– доктрины и стратегии национальной и информационной безопасности и поведения в киберпространстве[9];

– законы, защищающие свободы граждан на самовыражение и защиту интеллектуальной собственности[10].

Большое значение имеют общенациональные документы по безопасности стран, где специальные разделы посвящены информационной безопасности[11].

В России в последние два десятилетия были заложены фундаментальные положения государственной политики информационной безопасности в Военной доктрине страны[12] и в целой серии документов[13].

Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for Council concerning measures for a high common level of security of network and information systems across the Union. 6.07.2016. URL: http://eur-lex.europa.eu/legal-292content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc= OJ:L:2016:194:TOC (дата обращения 17.02.2020).

[8] European Union Action Plan on Promoting Safer Use of the Internet. 276/1999/EC. URL: http://cordis.europa.eu/programme/rcn/665_en.html (дата обращения 13.04.2020); а также: О мерах по обеспечению информационном безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: указ Президента Российской Федерации № 351 от 17.03.2008. URL: http://minsvyaz.ru/common/ upload/UKAZ_351 l.pdf (дата обращения 9.04.2019); Об информации, информационных технологиях и о защите информации: Федеральный закон РФ от 14.07.2006. URL: http://docs.cntd.ru/document/ 901990051 (дата обращения 12.06.2018)

[9] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Утв. Президентом Российской Федерации Пр. № 1753 от 01.08.2013. / Совет Безопасности РФ. URL: https://xn--blaew.xn--plai/upload/sitel/document_file/Osnovy_gospolitiki_v_oblasti_mezhd_inf_ bezopasnosti.pdf (дата обращения 17.09.2019)

[10] Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. Минск, 2001.

[11] Стратегия национальной безопасности Российской Федерации до 2020 года / Утверждена указом Президента Российской Федерации от 12 мая 2009 года № 537 // URL: http://www.mid.ru/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/ content/id/294430 (дата обращения 13.04.2020); Department of Defense Strategy for Operating in Cyber Space. U.S. Department of Defense. 2011. July; National security strategy. The White House. 2010, May; OECD "Internet Content Self-Regulation Dialogue". Member Statement on "Impact of Self-Regulation and Filtering on Human Rights to Freedom of Expression" Paris, 1998. URL: http://www.gilc.org/speech/ratings/gilc-oecd-398.html (дата обращения 05.03.2020); WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs) Marrakesh, 1994. URL: http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm (дата обращения 11.02.2020).

[12] Путин В.В. Указ № 815 от 26 декабря 2014 «О признании утратившим силу Указа Президента РФ от№146 от 2010 «О Военной доктрине Российской Федерации».

[13] Концепция развития информационного общества Европейского союза. 11.05.07. URL: http://geum.ru/next/art-181681.php (дата обращения 07.06.2019); О государственной программе Российской Федерации «Информационное общество (2011–2020 годы): распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815 // Российская газета. 16.11.2010. URL: http://www.rg.ru/2010/ll/16/infobschestvo-site-dok.html (дата обращения 19.03.2019); О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы. Указ Президента Российской

Во *вторую группу* источников включены работы отечественных и зарубежных социологов и политологов, посвященных:

– изучению проблем современного сложного общества, факторов глобальной информатизации[14];

– теории международных отношений[15];

– использованию невоенных инструментов внешнеполитического влияния и анализу информационно-силовых факторов национальной и международной безопасности[16];

– роли политики силы в международных и военно-политических отношениях[17]. Среди современных исследователей значительный вклад в

Федерации 09.05.2017 г. № 203. URL: http://docs.cntd.ru/document/420397755 (дата обращения 13.04.2020); Постановление Правительства РФ от 28 января 2002 г. N 65 «О федеральной целевой программе "Электронная Россия (2002–2010 годы)» // URL: http://dokipedia.ru/document/5273762 (дата обращения 14.01.2020); Стратегия развития информационного общества в Российской Федерации. Утверждена 7.02.2008. Пр-212. URL: http://docs.cntd.ru/document/902087132 (дата обращения 08.02.2020).

[14] Malicious Cyber-Enabled Activities. Washington, April, 2015. URL: https://www.treasury.gov/resource-center/sanctions/Programs/Documents/cvber_eo.pdf (дата обращения 13.04.2020); Castells M. The Information Age: Economy, Society and Culture. Vol.I: The Rise of the Network Society. 2-nd ed. Cambridge MA. Oxford UK: Blackwell Publishers,2010; Castells M. The Information Age: Economy, Society and Culture. Vol.II: The Power of Identity. Malden MA. Oxford UK: Blackwell Publishers, 1996; Бек У. Что такое глобализация? / пер. с нем. А. Григорьева и В. Седельника, общая ред. и предисл. А. Филиппова. М.: Прогресс-Традиция, 2001; Глобализация: человеческое измерение / ред. совет А.В. Торкунов (пред). М.: РОССПЭН, 2003; Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития. М. 1999; Кастельс М. Становление общества сетевых структур // Новая постиндустриальная волна на Западе: Антология. М.: Academia, 1999; Тоффлёр Э. Третья волна / под ред. П.С. Гуревича. М.: АСТ, 1999.

[15] Чугунов А.В. Развитие информационного общества: теории, концепции и программы: учебное пособие. СПб.: Ф-т филологии и искусств СПбГУ, 2007; Бжезинский З. Между двумя веками: роль Америки в эру технотроники / Between Two Ages: America's Role in the Technetronic Era / пер. с англ. И.М. Максимовой. М.: Прогресс, 1972; Хрусталев М.А. Методология прикладного политического анализа: учебное пособие / Московский гос. ин-т междунар. отношений (ун-т) МИД России, инновационная образовательная прогр. М.: Проспект, 2010; Богагуров А.Д., Хрусталев М.А., Косолапов И.А. Очерки теории и политического анализа международных отношений. М.: НОФМО, 2002.; Шаклеина Т.А. Россия и США в мировой политике. М.: Аспект Пресс, 2012; Лебедева М.М. Мировая политика. Учебник для бакалавров. Изд. 2-е., перераб. М.: Кнорус, 2013.

[16] Подберезкин А.И., Александров М.В. Мир в XXI веке: прогноз развития международной обстановки по странам и регионам: монография / под ред. М.В. Александрова, О.Е. Родионова. М.: МГИМО, Центр военно-политических исследований, 2018; Подберезкин А.И. Состояние и долгосрочные военно-политические перспективы развития России в XXI веке / Моск. гос. ин-т междунар. отношений (ун-т) М-ва иностр. дел Рос. Федерации, Центр военно-политич. исследований. М.: Издательский дом «Международные отношения», 2018.; Антюхова Е.А. Публичная дипломатия: теория и практика / Е.А. Антюхова, Б.Х. Бахриев, К.П. Боришполец, Х.Р. Джаббари Насир, Е.С. Зиновьева, Т.В. Зонова, В.В. Каберник, М.М. Лебедева, Ю.А. Никитина, А.И. Подберезкин, О.А. Тимофеева, М.В. Харкевич, Д.Д. Шебалин, Е.О. Шебалина; под ред. Лебедевой М.М. М.: Аспект Пресс, 2017.

[17] Гринберг Т.Э. Политические технологии. М.: Аспект Пресс, 2012; Подберезкин А.И. Стратегия национальной безопасности России в XXI веке: аналитич. доклад. М.: МГИМО-Университет, 2016; Davis, Paul K., O'Mahony A. A Computational Model of Public Support for Insurgency and Terrorism: A Prototype for More-General Social-Science Modeling, Santa Monica, Calif.: RAND Corporation, TR-1220-OSD. As of November 13, 2015; Проблемы информационной безопасности в международных военно-политических отношениях. Под ред. А.В. Загорского, Н.П. Ромашкиной. М.: ИМЭМО РАН, 2016; Манойло А.В.

изучение различных теоретических аспектов международной безопасности и мировой политики внесли: В.А. Веселов[18], А.А. Кокошин[19], Н.А. Косолапов, В.М. Кулагин[20], М.М. Лебедева[21], С.А. Панарин[22], А.В. Торкунов[23], А.И. Уткин[24], А.В. Фененко[25] и др;

– особое внимание уделено исследованиям травм современного общества, особенно связанным с деформациями общественного сознания[26].

Наконец, к третьей группе источников относятся работы, посвященные анализу социальных сетей Интернета как инструментам политического влияния[27]. Рассмотрение процессов глобальной информатизации сделано на основании работ М. Кастельса[28], Н. Лумана[29], М. Маклюэна[30], Ю.

Государственная информационная политика в особых условиях. М.: МИФИ, 2003; Козин В. Политика и стратегия США в геополитической динамике XXI века. М.: Граница, 2014.

[18] Веселов В.А. Международная безопасность и контроль над вооружениями. М.: Макс-Пресс, 2005.

[19] Кокошин А.А. Политико-военные и военно-стратегические проблемы национальной безопасности России и международной безопасности. М.: Высшая школа экономики, 2013.

[20] Кулагин В.М. Международная безопасность. М.: Аспект Пресс, 2007; Кулагин В.М. Мир в XXI веке: многополюсный баланс сил или глобальный pax democratica? (Гипотеза «демократического мира» в контексте альтернатив мирового развития) // Полис, 2000. № 1. С. 23-37.

[21] Лебедева М.М. Мировая политика. Учебник для бакалавров. М.: Кнорус, 2013.

[22] Панарин С.А. Безопасность как ценность и норма: опыт разных эпох и культур. СПб: Интерсоцис, 2012.

[23] Симония Н.А., Торкунов А.В. Новый мировой порядок: от биполярности к многополюсности // Полис. Политические исследования, 2015. № 3. С. 27-37.

[24] Уткин А.И. Новый мировой порядок. М.: Алгоритм, Эксмо, 2006.

[25] Фененко А.В. Современная международная безопасность: Ядерный фактор. М: Аспект Пресс, 2013.

[26] Тощенко Ж.Т. Общество травмы: между эволюцией и революцией (опыт теоретического и эмпирического анализа). М: Весь Мир, 2019; Штомпка П. Социальное изменение как травма // Социологические исследования. 2001. № 1. С.6-16; Штомпка П. Культурная травма в посткоммунистическом обществе // Социологические исследования . 2001. № 2. С. 3-12; Alexander J.C. The meaning of social life: a cultural sociology. Oxford: Oxford University Press, 2003; Alexander J.C. Trauma: A Social Theory. Cambridge: Polity Press, 2012; Alexander J.C. The Drama of Social Life. Cambridge: Polity Press, 2017.

[27] Подберезкин А.И. Проект долгосрочной стратегии национальной безопасности России с методологическими и методическими комментариями: аналит. доклад / [А.И. Подберезкин (рук. авт. кол.) и др.]. М.: МГИМО-Университет, 2016; Носетти Ж. Кремль «ВКонтакте»: власть и интернет в России. Центр Россия/ННГ, 2011; Сазанов В.М. Социальные сети – публичная сфера. М.: Лаборатория СВМ, 2012; Казаринова Н.В. Основы теории коммуникации. СПб.: Роза мира, 2006; Лещенко А.М. Социальные сети как механизм конструирования коммуникации в современном обществе. Автореф. дис. канд. филос. наук. Пятигорск, 2011; Boyd D. Taken Out of Context: American Teen Sociality in Networked Publics. – A dissertation submitted in partial satisfaction of the requirements for the degree of Doctor of Philosophy in Information Management and Systems and the Designated Emphasis in New Media in the Graduate Division of the University of California. Berkeley, 2008.

[28] Castells M. The rise of the network society: The information age: Economy, society, and culture. John Wiley & Sons, 2011. Т. 1.; Castells M. The power of identity: The information age: Economy, society, and culture. John Wiley & Sons, 2011.

[29] Луман Н. Введение в системную теорию. М.: "Логос", 2007.

[30] Маклюэн М. Галактика Гуттенберга: становление человека печатающего. М.: Академический проект: Фонд «Мир», 2005; Маклюэн М. Понимание медиа: внешние расширения человека. М.: Канон-пресс, 2003.

Хабермаса[31] и других социологов, которые понимают сетевой характер как главную определяющую черту глобального информационного общества. Эти базовые положения присутствуют в работах, комментариях и интерпретации отечественных ученых: Т.А. Алексеевой[32], Э.Я. Баталова[33], А.Д. Богатурова[34], В.Н. Конышева[35], П.А. Цыганкова[36], В.Ф. Петровского[37], и в авторитетных работах С.А. Ланцова[38], Н.Р. Сетова[39] и др.

Теоретическая и методологическая основа исследования. Проработка теоретических и методологических основ исследования имеет важное значение, потому что она связана с осознанием и изучением тех фундаментальных изменений, которые произошли в современной системе МО и, как следствие, – силовых (прежде всего, информационно-сетевых) средств политического влияния. Именно поэтому в работе было посвящено значительное внимание изучению методологических новаций относительно общей формулы К. Клаузевица о том, что «война есть крайнее средство политики» и «война — это акт насилия, имеющий целью заставить противника выполнить вашу волю»[40]. При этом данная формула отнюдь не предполагает только военного «насилия», что очень современно, потому что

---

[31] Хабермас Ю. Вовлечение другого. Очерки политической теории. СПб.: Наука. 2001.

[32] Алексеева Т.А. Современная политическая мысль (XX–XXI вв.): политическая теория и международные отношения. М.: Аспект Пресс, 2015.

[33] Баталов Э.Я. Американская политическая мысль XX века. М.: Прогресс-Традиция, 2014.

[34] Богатуров А.Д. Очерки теории и политического анализа международных отношений / А.Д. Богатуров, Н.А. Косолапов, М.А. Хрусталев; научно-образоват. форум по междунар. отношениям. М. 2002.

[35] Конышев В.Н. Американский неореализм о природе войны: эволюция политической теории. СПб: Наука, 2004.

[36] Цыганков П.А. Эволюция классических парадигм в западной теории международных отношений // Общественные науки и современность, 2004. № 2. С.119-130.

[37] Петровский В.Ф. Американская внешнеполитическая мысль. Критический обзор организации, методов и содержания буржуазных исследований в США по вопросам международных отношений и внешней политики. М.: «Международные отношения», 1976.

[38] Ланцов С.А., Усмонов Ф.И. Проблемы безопасности в теории международных отношений: сравнительный анализ основных направлений [Электронный ресурс] // Журнал ПОЛИТЭКС, 2008. Т.4.№2.С.151-163. URL: https://cyberleninka.ru/article/n/problemy-bezopasnosti-v-teorii-mezhdunarodnyh-otnosheniy-sravnitelnyy-analiz-osnovnyh-napravleniy/viewer (дата обращения 04.02.2020).

[39] Сетов Н.Р. Политический реализм: теория и метод. М.: Издательство Московского университета, 2013. С. 15.

[40] Клаузевиц К. «О войне». М.: АСТ, 2019. С. 27.

актуальными в наши дни стали методологические подходы, интерпретирующие невоенные, смысловые «акты насилия»[41].

В качестве общей теоретико-методологической базы исследования используется системный подход Т. Парсонса[42], Н. Лумана[43] и др., согласно которому международная безопасность представляет собой систему отношений, характеризующуюся целостностью и взаимозависимостью самого широкого круга субъектов и акторов международной обстановки. Теоретико-методологические принципы данного подхода в своей основе были разработаны такими исследователями МГИМО МИД СССР И МИД России как М.А. Хрусталев[44], А.С. Злобин, А.Д. Богатуров[45], Т.А. Шаклеина[46], М.М. Лебедева[47], Т.А. Алексеева[48], А.И. Подберёзкин[49], К.П. Боришполец[50], а также сотрудниками центра Военно-политических исследований МГИМО МИД России – Корпорации ВКО «Алмаз-Антей», в некоторых из которых принимал участие и автор.

Понимание новых реалий международной безопасности будет базироваться на методологии, предлагаемой представителями направления теории международных отношений, согласно которому значимыми акторами безопасности являются не только государства, но и негосударственные акторы. Подобного подхода придерживаются такие авторы как Д. Най[51], В.М. Кулагин[52] и ряд других.

---

[41] Кравченко С.А. Спираль усложнения насилия: востребованность гуманистической политики // Политические исследования, 2019. № 5. С. 43-55.

[42] Парсонс Т. Система современных обществ. М.: Аспект Пресс, 1998.

[43] Луман Н. Социальные системы. СПб.: Наука, 2007.

[44] Хрусталев М.А. Методология прикладного политического анализа. М.: Проспект, 2010.

[45] Богатуров А.Д., Хрусталев М.А., Косолапов Н.А. Очерки теории и политического анализа международных отношений. М.: НОФМО, 2002.

[46] Шаклеина Т.А. Россия и США в мировой политике. М.: АСПЕКТ ПРЕСС, 2012.

[47] Лебедева М.М. Мировая политика. Учебник для бакалавров. М.: Кнорус, 2013.

[48] Алексеева Т.А. Современные политические теории. М.: РОССПЭН, 2000.

[49] Некоторые аспекты анализа военно-политической обстановки: монография / под ред. А.И. Подберёзкина. М.: МГИМО-Университет, 2014.

[50] Боришполец К.П. Методы политических исследований: Учебное пособие для студентов вузов. 2-е изд. испр. и доп. М.: Аспект Пресс, 2010.

[51] Nye J.S. The future of power // Public Affairs, 2011.

[52] Кулагин В. Глобальная или мировая безопасность // Международные процессы. 2007. Т. 5. № 2. С. 38-51.

Источниковедческая база исследования. В качестве источников исследования автор рассматривает сетевые интернет-ресурсы, в частности и прежде всего «Фейсбук», «Твиттер», документы и публикации в отечественных и иностранных СМИ, публичные выступления политиков и высших должностных лиц, а также многочисленные исследовательские работы, приведенные в списке литературы.

Цель исследования: проанализировать сложную природу власти социальных сетей, её влияние на характер международной и национальной безопасности. Для достижения цели исследования поставлены следующие **задачи**:

– охарактеризовать влияние современной информационной революции на становление сложных социальных сетей;

– исследовать современные социальные сети и другие Веб 2.0 технологии, выделить их наиболее значимые факторы проявления власти;

– определить влияние социальных сетей и Веб 2.0 технологий на международную и национальную безопасность. «исследовать современные социальные сети и другие Веб 2.0 технологии, выделить их наиболее значимые факторы проявления власти».

Область исследования соответствует пункту 1 «Политическая власть как основной предмет политической социологии. Методы, функции, формы проявления политической власти в системе общественных отношений. Политическое сознание и поведение социальных групп, общностей, классов, организаций, индивидов. Взаимосвязь и взаимовлияние политической и социальной сфер общественной жизнедеятельности. Соотношение и пересечение научных интересов и понятийных аппаратов политической социологии, социологии и политологии» паспорта специальности ВАК 22.00.05 «Политическая социология».

Объектом исследования являются социальные сети, рассматриваемые как инструмент политической власти.

Предметом исследования является влияние социальных сетей на международные отношения и международную безопасность в контексте изучения новых вызовов национальной безопасности России.

Практическая значимость работы. Изучение влияния политической власти социальных сетей на международную и национальную безопасность характеризуется практической значимостью, когда полученные знания могут быть использованы Российской Федерацией при выработке государственной информационной политики, в том числе в области регулирования интернета, а также при выработке внешнеполитической позиции на международных переговорах по обеспечению информационной безопасности на площадке ООН и в рамках других международных структур. Эта тенденция проявилась в полной мере в первом десятилетии нашего века, но не находила долгое время соответствующего внимания среди исследователей-международников, хотя именно в XXI веке можно говорить о появлении феномена в международных отношениях – политики «новой публичной дипломатии»[53].

Научная новизна результатов диссертационного исследования.

1) Выявлена природа современного цифрового пространства, раскрыта его сложная дифференциация, амбивалентность его функций;

2) обоснована усложняющаяся природа политической власти, обусловленная качествами киберпространства;

3) показана взаимосвязь кибервласти с конкретными кибератаками, нацеленных на обретение реальных капиталов, что производит новые сложные риски рукотворного типа;

4) обосновано воздействие кибервласти на характер международных отношений вообще и национальную безопасность в особенности, а также взаимосвязь кибервласти с «цифровой дипломатией»;

5) раскрыто влияние кибервласти на процесс усложнения природы современного насилия;

---

[53] Публичная дипломатия: теория и практика / под ред. М.М. Лебедевой. М.: Аспект Пресс, 2018. С. 36-54.

6) исследовано воздействие социальных сетей на «драматизацию сознания» (М. Кастельс), показаны новейшие манипулятивные приемы, деформирующие мировосприятие людей;

7) конкретно проанализированы травмы сознания, проявляющиеся в разрывах ценностей и норм, усвоенных в процессе социализации, которые выражаются как новая форма политического насилия, несущая вызовы национальной безопасности.

Основные положения, выносимые на защиту.

1) Нами дана характеристика современному цифровому киберпространству, квинтэссенция которого видится в следующем. Цифровое киберпространство доступно далеко не в равной мере для всех стран, раскрыта суть его дифференциации: мировые цифровые гиганты США и Китая влияют на характер международных отношений и на международную безопасность, препятствуя появлению на этом поле новых политико-цифровых акторов. По нашему убеждению, в целях укрепления национальной безопасности, России необходимо создать свое собственное цифровое облако. Благодаря гетерархической природе сетевой, ацентричной организации, киберпространство представляет собой своеобразную ризому, будучи внеструктурным и нелинейным способом формирования целостности в виде совокупности самых разнородных смыслов. В нем отсутствует единый центр, но есть множество кластеров тесных («сильных») связей различных акторов и множество удаленных («слабых») связей с другими кластерами, все вместе образующими единую глобальную сеть. Киберпространство может постоянно копироваться, множиться и воспроизводиться благодаря каскадам бифуркаций, что в целом характерно для нелинейно развивающегося социума. Последствия функционирования киберпространства, сочетающего человеческое агенство и актанты, амбивалентны. С одной стороны, оно создает множество возможностей для быстрого доступа к общественным благам, открывает новые пути и средства для всех людей участвовать в гражданском обществе, но, с другой стороны,

это также создает уникальные возможности для самых различных акторов использовать киберпространство для развертывания мощных средств– актантов стратегического действия, ведения военных операций.

2) Обосновано, что благодаря киберпространству усложняется природа политической власти, ныне функционирующей в детерриторизированном пространстве и во «вневременном времени». По своей природе политическая власть в киберпространстве отличается от «классической» власти, предполагающей, навязывание воли посредством права, авторитета или традиций (М. Вебер) или способность класса, владеющими основными средствами производства, осуществлять социально-политическое господство (К. Маркс). Ныне “собственники средств определения” смыслов (У. Бек) фактически владеют весьма значительным ресурсом политической властью, что позволяет им выражать свои интересы. Сформировалась кибервласть, представляющая собой сложную систему ресурсов, структурированных вокруг производства и обмена цифровой информации, а также контроля над ней. Её сложность, в частности, проявляется в том, ресурсы оказывают нелинейное действие: сравнительно небольшие факторы (искусственно произведенные симулякры и фейки) могут быть весьма значимыми по своим воздействиям на социум. Вместе с тем, кибервласть за счет создания цифровых облаков постепенно трансформируется во властную гегемонию, т.е. супервласть, которая не ограничивается контролем над сугубо кибернетическими ресурсами, вбирает в себя человеческие, финансовые, экономические, символические, культурные и политические ресурсы, создаваемые или задействованные в этой системе. 3) Кибервласть позволяет осуществлять кибератаки, нацеленные на конвертацию виртуальных смыслов в реальные капиталы – экономического, политического, культурного, социально-психологического, военного характера. Кибервласть функционирует в цифровом поле борьбы, в котором киберакторы, от индивидов до государств, конкурируют за капитализацию своего места в данном поле (П. Бурдье). Кибервласть производит новые сложные риски,

ведущие к дерегуляции международного порядка. Кроме того, кибервласть как сложная система способна к саморефлексии, что потенциально производит разнообразные ненамеренные последствия для функционирования миропорядка.

4) Показаны и раскрыты две тенденции в области современных международных отношений: смещение суверенитета и власти государств в область киберпространства и нарастающая зависимость их от цифровых технологий, а также диффузия кибервласти между государственными и негосударственными акторами, что вместе создает вызовы национальной безопасности. Национальная безопасность в современных условиях во все большей степени определяется информационно-цифровыми ресурсами кибервласти. Страны, которые достигнут технологического и политического превосходства в киберпространстве, будут претендовать на мировое господство. Битва за кибервласть между державами будет важнейшей характеристикой ближайших лет развития международных отношений. Эти вызовы призвана минимизировать «цифровая дипломатия», подразумевающая весьма широкий набор управленческих задач – и традиционных, и новых, но решаемых с помощью киберинструментов в режиме онлайн. В ситуации борьбы за кибервласть цифровая дипломатия включает в себя элементы кибердавления, т.е. стремится к неявному противостоянию с противником с целью создания благоприятных условий для реализации реальных политических действий в своих интересах.

5) Изменилась эффективность использования тех или иных инструментов насилия – они становятся информационно-цифровыми и надзорно-цифровыми. Для победы в настоящее время необходимо с помощью «игры» кодами сигнификациии принудить правящую элиту противника принять систему ценностей, интересов и норм, что возможно сделать не только с помощью военной силы, но, прежде всего, с помощью невоенных инструментов силовой политики – информационно-когнитивных

средств, цифрового надзора, манипулирования общественного сознания с помощью симулякров и симуляций.

6) Исследование социальных сетей выявило то, что они стали мощным инструментом для сознательной политики дезинформации, фейков, искажающих реальности, которые могут менять достаточно быстро и в глобальном масштабе информационно-когнитивный фон в странах и регионах. Благодаря сетям возникли новые формы манипулирования общественным сознанием, которые используются для формирования политической напряженности, дезинформация граждан о работе органов государственного управления. Это приводит к провоцированию столкновений религиозного, социально-политического и национального характера, подрыву авторитета власти, нанесению ущерба жизненно важным интересам государства в разных областях. Показано, что в социальных сетях осуществляется «драматизация сознания» и манипуляция им с помощью симулякров и фейков, представленных в виде тех или иных «гуманистических» и «планетарных ценностей».

7) Исходя из того, что «общество травмы» стало современной реальностью (Ж.Т. Тощенко), в развитии этой проблематики нами проанализированы травмы сознания, проявляющиеся в разрывах ценностей и норм, усвоенных в процессе социализации, которые выражаются как новая форма политического насилия, несущая вызовы национальной безопасности. Такие формы новейших манипуляций сознанием как троллинг в социальных сетях, астротурфинг, сокпаппетинг обладают возможностями для форматирования общественного мнения к будущим политическим и идеологическим акциям путем нанесения с помощью кодов сигнификаций травм исторической памяти, создания второго «негативного тела» политического деятеля, перформансов с заданным провокационным смыслом.

Апробация результатов исследования. Основные положения диссертационного исследования были изложены в аналитических работах

Центра военно-политических исследований МГИМО с 2014 по настоящее время, подготовленных по заказу Министерства иностранных дел РФ, Концерна ВКО «Алмаз-Антей», РГНФ и Минобороны, получивших положительную оценку:

– «Долгосрочное прогнозирование развития отношений между локальными человеческими цивилизациями в Евразии» (проект РГНФ № 15-37-14016);

– «Динамика мирового рынка торговли продукцией военного назначения, мониторинг международного и российского законодательства в области осуществления внешнеторговой деятельности в отношении продукции военного назначения» – заказчик ВКО «Алмаз-Антей»;

Кроме того, автор участвовал в аналитических работах Центра, которые были опубликованы:

– «Информационно-аналитическая система стратегического планирования противодействия угрозам национальной безопасности»;

– «Долгосрочные сценарии развития стратегической обстановки, войн и военных конфликтов в XXI веке»;

– «Долгосрочное прогнозирование развития международных отношений»;

– «Военно-политические аспекты прогнозирования мирового развития»;

– «Долгосрочное прогнозирование сценариев развития военно-политической обстановки».

– «Стратегическое сдерживание: новый тренд и выбор российской политики: монография / А.И. Подберёзкин, М.В. Александров, К.П. Боришполец и др.. – М.: МГИМО-Университет, 2019. – 649 с.

Основные положения диссертационной работы были опубликованы в изданиях, рекомендованных ВАК при Минобрнауки РФ:

– Подберёзкин А.И., Жуков А.В. Публичная дипломатия в силовом противостоянии цивилизаций // Вестник МГИМО-Университета. – 2015. – № 6(45). – С. 106-116.

– Подберёзкин А.И., Жуков А.В. Стратегия «силового принуждения» в условиях сохранения стагнации в России // Обозреватель - Observer. – 2018. – № 4. – С. 22-34.

– Подберёзкин А.И., Жуков А.В. Факторы безопасности для российской нации, государства и общества. Угрозы силового использования социальных сетей // Обозреватель - Observer. – 2017. – № 9 (332). – С. 23-40.

– Подберёзкин А.И., Жуков А.В. Оборона России и стратегическое сдерживание средств и способов стратегического нападения вероятного противника // Вестник МГИМО-Университета. – 2018. – № 63(6). – С. 141-158.

– Жуков А.В. Институты развития человеческого капитала России и политика «силового принуждения» // Обозреватель – Observer. – 2020. – № 4 (363). – С. 27-44.

– Жуков А.В. Киберпространство как сфера международных отношений и национальной безопасности // Научное обозрение. Серия 2. Гуманитарные науки. – 2020. – № 3-4. – С. 60-68.

– Жуков А.В. Социальные сети как фактор стратегической безопасности // Научное обозрение. Серия 2. Гуманитарные науки. – 2020. – № 5. – С. 23-31.

Одна из работ опубликована в издании, входящем в Скопус: Подберезкин А.И., Жуков А.В. Травматизация сознания как новая форма политического насилия: Рецензия на книгу члена-корреспондента РАН Ж.Т. Тощенко «Общество травмы: между эволюцией и революцией (опыт теоретического и эмпирического анализа)» // Вестник Российского университета дружбы народов. Серия: социология, 2020. № 2 (в печати).

ГЛАВА 1. МЕЖДУНАРОДНЫЕ ОТНОШЕНИЯ В КИБЕРПРОСТРАНСТВЕ: СТРАТЕГИЧЕСКИЙ КОНТЕКСТ

1.1. Киберпространство как сфера международных отношений и национальной безопасности

Понятие «киберпространства» прошло долгий путь концептуализации с момента своего появления в научно-фантастической литературе в начале 1980-х годов[54]. После создания Т. Бернесом-Ли «Всемирной сети» (World Wide Web) в начале 1990-х гг. в течение трех последующих десятилетий оно стало активно использоваться для обозначения виртуального пространства институциональной структуры общества. В то же время киберпространство не следует путать с самим Интернетом, по определению М. Кастельса, «кибер-гетто»,[55] или Всемирной паутиной (WWW). Если Интернет представляет собой инфраструктуру технического и программного обеспечения, т.е. глобальную сеть компьютеров, использующих особые протоколы для коммуникации друг с другом, а WWW есть система взаимосвязанных гипертекстовых документов, которые доступны через Интернет, то киберпространство представляет собой *метафору места* «соседствующих пространств» (М. Кастельс), которые, как считает Дж. Урри, становятся перманентно «*движущимися местами*». Ибо места «подобно кораблям движутся туда - сюда и не фиксированы внутри одного расположения. Места путешествуют, медленно или быстро, на более длинные или короткие расстояния внутри человеческих или нечеловеческих сетей»[56]. Это принципиально новая реальность весьма важна для осуществления коммуникативных социальных практик между политическими акторами. Метафора признает возможность разных смыслов,

[54] Gibson W. Burning Chrome // Omni, 1982. No. 46. P. 72-107.

[55] Castells M. The Internet Galaxy: Reflexions on the Internet, Business, and Society. Oxford: Oxford University Press, 2002.

[56] Urry J. Mobilities. Cambridge: Polity Press, 2008. P. 42.

позволяет раскрыть игру истины, характерную для научного знания о современном обществе[57], которая широко используется в трудах З. Баумана, У. Бека, Э. Гидденса. В смысле коммуникативного места киберпространство не так ново, ибо оно появляется задолго до компьютеров и Интернета. На сегодняшний день, оно функционирует как *интерфейс* на стыке таких информационно-коммуникативных технологий как телефония, телевидение, компьютерная техника, передача данных web 1.0, web 2.0. Другими словами, хотя «киберпространство» как термин существует лишь с 1982 г., когда У. Гибсон придумал его в рассказе «Сжигание Хром», само это явление как область машинно-опосредованной коммуникации людей возникает вместе с первыми телефонными аппаратами почти 150 лет назад. Но именно благодаря общему киберпространству современное общество постепенно на протяжении XX века становится *специфически сетевым*[58] *и цифровым*[59], т.е. таким, где отношения в машинно-опосредованных социальных и медиасетях дополняют или заменяют коммуникации, основанные на взаимодействии политических акторов лицом к лицу. Хотя сами социальные сети как структурная форма существовали в истории человечества на всем его протяжении (например, христианские ордена), в нынешнюю эпоху сетевой принцип организации общества становится ключевым благодаря развитию *цифровизации* киберпространства. Как замечает по этому поводу М. Кастельс, сетевое общество – «это не просто общество на основе социальных сетей…это общество, где ключевые социальные структуры и деятельность его членов организованы вокруг сетей электронных коммуникаций»[60]. Современное *дигитализированное* киберпространство представляет собой «постчеловеческую рациональность», которая становится предметом

[57] Метафора // Постмодернизм. Энциклопедия. Мн.: Интерпрессервис; Книжный дом, 2001. С. 464-469.

[58] Castells M. The Rise of the Network Society. Oxford: Wiley-Blackwell, 2010.

[59] Mosco V. Becoming Digital. Toward a Post-Internet Society. Bingley: Emerald Publishing Limited, 2017; Vanderburg W.H. Our War on Ourselves. Toronto: University of Toronto Press, 2011; Vanderburg W.H. Our Battle for the Human Spirit. Toronto: University of Toronto Press, 2016.

[60] Kreisler H. Identity and Change in the Network Society. Conversation with Manuel Castells // Conversations with History, Institute of International Studies, UC Berkeley, 08.05.2001 [online]. URL: http://globetrotter.berkeley.edu/people/Castells/castells-con4.html (дата обращения 15.05.2019).

социологических исследований[61]. Киберпространство в сравнении с другими пространствами человеческой деятельности обладает, таким образом, следующими чертами:

1) Современное киберпространство не может существовать без возможности использования естественного электромагнитного спектра. Без него не только терабайты цифровых данных не смогут появляться, передаваться и накапливаться, но и сами ИКТ (расшифровать один раз) уже не смогут функционировать, т.к. аналоговые средства коммуникации почти ушли в прошлое. Интегральные схемы и другие микроэлектронные устройства напрямую зависят от работы электронов. Волоконно-оптические кабели нужны только для того, чтобы распространять свет между соединенными узлами. Сети ИКТ также зависят от эффективности использования электромагнитного спектра, ибо их развитие идет через пространство радиочастот и микроволн.

2) Киберпространство является сложным искусственным ареалом. Это делает киберпространство уникальным по сравнению с наземным, морским, воздушным и космическим ареалами. Без интегральных плат, полупроводников, микросхем, оптоволокна, антенн и других ИКТ не было бы киберпространства, способного распространять электромагнитные волны. Космос существовал бы, даже если бы человечество не смогло разместить спутники на околоземной орбите; море существовало бы, если бы люди не смогли строить корабли и точно так же воздушное пространство существует независимо то того, научились бы люди летать или нет. Киберпространство же не существовало бы, если не способность людей изобретать и производить технологии, позволяющие использовать различные свойства электромагнитные спектра.

3) Киберпространство может постоянно копироваться, множиться и воспроизводиться благодаря каскадам бифуркаций, что характерно для

[61] Braidotti R. The Posthuman. Cambridge: Polity Press, 2015. P. 73.

нелинейно развивающегося социума. В физическом пространстве есть только один воздух, одна вода, одна земля и один космос. В отличие от этого, киберпространств как множества виртуальных, нефизических мест можно сгенерировать сколько угодно. Это означает, что демаркация или уничтожение киберпространства в самом киберпространстве невозможно. Ценность всех производимых и обмениваемых киберресурсов определяется только извне как их полезность в достижении тех или иных реальных социальных целей. Поэтому кибератаки и киберпреступления осуществляются только ради конвертации виртуальных смыслов в реальные капиталы – экономического, политического, культурного, социально-психологического, военного характера. Инструментальная и при этом высокоэффективная природа киберпространства делает почти безрезультатными попытки ограничения виртуальной активности. Любые сайты и сети могут быть всегда восстановлены или отремонтированы благодаря относительно недорогому и легкодоступному оборудованию и программному обеспечению, чтобы продолжать свою деятельность по капитализации социальных ресурсов.

4) Киберпространство предполагает свободу и анонимность. Оно предоставляет возможности скрывать личность и местоположение участников из-за его физической архитектуры и программных протоколов, которые позволяют относительно легко использовать псевдонимы и прокси-серверы, которые довольно трудно раскрыть. Именно поэтому охота за личными данными является крупнейшей областью незаконных операций и сферой деятельности специальных служб многих стран.

5) Киберпространство радикально увеличивает скорость, объем и дальность связи не только государств и корпораций, но и отдельных граждан, которые могут использовать его для глобального, почти мгновенного общения, используя разнообразные информационные средства от текста до видео. Хотя киберпространство *распределено неравномерно* – от вездесущности в развитых странах до полного отсутствия в других местах –

доступ к нему во всем мире постоянно расширяется, в том числе в самых бедных регионах, где сектор телекоммуникаций, как правило, является одним из наиболее быстро растущих секторов экономики. Темпы такого распространения также определяются демократичностью самих цифровых технологий, что является еще одной их важной чертой.

6) Барьеры для входа в киберпространство, какими бы они ни были, еще больше снижаются в связи с распространением недорогих устройств с возможностью подключения к Интернету, которые сочетают в себе функции голосовой связи, просмотра и размещения веб-контента, а также возможности фотографирования и видеосъемки.

7) Благодаря *гетерархической* природе сетевой организации структурно киберпространство представляет собой *ризому* – метафорическое обозначение, предложенное Ж. Делезом и Ф. Гваттари, внеструктурного и нелинейного способа организации целостности[62]. В киберпространстве отсутствует единый центр, но есть множество кластеров тесных («сильных») связей различных акторов и множество удаленных («слабых») связей с другими кластерами, все вместе образующими единую глобальную сеть (Рис. 1.).

[62] Deleuze G., Guattari F. A Thousand Plateaus. Minneapolis: University of Minnesota Press, 1987.

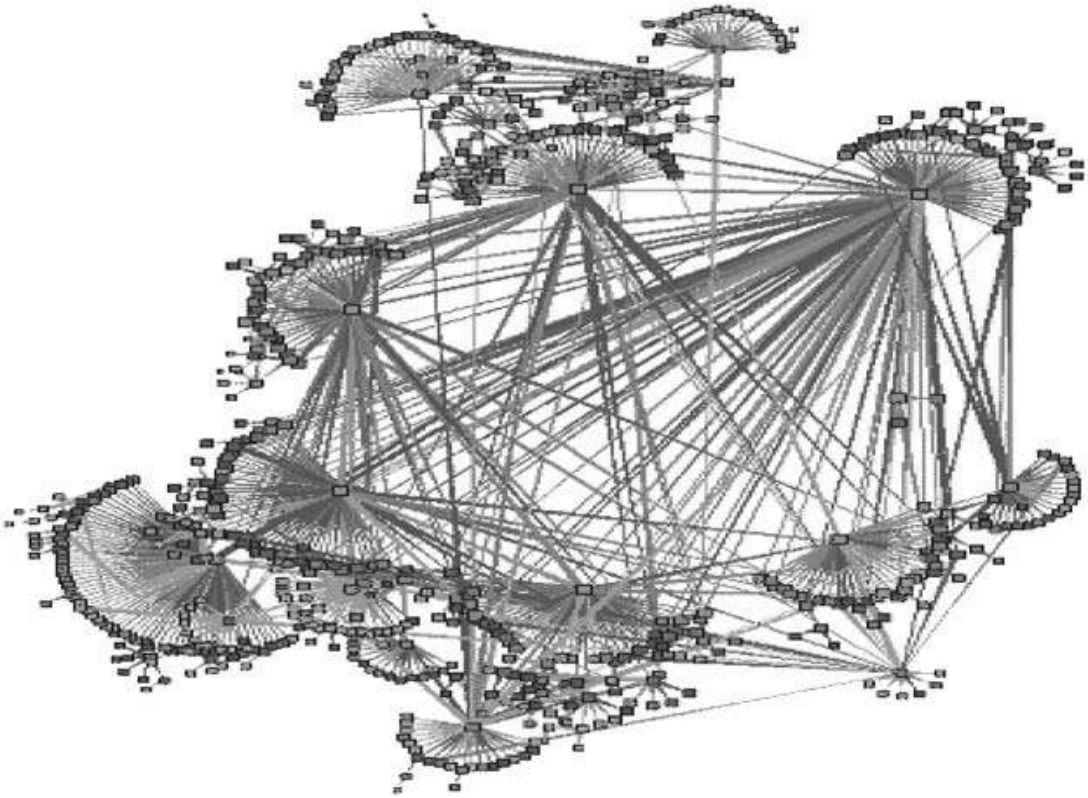


Рис.1. Визуализация киберпространства, образующего структуру сетевого общества

Источник: [Van Dijk J. The Network Society (3 ed.). London: Sage Publications, 2012. P. 32]

Особо подчеркнем *дифференциацию киберпространства, основываясь на факторе его неоднородности*. Сама дифференциация киберпространства способствует не только созданию принципиально новых властных структур, но перераспределению влияния государств в международных отношениях, обретающих возможность с помощью создания цифровых облаков осуществлять доминирование в мире, выступать в качестве силы в политико-экономических и геополитических конфликтах. Сегодня в международном киберпространстве существуют пять наиболее влиятельных цифровых корпораций в мире, которые представляют интересы США: Apple, Google, Microsoft, Amazon, Facebook. Им реально протипостоит только китайская Alibaba. Все они представляют интересы национальных военно-промышленных комплексов. Мировые цифровые гиганты, несомненно, влияют на характер международных отношений и на международную

безопасность. По нашему убеждению, в целях укрепления национальной безопасности, России необходимо создать свое собственное цифровое облако. Значительные усилия в этом направлении ныне предпринимаются. Важнейшим следствием сетевой организации киберпространства следует считать его *ацентричный характер* с точки зрения распределения власти. Как считает Ж. Деррида, ныне появляются структуры, в которых центр и *в* структуре и *вне* ее – «*центр ее в ином месте*. Центр – это не центр»[63]. Во-первых, не существует общепризнанного и общепринятого кибергегемона. Разоблачения Э. Сноудена о существующем потенциале разведывательных органов США осуществлять тотальную слежку за людьми по всему миру не сделали их неуязвимыми от подобных действий со стороны других акторов, о чем свидетельствует доклад спецпрокурора Р. Мюллера о вмешательстве в американские выборы 2016 г.[64] Гегемонический кибермир описывал бы мир, в котором ни одна страна не осмелилась бы начать кибератаки из-за страха возмездия со стороны такого гегемона, который был бы узаконен адаптированным международным правом и, возможно, уполномочен международным органом. Довольно сомнительно на сегодняшний день, что такая кибергегемония будет образована, признана и легитимизирована в ближайшем будущем. Дж. Най утверждает, например, что США остаются лидером в использовании Интернета в военных и социальных целях, но, с другой стороны, большая зависимость от повсеместной цифровизации делает их гораздо более уязвимыми для кибератак, чем какие-либо другие страны, поэтому сама идея доминирования в области киберпространства оказывается «бессмысленной»[65].

Во-вторых, как известно, не существует универсальной организации коллективной безопасности, подобной ООН или ОБСЕ, которая могла бы сбалансировать интересы национальной безопасности в киберпространстве.

---

[63] Дерида Ж. Структура, знак и игра в дискурсе гуманитарных наук. СПб.: Академический проект, 2000. С. 353.

[64] Mueller R. S. III Report On The Investigation Into Russian Interference In The 2016 Presidential Election. Vol. I of II. Washington, D.C., 2019.

[65] Nye J. S. Nuclear Lessons for Cyber Security? // Strategic Studies Quarterly, 2011. Vol. 5(4). P. 20.

Предупреждения о предстоящей гонке кибервооружения датируются уже самым началом 2000-х гг.[66] Однако до сих пор, в области сдерживания наращивания кибервласти мало что сделано. По результатам опроса экспертов в области кибербезопасности, признается, что гонка кибервооружений сегодня находится в самом разгаре[67]. Неспроста поэтому основатель и генеральный директор компании «Лаборатория Касперского» Евгений Касперский еще в 2012 г. призывал к созданию новой специализированной международной организации по кибербезопасности, которая должна была действовать как «независимая глобальная платформа для международного сотрудничества и заключения взаимных обязательств о неприменении кибероружия, а также для создания нормативной базы в области кибербезопасности критически важных инфраструктур»[68].

Таким образом, ацентричное киберпространство, используя терминологию М. Фуко, «говернментализировано» в наиболее ярком и точном смысле этого слова, т.е. смещает традиционную суверенную и дисциплинарную власть на периферию и производит власть «повсюду, но не потому, что она подчиняет себе все вокруг, а потому, что происходит отовсюду… не общество этатизируется, а управление говернментализируется»[69].

Исторически не имеющая аналогов плотная сеть взаимосвязанных компьютеров и людей, таким образом, представляет собой нечто парадоксальное, сочетающее человеческое агенство и актанты, способные проявлять саморефлексию и действовать как «актантные резомы»[70]. С одной

---

[66] Minkwitz O., Schofbanker G. Information warfare: Die Rustungskontrolle steht vor neuen Herausforderungen. Fur eine Informationskriegsordnung: Fruhzeitige Rustungskontrolle statt Rustungswettlauf. FoG: IS Arbeitspapier 2. Berlin: Forschungsgruppe Informationsgesellschaft und Sicherheitspolitik, 2000.

[67] Grauman B. Cyber Security: The Vexed Question of Global Rules. An independent report on cyber-preparedness around the world. Brussels, 2012. [online] URL: https://pdfs.semanticscholar.org/5259/62263586710d90abbb3584236ff835cc5f0f.pdf?_ga=2.152765370.26273978.1588134073-398395631.1585861038 (дата обращения 11.07.2019).

[68] CeBIT 2012: Eugene Kaspersky Calls for International Cyber-security Organisation. 2012, March 9 [online]. URL: http://www.bizcommunity.com/Article/82/391/72039.html (дата обращения 17.07.2019).

[69] Фуко М. Воля к истине: по ту сторону власти, знания и сексуальности. / Пер. с фр. М.: Касталь, 1996. С. 193.

[70] Latour B. The Pasteurization of France. Cambridge, MA: Harvard University Press, 1988.

стороны, она создает множество возможностей для быстрого доступа к общественным благам, открывает новые пути и средства для всех людей участвовать в гражданском обществе, но, с другой стороны, это также создает уникальные возможности для самых различных акторов использовать киберпространство для развертывания мощных средств – актантов стратегического действия, ведения военных операций, от которых очень трудно защититься и, тем более, которые трудно заранее предугадать. Более того, актантны как сложные системы способны к трудно контролируемой рефлексии, что создает предпосылки для возможных «нормальных аварий»[71]. Именно поэтому в современной военной науке киберпространство считается *пятой* важнейшей сферой политического противоборства наравне с сушей, морем, воздушным пространством и космосом [72].

Доступность, безграничность и ацентричность киберпространства делают проблему кибербезопасности на институциональном и национальном уровнях одной из центральных для государств в XXI веке. Происходит последовательная «киберизация» международных отношений, которая определяется как глубокое проникновение во все сферы международных отношений различных кибер-медиумов (событий, процессов, происходящих в киберпространстве), с одной стороны, и растущая зависимость действующих лиц в сфере МО от инфраструктуры, инструментов и средств, предлагаемых киберпространством, с другой стороны[73]. В то же время, необходимо подчеркнуть, что киберизация носит характер *риск-киберизации* международного порядка, поскольку именно в киберпространстве на сегодняшний день зарождаются и проявляются самые неконтролируемые, рукотворные риски с разнообразными ненамеренными последствиями,

[71] Perrow Ch. Normal Accidents: Living with High Risk Technologies. New Brunswick, NJ: Rutgers University Press, 1999.

[72] Rowland J., Rice M., Shenoi S. Whither Cyberpower? // International Journal of Critical Infrastructure Protection. 2014. Vol. 7 (2). P. 124-137. URL: http://dx.doi.org/10.1016/j.ijcip.2014.04.001 (дата обращения 13.04.2020).

[73] Kremer J.-F., Muller B. Cyberspace and International Relations: Theory, Prospects and Challenges. Heidelberg: Springer, 2014.

угрожающими международному порядку. «Мировое общество риска», используя терминологию У. Бека[74], возникает и разрастается прежде всего в киберпространстве, захватывая все больше людей и институциональных сфер в свою зону фундаментальной уязвимости, обусловленной характером новых рисков: они – 1) «делокализированы» (их причины и последствия не ограничены одним пространством); 2) «неисчисляемы» (ибо «включают “гипотетические” риски); 3) «не поддаются компенсациям»[75]. После известной атаки вируса Stuxnet на иранские ядерные центрифуги в 2010 г. на одной из вскоре последовавших конференций по кибербезопасности ведущий эксперт компании Symantec провел эксперимент, разъясняющий опасность киберугрозы. Он установил на сцене воздушный насос, работающий под управлением операционной системы производства Siemens, инфицировал контролирующую насос рабочую станцию тем же вирусом Stuxnet и запустил процесс в действие. Насос быстро надул воздушный шар, но процесс не остановился – шар надувался до тех пор, пока не лопнул. «Представьте, что это не воздушный шар, а иранская атомная электростанция», – сказал эксперт, поставив точку в вопросе о «серьезности» кибервойн[76]. Незадолго до этого целые государства впервые подверглись массовым кибератакам – на Эстонию (в 2007 г., после демонтажа «Бронзового солдата») и на Грузию (в 2008 г., во время войны с Россией). Поэтому, как указывает Е.С. Зиновьева, «Интернет как глобальная сеть, не знающая границ, вступает в противоречие с существующей Вестфальской политической системой мира»[77]. Политическая сфера и киберсфера находятся в состоянии конфликта. По мнению Г. Киссинжера, само существование государственной власти и суверенитета оказывается под угрозой. При этом «сложность ситуации усугубляется тем, что легче

[74] Beck U. World at Risk. Cambridge: Polity Press, 2010.

[75] Beck U. World at Risk. P. 52.

[76] Stuxnet: война 2.0 [Электронный ресурс] // Habr. 2010, 12 октября. URL: https://habr.com/ru/post/105964/ (дата обращения 18.08.2019).

[77] Зиновьева Е.С. «Цифровой Вестфаль»? [Электронный ресурс] // Эксперты МГИМО. 2013, 26 марта. URL: http://mgimo.ru/news/experts/document236588.phtml (дата обращения 03.04.2018).

предпринимать кибератаки, чем защищаться от них, и это, похоже, стимулирует уклон в сторону развития наступательных информационных технологий»[78]. При этом опасность подкрепляется важными обстоятельствами подобных киберрисков: анонимностью, невозможностью окончательного определения виновных и ответственных за кибератаки, а значит невозможностью юридически доказанного наказания, а также «отсутствием международных соглашений, для которых, вдобавок, даже если они подписаны, отсутствует система правоприменения»[79].

В этом смысле, несмотря на то, что киберпространство создает более плоскую, сетевую онтологию социальных коммуникаций, государства и их суверенитет не могут быть просто ликвидированы нашествием других кибератакторов, ибо до сих пор именно государства являлись основой международного права и международных отношений. Процесс учреждения «цифрового Вестфаля» далек от своего завершения и может занять, по экспертным оценкам, еще около 20 лет. Однако, диффузный период (в политическом и правовом смысле) развития киберпространства будет рано или поздно завершен. Это произойдет, когда будут определены характеристики национальных юрисдикций в киберпространстве в общепринятых нормативных терминах. И, в конце концов, как это всегда происходило раньше, международная система институционализирует кодекс прав и обязанностей всех кибератакторов, сделав одних победителями, а других проигравшими в схватке за новые ресурсы. На вершине новой киберсистемы международных отношений опять окажутся государства, но только те из них, кто будет считаться безопасными кибердержавами, они будут доминировать в наступающей эпохе социокиберэкономического мира. Поэтому в течение нынешнего переходного периода также должны быть приняты решения, которые позволят установить то, что признано «ответственным» киберповедением, что представляет собой «кибервласть» с

[78] Киссинджер Г. Мировой порядок. М.: АСТ, 2015. С. 448.
[79] Там же.

точки зрения институционализированных возможностей отдельных государств и каковы могут быть международные санкции за участие в кибервойнах. Но пока мы живем в период переходных конфликтов, когда страны борются за контроль над ресурсами, образованными на границе нового киберфронтира.

Таким образом, сегодня мы можем наблюдать две тенденции в области современных международных отношений: смещение суверенитета и власти государств в область киберпространства и нарастающая зависимость их от цифровых технологий, а также диффузия кибервласти между государственными и негосударственными акторами, что вместе ведет к размыванию и ослаблению национальной безопасности как таковой.

Традиционно считалось, что национальная безопасность государства зависит от таких факторов, как география, природные ресурсы, численность населения, поскольку они рассматривались как составные элементы, необходимые для создания военной мощи. Способность нации защищать свои собственные границы от нападений рассматривалась как главный символ национального могущества. Появление же киберпространства и реалий *кибервласти* требуют новых оценок того, как стратегическое влияние способно обеспечить национальную безопасность.

Поскольку киберпространство не имеет физических границ, возникают лакуны в понимании того, что считать территорией государства и как его защищать. Имеющиеся представления о том, что национальное киберпространство образовано из сети компьютеров и их программного обеспечения нельзя считать адекватным. Требуются новые способы определения власти в киберпространстве для эффективной защиты национальных интересов, в том числе для того, чтобы влиять на формирование поведения других киберакторов.

Прежде всего необходимо выделить структурные уровни, в рамках которых кибервласть может быть реализована, диагностирована и измерена.

На основе классификации Дж. Шелдона[80] предлагается различать четыре уровня киберпространства, которые могут иметь собственные индикаторы эмпирической диагностик:

1) Уровень инфраструктуры: физические аспекты киберпространства, которое включает в себя компьютерное оборудование, серверы, сетевые компоненты, кабели, спутники и другие специальные средства. Сюда также входят те устройства, с которыми взаимодействуют пользователи, такие как ПК, ноутбуки, планшеты и смартфоны. Этот уровень может быть измерен долей населения, имеющего доступ к Интернету, средним промежутком времени между обновлениями пользовательского оборудования, количеством интернет-провайдеров на долю населения и количества международных шлюзов, обеспечивающих глобальную связь.

2) Физический уровень: свойства киберпространства, которые ограничены физическими законами и включают контроллеры, связанные с передачей данных через инфраструктурный уровень. К ним относятся характеристики электромагнитного потока, такие как скорость прохождения фотонов в волоконно-оптических кабелях, состояние проводки, развитие беспроводной связи до международных спутниковых каналов. Индикаторы этого уровня могут включать долю населения, обслуживаемой медным кабелем, по сравнению с доступом к высокоскоростной волоконно-оптической связи, количество точек доступа Wi-Fi на душу населения, охват мобильной телефонной связью, среднее потребление данных на одного абонента и стоимость доступа по сравнению со средней зарплатой по стране.

3) Синтаксический уровень: способ форматирования и сжатия данных для обеспечения требуемого уровня коммуникации между различными компонентами интернет-инфраструктуры. Это включает в себя протоколы связи, программные компоненты и алгоритмы сетевой маршрутизации. Эмпирические показатели здесь могут включать в себя

[80] Sheldon J. Deciphering Cyberpower // Strategic Studies Quarterly. 2011. Summer. P.95-112.

качество шифрования данных, передаваемых между абонентами, долю компьютеров, защищенных антивирусом, и, наоборот, уровень распространенности зараженных компьютеров (например, ботнетов), степень приоритизации траффика (т.н. сетевой нейтралитет), а также количество зарегистрированных национальных доменных имен.

4) Семантический уровень: этот компонент показывает, как создается и используется информация в Интернете, чтобы привлекать к ней внимание пользователей. Сюда входят тип и популярность пользовательских интерфейсов, применяемое программное обеспечение, а также лингвистические, культурные и человеческие факторы, использованные при их разработке. Релевантные этому уровню киберпространства индексы измерения включают долю валового внутреннего продукта в онлайн-бизнесе, процент веб-страниц, созданных на языке коренного населения, процент населения, являющегося активным пользователем социальных сетей, уровень киберпреступности (кража данных, мошенничество и т.п.), а также развитость и эффективность законодательства и его правоприменения в области киберрегулирования.

Таким образом, киберпространство можно описать с точки зрения управления его уровнями, при этом власть на одном из них не предполагает власти на другом. Возможность количественного измерения диапазона отмеченных нами переменных на всех уровнях может быть использована для оценки «силы» государства и его суверенитета в киберпространстве. Это также позволяет рассчитать соотношение сил в ситуации экономической конкуренции или военного конфликта. В терминах теории поля П. Бурдье[81] киберпространство следует оценивать, прежде всего, как поле борьбы кибераторов, от индивидов до государств, за капитализацию всех уровней своего участия в его структуре, т.к. это повышает их возможности и ресурсообеспеченность, однако, парадокс заключается в том, что чем выше

[81] Бурдье П. Социальное пространство: поля и практики. М.: Институт экспериментальной социологии; СПб.: Алетейя, 2007; Бурдье П. Социология социального пространства. М.: Институт экспериментальной социологии; СПб.: Алетейя, 2007.

уровень капитализации в киберпространстве (по обозначенным выше полям), тем выше уязвимость от опасностей и рисков, увеличивающих вероятность небезопасности собственного положения. Этот эффект следует обозначить как парадокс риска Н. Лумана, который, представляется, применим к пониманию природы риска киберкапитализации. Социолог еще в конце 1980-х гг. выявил эффект, связанный с тем, что в современном обществе уже нет поведения, свободного от риска, и любые попытки уменьшить риск сами являются рискованными[82]. Для дихотомии риск/безопасность, это означает, что нет абсолютной надежности или безопасности, тогда как из дихотомии риск/опасность вытекает, что нельзя избежать риска, принимая какие-либо решения. В киберпространстве парадокс риска Н. Лумана показывает, как повышение капитала на одном уровне сопровождается увеличением рисков и опасностей на тех же или других уровнях киберструктуры, тем самым делая невозможным достижение зоны абсолютной безопасности. Например, чем больше населения подключено к Интернету (инфраструктурный уровень), тем больше устройств подвергается хакерским атакам (синтаксический уровень). Чем больше развит синтаксический уровень, тем больше рисков снижения качества распространяемой информации, цензурирования, приоритизации трафика (несоблюдения сетевого нейтралитета), троллинга и т.п. (семантический уровень).

Количество и качество кибератак по мере прогресса технологий защиты данных не уменьшаются, а только растут[83]. Для нанесения информационного вреда используются те же самые технологии, которые изначально создавались для киберзащиты. Например, с одной стороны, шифрование трафика помогает усилить защиту пользователей, но, с другой, рост объемов как легитимного, так и вредоносного шифрования лишь умножает проблемы для защищающихся в процессе выявления потенциальных угроз и мониторинга их активности. В итоге, защищаться

[82] Луман Н. Риск и опасность // Отечественные записки. 2013. № 2(53). С. 19-51.

[83] Cisco 2018 Annual Cybersecurity Report. Cisco Systems Inc., 2018; Кибербезопасноть 2016–2017: от итогов к прогнозам. М.: Positive Technologies, 2016.

становится все сложнее, а уязвимости становятся все более разнообразными. Фиксируется стремительный рост вредоносного программного обеспечения самого высокого качества за последние годы. Например, на Рис. 2. показан 11-кратный рост киберугроз только с января 2016 по октябрь 2017 г., обнаруженный специалистами компании Cisco.

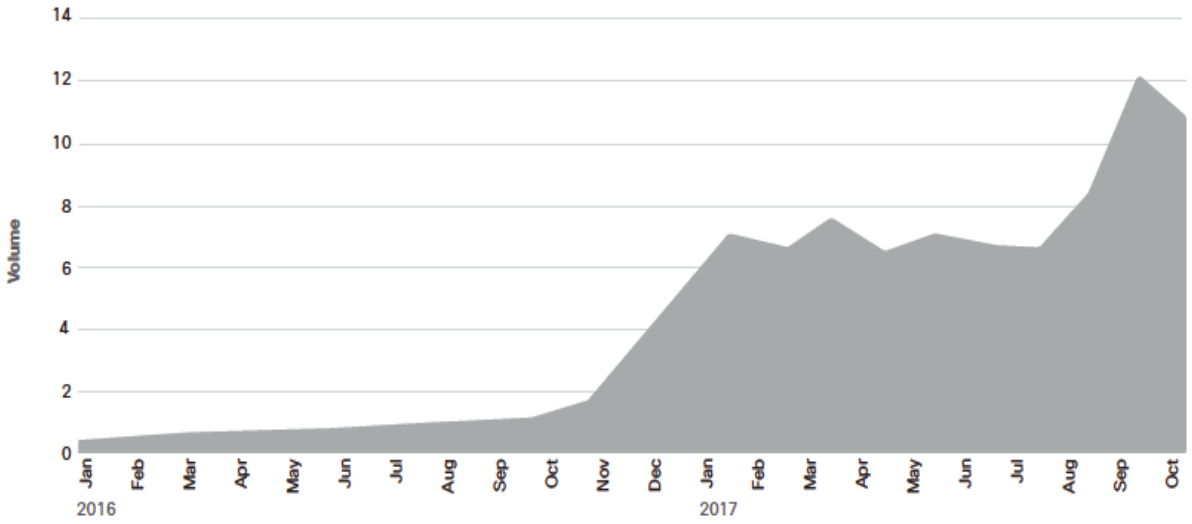


Рис. 2. Объем вредоносного ПО в Интернете, зафиксированный в компании Cisco за период с января 2016 по октябрь 2017 г.

Источник: [Cisco 2018 Annual Cybersecurity Report. Cisco Systems Inc., 2018.]

Вывод, который делают специалисты, оказывается неутешительным: киберпространство сегодня используется в большей степени не для поддержки и развития интересов пользователей в коммуникации и получении информации и знаний, а для атаки потенциальных противников.

Это связано с рядом причин. Во-первых, передача данных опирается на несовершенные сетевые протоколы и открытые архитектуры, и в философии сетевой защиты до сих пор преобладает обнаружение угроз постфактум, а не предупредительное устранение уязвимостей. Во-вторых, атаки в киберпространстве происходят с большой скоростью и эффективностью, подвергая всю систему безопасности экстремальному и почти мгновенному давлению, поскольку атакующий должен быть успешным только один раз,

тогда как защищающийся должен быть успешным все время. В-третьих, в силу своей повсеместности расстояние в киберпространстве не является проблемой, как в других областях человеческой деятельности. Атаки могут возникать из одной точки мира и мгновенно достигать другой. В-четвертых, приписывание ответственности за атаки и поиск, «кто виноват»[84] является по большей части проблематичным, что усложняет любые возможные ответные действия и решения. И, наконец, в-пятых, глубокая зависимость от киберпространства всего современного общества дает благодатную почву для развертывания стратегических действий против противника.

1.2. Структура кибервласти и стратегический потенциал государства в XXI веке

Киберпространство и власть над ним становятся сегодня фундаментом научно-технологического и социально-экономического развития всех наций, открывая перед ними новые горизонты модернизации всех сторон жизни общества. Кибернетическая власть или просто кибервласть все более превосходит по своему влиянию традиционные политические, экономические и военные формы доминирования, понимаемые как господство овеществленных структур, осуществляющих насилие в отношении различных слоев общества[85]. Кибернетическая власть также отлична от традиционной трактовки власти.

По своей природе политическая власть в киберпространстве отличается от «классической» власти, которая имела рельефно выраженную *социально-экономическую* обусловленность. Так, по К. Марксу, экономически господствующий класс обладает властью. Поэтому, преобразование структур капиталистического общества, преодоление отчуждения он связывал со

[84] Douglas M. Risk and Blame: Essays in Cultural Theory. London: Routledge, 1992.

[85] Вебер М. Основные социологические понятия // М. Вебер. Избранные произведения. М.: Прогресс, 1990.

становлением власти рабочего класса[86]. По М. Веберу, власть это форма социального взаимодействия, при котором одна сторона навязывает волю другим с помощью права, авторитета или традиций. Власть исторически развивается. Им были выделены следующие типы власти: легальная, харизматическая и традиционная[87]. Как считал Т. Парсонс, власть – экономический, политический, ценностный ресурс, позволяющий руководителям, имеющими соответствующий статус, определять характер целедостижения больших и малых коллективов[88]. М. Фуко был первым, кто показал выход власти за пределы политического и экономического пространства. По его мнению, власть представляет собой сложные взаимодействия людей, проявляющиеся в виде противостояния в самых различных формах господства и подавления, знании и повседневных дискурсивных практиках[89]. По Р. Эмерсону, власть – структурный и функциональный ресурс, обусловленный социальными отношениями зависимости[90]. Э. Гидденсу связывал власть с преобразующей способностью социального актора[91]. Как считает Дж. Александер, власть – символические коды доминирования и господства[92].

Политическая власть в киберпространстве это власть “собственников средств определения” смыслов (У. Бек) – соответственно, ныне важно проанализировать характеров акторов-собственников этой власти, их политические интересы.

В самом общем смысле кибервласть можно определить как *сложную систему ресурсов, структурированных вокруг производства и обмена цифровой информации, а также контроля над ней*. Подчеркнем, речь идет о

---

[86] Маркс К. Социология. Сборник. М.: «КАНОН-пресс-Ц», «Кучково поле», 2000.

[87] Вебер М. Политика как призвание и профессия // М. Вебер. Избранные произведения. М.: «Прогресс», 1990.

[88] Парсонс Т. О понятии «политическая власть» // Антология мировой политической мысли. Т.2. М., 1997.

[89] Фуко М. Интеллектуалы и власть: Избранные политические статьи, выступления и интервью. М.: Праксис, 2002. - 384 с.

[90] Emerson R.M. // American Sociological Review, 1962. № 27.

[91] Гидденс Э. Устроение общества: Очерк теории структурации. М.: Академический проект, 2003.

[92] Alexander J. C. The Civil Sphere. Oxford University Press, 2006.

сложной системе, функционирующей «по-новому и другим способом»[93]. Сложность, в частности, проявляется в том, ресурсы оказывают *нелинейное действие*: сравнительно небольшие факторы могут быть весьма значимыми[94]. Из этого следует, что в силу повсеместности распространения киберпространства и усиления зависимости от него кибервласть постепенно трансформируется во властную *гегемонию*, т.е. супервласть, которая не ограничивается контролем над сугубо кибернетическими ресурсами, включающими в себя структурные уровни киберпространства, обозначенные нами в предыдущем параграфе, но также вбирает в себя человеческие, финансовые, экономические, символические, культурные и политические ресурсы, создаваемые или задействованные в этой системе. Не случайно, по рыночной капитализации такие Интернет-гиганты как Alphabet (Google), Amazon, Tencent, Alibaba Group входят в десятку крупнейших компаний мира, работа в них считается очень престижной, а их технические возможности привлекают самое пристальное внимание со стороны политиков, спецслужб и военных.

Ярким воплощением усиливающейся гегемонической роли кибервласти является набирающая обороты Четвертая индустриальная революция (Рис. 3.).

[93] Urry J. Global Complexity. Cambridge: Polity Press, 2003. P. 23.
[94] Urry J. Climate Change and Society. Malden: Polity Press, 2011. P. 41-42.



Рис.3. Развитие мировой промышленности в разрезе индустриальных революций[95]

Впервые термин «индустрия 4.0» появился в Европе всего лишь 2011 году на одной из промышленных выставок в Ганновере, где правительство Германии представило стратегию более широкого применения информационных технологий в производстве. Этому примеру последовали и другие страны, а термин «индустрия 4.0» быстро стали использовать как синоним Четвертой промышленной революции[96]. Суть ее заключается в том, что материальный мир соединяется с виртуальным, в результате чего рождаются новые *киберфизические комплексы*, объединенные в единую дигитализированную экосистему. Индустрия 4.0. характеризуется как «глубинное изменение» общества на основе технологий повсеместной цифровизации, ведущих в итоге к *сапиентизации* (от лат. *sapiens* – разумный) реальности. Элементы и одновременно этапы такой сапиентизации можно трактовать как направления развития кибервласти:

[95] Коробенков А. Цифровая система управления производством – важный шаг к "Индустрии 4.0" [Электронный ресурс] // Технологии в электронной промышленности, № 7’2016. P.50-52. URL: https://controleng.ru/wp-content/uploads/11_91.pdf (дата обращения 12.04.2020).

[96] Шваб К. Четвертая промышленная революция. М.: «Эксмо», 2016.

1) **Большие данные**. Хотя проблематика «информационного взрыва» обсуждается в литературе с 1940-х гг. [97], разработка программ анализа больших данных становится особенно актуальной только в связи с глобальным развитием Интернета в 2000-е гг. Глобальный доступ к Интернету миллиардов людей по всему миру и прогресс в области информационных технологий сделал возможным мониторинг активности пользователей с целью выявить закономерности, тенденции и взаимосвязи в их поведении и взаимодействии друг с другом. Ярким примером политической капитализации кибервласти больших данных стали итоги выборов в США и референдума о выходе Великобритании из ЕС в 2016 г. За предвыборной кампанией Д. Трампа и за кампанией в поддержку «Брекзита» стояла одна и та же компания «Cambridge Analytica», чей анализ больших данных и таргетированная политическая реклама в социальных сетях позволили смоделировать реальное поведение избирателей.

2) **Интернет вещей**. Реализация концепции «Интернета вещей» подразумевает подключение к беспроводным сенсорным сетям неодушевленных предметов от бытового назначения («умный дом») до промышленных роботов. В 2008-2009 гг. количество подключенных к Интернету девайсов превзошло количество пользователей и к 2020 г. прогнозируется их увеличение до 50 млрд.[98] В передовых странах уже созданы и действуют специальные программы по развитию промышленного Интернета. В качестве примера эффективности Интернета вещей можно привести завод Chrysler в Толедо (США). Каждый день здесь выпускается более 700 кузовов для автомобилей Jeep Wrangler. При этом задействованы 259 немецких роботов KUKA, которые «общаются» с 60 000 других устройств и станков. Обмен и хранение данными организованы по облачной технологии. В то же время кибервласть, основанная на Интернете вещей,

[97] Press G. A Very Short History of Big Data [Электронный ресурс] // Forbes.com. 2013, 09 May. URL: https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#92208b965a18 (дата обращения: 21.05.2019).

[98] Evans D. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Cisco Internet Business Solutions Group (IBSG), 2011.

элиминирует границу между приватным и публичным пространством, превращая общество в т.н. *омниоптикон,* где все люди и их поведение оказываются на виду у разных окружающих вещей, и это не говоря о технологиях отслеживания мобильных телефонов и других гаджетов, специально созданных для выхода в Интернет. В частности, развитие системы распознавания лиц на основе работы IP-камер видеонаблюдения, а также установка «умных» мусорных баков сделало Лондон самым «прозрачным» и «наблюдаемым» городом мира [99].

3) **Гибридная реальность**. Следующим этапом развития технологий виртуальной и дополненной реальности является создание *гибридного мира*, где граница между реальным и кибернетическим стирается или престает играть значимую роль[100]. Максимизация правдоподобности и возможность взаимодействия с виртуальным объектом, «живущим» в реальном мире – ключевые моменты в смешанной реальности. Уже функционирующий пример смешанной реальности из современной жизни – сканер текста со встроенным переводчиком (например, «Google-переводчик»). Если приложения виртуальной реальности требуют изоляции физического мира и полного погружения органов чувств в цифровой мир, а технология дополненной реальности всего лишь выводит на дисплей заложенную в них информацию (очки Google-glass), то здесь мы наблюдаем целый процесс гибридизации: сканирование текста, его распознавание, перевод, подбор похожего шрифта, коллажирование (замена исходного текста на скриншоте на перевод). В итоге мы получаем полностью новую альтернативную реальность, а не просто виртуальную или дополненную. Впечатляющую работу в этом направлении ведет «Майкрософт», разрабатывая гарнитуру HoloLens. Это самостоятельное устройство, не требующее ни смартфона, ни ПК, которое не изолирует никаких органов чувств, объединяя физический и

[99] The Most Spied Upon Cities In The World [Электронный ресурс] // Worldatlas. 2017, April 25. URL**:** https://www.worldatlas.com/articles/most-spied-on-cities-in-the-world.html (дата обращения 02.03.3018).

[100] Latour B., Woolgar S. Laboratory Life: The Construction of Scientific Facts. Princeton: Princeton University Press, 2013.

цифровой миры в единое целое. Устройство воспроизводит звук, но в то же время не мешает слышать того, что происходит вокруг, подразумевает управление предметами пальцами рук и голосом, строит голограммы, но в то же время не заполняет пространство и не мешает взгляду. Известное американское агентство передовых оборонных проектов DARPA также уже испытывает специальный шлем, оборудованный полупрозрачным экраном, который находится перед одним глазом солдата и позволяет видеть все, что происходит вокруг него не поворачивая головы, а также выводит на экран все необходимые для дальнейших действий параметры: расстояние до объекта, координаты и т.д. Смешанная реальность находится пока на начальном этапе своего внедрения, чего не скажешь о бурном развитии еще одной точки приложения кибервласти – искусственного интеллекта.

4) **Искусственный интеллект**. С учетом активного развития робототехники, внедрения виртуальных чат-ботов типа «Siri», а также разработки программного обеспечения на основе нейронных сетей (самообучающихся программ) искусственный интеллект (ИИ) уже стал неотъемлемой частью повседневной коммуникации. Посттьюринговые технологии делают современные образцы виртуальных аватаров и чат-ботов не отличимыми от людей по внешнему виду и используемым паттернам коммуникации. Хотя экспертами признается, что в ближайшие 20 лет мы вряд ли столкнемся с машинным интеллектом, полноценно сравнимым или тем более превосходящим человеческий, в ближайшие годы машины не хуже, а то и лучше будут справляться с выполнением все большего числа конкретных задач[101]. Конечная стадия развития технологии ИИ – появление разумных машин в виде отдельных «личностей» или в виде «универсальной среды». Создание такого ИИ будет означать новый этап эволюции и полную перестройку общественной жизни. Поэтому лидерство в области разработки ИИ признается первостепенным в обеспечении национальной безопасности,

[101] Preparing for the Future of Artificial Intelligence. Washington: Executive Office of the President National Science and Technology Council Committee on Technology, 2016.

о чем открыто заявляют такие политические лидеры как Д. Трамп и В.В. Путин[102].

5) **Общество 5.0.** Завершающим этапом развития кибервласти и сопутствующих технологий в обозримом будущем будет последовательное создание нового типа общества, основанного на роботизации и повсеместных вычислениях устройствами, пронизывающими окружающую среду (т.н. *юбикомп*). Сюда входят не только такие продвинутые разработки в области «окружающего интеллекта», как нательные компьютерные устройства, «умная» одежда, «умная пыль» (самоорганизующиеся подключенные к сети крошечные устройства без дисплеев), «гибкие пленки» (OLED-дисплеи) и материальные ощутимые интерфейсы (трехмерные микроэлектронные – механические устройства), но и поддержка на государственном уровне определенного образа жизни граждан. В Японии с 2016 г. официально принята на вооружение программа создания «Общества 5.0», т.е. «супер-умного» общества, основанного на максимальной степени интеграции физического и киберпространства, роботизации и повсеместном развитии искусственного интеллекта [103]. В Обществе 5.0 предполагается устранить все сдерживающие региональные, возрастные, гендерные и нормативные барьеры на пути внедрения новой симбиотической социальной системы, что, как предполагается, даст новый толчок экономическому развитию Японии и будет способствовать решению ее социальных, экологических и демографических проблем.

---

[102] Д. Трамп: «Сохраняющееся американское лидерство в сфере ИИ играет важнейшую роль в поддержании экономической и национальной безопасности Соединенных Штатов» /Artificial Intelligence for the American People [Электронный ресурс] // White House. URL: https://www.whitehouse.gov/ai/ (дата обращения 26.07.2019); В.В. Путин: «…Если кто-то сможет обеспечить монополию в сфере искусственного интеллекта,…тот станет властелином мира…мы, конечно, должны обеспечить технологический суверенитет в сфере искусственного интеллекта. Это важнейшее условие состоятельности нашего бизнеса и экономики, качества жизни граждан России, безопасности, в конце концов, и обороноспособности государства». / Совещание по вопросам развития технологий в области искусственного интеллекта [Электронный ресурс] // Президент России. 2019, 30 мая. URL: http://www.kremlin.ru/events/president/news/60630 (дата обращения: 13.06.2019).

[103] Report on the 5th Science and Technology Basic Plan. Tokyo:Council for Science, Technology and Innovation, Cabinet Office, Government of Japan, 2015.

Как мы видим, развитие кибервласти в эпоху Четвертой индустриальной революции, меняет, как говорит К. Шваб, «не только то, «что» и «как» мы делаем, но и то, кем мы являемся»[104]. В этой связи можно предположить, что соперничество в области киберпространства между различными акторами и прежде всего нациями неминуемо будет нарастать, т.к. на кон поставлено не только процветание, но и благополучие людей, что является предметом стратегии национальной безопасности любой державы. Это требует рассматривать кибервласть в стратегическом смысле как деятельность, направленную на достижение политических целей.

В этом отношении общим местом в исследованиях стратегического значения киберпространства является признание того, что оно становится пятой областью развертывания силового противоборства государств наравне с традиционными аренами военных действий – сушей, морем, воздухом и космосом[105]. Необходимо понимать, что киберпространство так же, как и остальные, имеет политическое значение, и стратегические действия, направленные на усиление собственных позиций и ослабление позиций противника, здесь неизбежны. Поэтому с самого начала исследований киберпространства проблематика наращивания и распределения кибервласти как политического ресурса становится предметом теоретического анализа [106]. Кибервласть технически, тактически и даже оперативно отличается от других политических инструментов военного и невоенного назначения, но, тем не менее, она не выходит за рамки стратегического поля, поэтому ее можно анализировать как разновидность политической власти. Г. Моргентау подчеркивал, что под властью следует понимать «все то, что обеспечивает контроль одного человека над другим. Таким образом, она включает все виды социальных отношений, отвечающих этой цели, – от физического насилия до самых тонких психологических связей, позволяющих одному разуму

[104] Шваб К. Четвертая промышленная революция. М.: «Эксмо», 2016. С. 9.
[105] Харрис Ш. Кибервойн@: пятый театр военных действий. М.: Альпина нон-фикшин, 2016.
[106] Jordan T. Cyberpower: The Culture and Politics of Cyberspace and the Internet. London: Routledge, 1999.

контролировать другой»[107]. В этом смысле кибервласть является продолжением политики, а значит ее ключевой особенностью является способность в условиях мира и/или войны манипулировать стратегической средой в своих интересах, с тем, чтобы наращивать свое доминирование над предполагаемыми противниками. В то же время кибервласть обладает своей собственной спецификой, которую необходимо учитывать, если рассматривать киберпространство как сферу политического противостояния. Здесь можно выделить несколько важных характеристик, которые вносят новое содержание в понимание стратегического потенциала киберпространства:

– Кибервласть абсолютна в стратегическом смысле. Наземные, морские, воздушные и космические силы способны оказывать стратегическое влияние на каждую из других областей, но ничто не имеет столь универсального, единовременного и мощного стратегического эффекта, воздействующего сразу на все области национальной безопасности, как кибервласть. Учитывая нарастающую киберзависимость вооруженных сил, экономики и общества в целом, а также возможности использования различных инструментов власти, таких как дипломатия, средства массовой информации и коммерция, киберпространство и основанная на ней кибервласть становятся *уникальными и универсальными* стратегическими ресурсами. Сухопутные, морские, воздушные и космические силы могут вернуться в казармы, порты, на аэродромы или, в случае спутников, просто превращаются в космический мусор. Кибервласть же не возвращается к отправителю и почти не расходуется.

– Кибервласть может и имеет латентный характер. Одной из привлекательных сторон киберпространства, как уже говорилось, является возможность для многих пользователей тайно использовать его в глобальном масштабе, не опасаясь ответственности или симметричного ответа от

[107] Моргентау Г. Политические отношения между нациями. Борьба за власть и мир (отрывок) // Политология: хрестоматия / Сост. проф. М.А. Василик, доц. М.С. Вершинин. М.: Гардарики, 2000. С.743-754. С. 750.

жертвы. Вредоносное ПО (раскрыть) может быть размещено в сетях без ведома жертвы до тех пор, пока оно не будет активировано и не нанесет планируемый урон. Разоблачения Э. Сноудена о программе всемирной слежки PRISM лишний раз показывают, что чем больше масштабы стратегической кибервласти, тем более скрытной она является в отличие от всех других форм военной мощи.

– Кибервласть комплементарна по отношению к реальной «твердой силе». Это означает, что в отличие от эффективных инструментов силового принуждения с помощью военной силы, принудительной дипломатии, экономических санкций кибервласть в автономном режиме не способна привести к уничтожению противника в военном или политическом смысле. Потенциал силового давления и принуждения в киберпространстве пока ограничен и, вероятно, останется таковым. Ни одна кибератака сама по себе еще не привела к падению правительства или экономики какой-то страны. Любые подобные действия так или иначе должны сопровождаться реальной силовой политикой в открытом режиме. Например, несмотря на весь ущерб, нанесенный компьютерным червем Stuxnet в отношении Ирана в 2010 г., он явно не принудил иранских лидеров отказаться от своей ядерной программы. Масштабные кибератаки на одну из самых киберзависимых стран в мире, Эстонию, в 2007 г. также не привели к каким-либо существенным политическим результатам. В будущем ситуация может измениться, но для этого кибервласть должна будет лишиться своего предыдущего качества и стать полностью прозрачной и видимой со стороны противника, чтобы условия открытой войны соблюдались полностью и ее последствия учитывались всеми сторонами.

Возникает вопрос, можно ли трактовать стратегическую кибервласть как разновидность «мягкой силы»? Как известно, «мягкая сила» нацелена на человеческий фактор, чтобы «заставить других самим желать то, что вы от

них хотите» [108] путем информационного влияния. Дж. Най, придумавший этот термин, всегда подчеркивает, что мягкая сила действует с помощью «средств сотрудничества», т.е. носит открытый и прямой характер, используя для убеждения и привлечения людей на свою сторону позитивные стороны культуры, политических ценностей и внешней политики страны влияния. Успех «мягкой силы» был с очевидностью продемонстрирован в 1990-е г., когда сознание широких масс и правящих элит советского блока было настолько «очаровано» духом свободы, успеха и благополучия, прорывавшегося с Запада вместе с музыкой, книгами, радио и ТВ-передачами, что в итоге вся система международных отношений, основанная на «холодном» противостоянии двух идеологических лагерей не выдержала и была сломлена без единого выстрела друг в друга. Сегодня же, в эпоху глобализированного модерна, т.е. почти повсеместного утверждения институтов и ценностей модерна, основанного, прежде всего, на западных идеях, мягкая сила самого Запада становится менее эффективной. «Великое выравнивание», т.е. рост благополучия незападных цивилизаций, с одной стороны, и стремление последних к последовательной глокализации, анклавизации и индигенизации на базе укрепления национальной, культурной, религиозной идентичности, с другой, ведут к ослаблению Запада как центра мягкой силы. В этом смысле абсолютным провалом стратегии западной «мягкой силы» можно считать формирование радикально антизападной экстремистской группировки «Исламское государство» в 2013-2015 гг. на территориях, освобожденных силами западной коалиции от тиранических режимов на Ближнем и Среднем Востоке.

Поэтому важнейшими условиями для эффективной работы «мягкой силы» должны быть три вещи: 1) стабильно функционирующий рынок идей, где существует конкуренция сообщений, свободных от сдерживающего влияния государства; 2) доступ к самым разнообразным каналам

[108] Nye J.S., Jr. Soft Power: The Means to Success in World Politics. New York: Public Affairs, 2004. P.5.

коммуникации для максимального охвата аудитории и 3) сами реципиенты должны быть открыты для восприятия информации, которую они считали бы привлекательной, достоверной и эмоционально насыщенной. Таким образом, если в информационном пространстве действуют механизмы цензуры, пропаганды, медиаканалы находятся под контролем государства, а сами реципиенты по тем или иным не восприимчивы к новым идеям, тогда «мягкая сила» превращается в слишком слабую или вовсе терпит неудачу. Более того, как отмечают Й. Холл и Ф. Смит [109], «мягкая сила» зачастую не может компенсировать собой сложившиеся негативные аттитюды к ее источнику в общественном мнении, как это происходит, например, в отношениях между Китаем и его соседями, которые, несмотря на колоссальные китайские инвестиции в продвижение своего позитивного имиджа в регионе через все возможные медиа, не становятся его ни политическими, ни идеологическими союзниками.

Политика, опирающаяся только на «мягкую силу», сегодня оказывается слишком ненадежной, поэтому сам Дж. Най признает необходимость разработки в современных условиях концепции т.н. «умной силы», которая последовательно сочетает «мягкую» и «твердую» силы в своем воздействии на оппонента [110]. Для этого им применяется концепция «трех лиц» власти, каждое из которых может иметь «твердую» и «мягкую» составляющие [111]:

1) **явная власть** – здесь происходит открытая, явная борьба за изменение поведения оппонента в соответствии с определенными нормативными представлениями;

2) **латентная власть** – это скрытое вовлечение в игру по определенным правилам, где происходит легитимация той или иной проблематики, интересов, вариантов действий, но всегда в рамках заданной

[109] Hall I., Smith F. The struggle for soft power in Asia: Public diplomacy and regional competition // Asian Security. 2013. Vol. 9(1). P. 1-18.

[110] Nye J.S., Jr. The Future of Power. New York: Public Affairs, 2011; Най Дж. Будущее власти: как стратегия умной силы меняет XXI век. М.: АСТ, 2014.

[111] Nye J.S., Jr. The Future of Power. New York: Public Affairs, 2011. P. 10-18.

(и выгодной) «повестки дня», что тем самым позволяет контролировать оппонента и предвидеть его стратегию;

3) **невидимая власть –** она подразумевает глубокое «невидимое» управление, а точнее говоря, манипуляцию поведением и сознанием людей на уровне базовых предпочтений, потребностей и аттитюдов без осознания ими происходящего.

Эти три аспекта стратегической власти присутствуют и в киберпространстве, предоставляя широкие возможности для реализации и «твердой», и «мягкой» силы одновременно. На этой основе мы можем выделить три основных стратегии кибервласти: *кибератаки*, *кибердавление* и то, что можно было бы обозначить как *рефлексивное киберуправление*. В то же время специфика киберпространства зачастую делает, на наш взгляд, невозможным подобное различение, т.к. некоторые открытые действия имеют невидимый источник происхождения, а «мягкие» информационные действия могут маскировать политику принуждения. Такие действия носят *гибридный* характер. В любом случае следует классифицировать стратегические методы кибервласти на основе типологии Дж. Ная и дать релевантные примеры (Таб. 1.).

Типы кибервласти	**Типы применяемой силы**		
	«Твердая сила»	«Мягкая сила»	«Гибридная сила»
Кибератаки	DDoS-атаки, вирусы, хакинг, кибертерроризм	Спам-реклама	Слежка за пользователями в сети, кибершпионаж
Кибердавление	Цензура, публикация секретных данных, ограничение/отключение Интернет-траффика	Цифровая дипломатия	Мобилизация на социальные действия

Рефлексивное киберуправление	Искажение и утаивание информации (фейки, постправда), троллинг, сокпаппетинг, астротурфинг в социальных сетях (провокации, обман, интриги, инсинуации, слухи)	Вовлечение в киберсообщества, формирование повестки дня	Политический маркетинг, премодерация и постмодерация информационных потоков

Таб. 1. Стратегические действия в киберпространстве

Как видно из таблицы, т.н. «гибридная сила» носит черты как «мягкой», так и «твердой» силы, поскольку она не является ни агрессивно-силовым, ни культурно-идеологическим средством в чистом виде. Вневременной характер киберпространства, невидимость неискушенному взгляду происходящих в нем процессов, многообразие возникающих здесь социальных связей позволяет применять более гибкие и эффективные методы стратегического влияния и контроля. При этом любые действия кибервласти могут иметь результаты как на уровне самого киберпространства, включая все четыре уровня его структуры, так и конвертироваться в значимые ресурсы за его пределами, при этом гораздо быстрее, чем конвертация обычных ресурсов. Например, распространение информации в социальных сетях о самосожжении тунисского торговца фруктами М. Буазизи в конце 2010 г. на следующий же день вывело тысячи людей на улицы, а в течение двух последующих недель привело к свержению власти в Тунисе и запустило региональную волну политических протестов и революций, известную сегодня как «Арабская весна». «Власть, которая обладает коммуникационной монополией на радио, телевидение, печатные органы, оказывается парализованной опережающими действиями,

организуемыми через социальные сети, а эффект неожиданности, производимый этими действиями и дает выигрыш оппозиции» [112]. Быстрая социальная мобилизация через социальные сети, т.е. конвертация кибервласти в реальный стратегический капитал, до сих пор является очень востребованным инструментом в любом политическом или ином конфликте.

Цифровая дипломатия (также известная как «сетевая дипломатия», «дипломатия Web 2.0», «Интернет-дипломатия», «публичная дипломатия 2.0», «публичная дипломатия web 2.0») в контексте кибервласти представляет собой использование интерактивных средств Интернет-платформ и новых ИКТ для содействия в реализации внешнеполитических целей. Самый яркий пример здесь – это «Твиттер-дипломатия» политических лидеров по всему миру. За последние годы платформа мгновенных коротких сообщений «Твиттер» стала самой популярной в цифровой дипломатии по всему миру. По данным за 2018 г. существуют уже 951 твиттер-аккаунт, принадлежащий главам государств и министрам иностранных дел в 187 странах, представляющих 97% членов ООН[113]. Их общая аудитория составляет почти 500 млн. чел. «Твиттер» позволяет емко и оперативно передавать информацию, оценки и получать реакцию людей со всего мира, тем самым создавая мировое общественное мнение. Однако, есть только один лидер, который сделал «Твиттер» своим основным дипломатическим инструментом, и это Д. Трамп. Он имеет более 60 млн. фолловеров и около двухсот подписок от государственных лидеров. То, как часто он использует «Твиттер» для прямых и нелицеприятных выпадов в сторону других стран и их представителей, перевернуло представление о дипломатии вообще. «Твиттер» Трампа и некоторых других лидеров, по сути, стал источником альтернативной или даже анти-дипломатии, в рамках которой можно говорить и писать то, что не принято высказывать вслух. Большинство

[112] Системный мониторинг глобальных и региональных рисков: Арабский мир после Арабской весны / Отв.ред. А.В. Коротаев, Л.М. Исаев, А.Р.Шишкина. М.: ЛЕНАНД, 2013. С.396

[113] Lüfkens M. Twiplomacy Study 2018 [Электронный ресурс] // Twiplomacy. 2018, July 10. URL:https://twiplomacy.com/blog/twiplomacy-study-2018/?source=post_page (дата обращения 13.04.2020)

инвектив Трампа не находят прямого ответа от своих адресатов, и это еще больше усиливает его позиции в мировой дипломатии, т.к. оставляет последнее слово за ним. В любом случае, кибервласть Трампа от этого только увеличивается, уже сделав его аккаунт номером один среди мировых лидеров. Даже аккаунты Папы Римского и премьер-министра Индии (с населением более миллиарда человек) имеют меньше подписчиков.

Однако, «Твиттер-дипломатия» представляет собой лишь одну из многих других возможностей того, для чего может применяться «мягкая» кибервласть. Американский эксперт Ф. Хэнсон выделяет, как минимум, восемь направлений эффективной цифровой дипломатии [114]:

1) менеджмент в сфере знаний и компетенций: использование различных ведомственных и государственных знаний, сведений и компетенций для их накопления, оптимизации и совместного использования в рамках достижения национальных интересов за рубежом;

2) публичная дипломатия: установление и поддержание связей с Интернет-аудиторией в онлайн-режиме и использование ИКТ для таргетированной коммуникации с влиятельными инфлюенсерами в киберпространстве с целью привлечения их к работе в интересах государства;

3) менеджмент в сфере информационных потоков: агрегация и анализ информации при разработке государственных решений, а также прогнозирование и учет возникновения новых социальных и политических движений и настроений в обществе на основе такого анализа;

4) консульская коммуникация: создание прямых каналов связи для граждан, путешествующих за границу, обеспечение бесперебойной горячей линии в кризисных ситуациях;

5) связь при стихийных бедствиях: надежное функционирование инфраструктуры ИКТ в чрезвычайных ситуациях;

---

[114] Hanson F. Revolution@State: The Spread of eDiplomacy. Lowy Institute for International Policy, 2012.

6) обеспечение свободы информации: поддержка распространению технологий, позволяющих сделать интернет максимально свободным и открытым в целях содействия свободе слова и демократии;

7) привлечение внешних ресурсов: создание удобных цифровых платформ для внешней экспертизы государственных программ и целей;

8) государственное управление: обеспечение эффективного развития, координации и планирования внешнеполитических аспектов работы государственных министерств и ведомств.

Таким образом, «цифровая дипломатия» подразумевает весьма широкий набор управленческих задач – и традиционных, и новых, но решаемых с помощью киберинструментов в режиме онлайн. В ситуации борьбы за кибервласть цифровая дипломатия включает в себя элементы кибердавления, т.е. стремится к неявному противостоянию с противником с целью создания благоприятных условий для реализации реальных политических действий в своих интересах.

Однако, наибольший интерес с точки зрения стратегической реализации кибервласти для нас представляет рефлексивное киберуправление как, возможно, наиболее эффективный, но наименее признаваемый элемент влияния на сознание и поведение людей в киберпространстве и за его пределами.

Само понятие рефлексивного управления своим появлением обязано работам российско-американского математика В.А. Лефевра, который в 1970-е гг. разработал теорию рефлексивной системы [115]. С помощью этой теории социолог представил любые взаимодействия «разумных» субъектов как систему рефлективных процессов, т.е. процессов, требующих постоянного осознания и учета «внутреннего мира» Другого с целью понимания его поведения и адаптации к нему. В ситуации конфликта эти процессы вовлекают еще один элемент – управление внутренним миром

[115] Лефевр В.А. Конфликтующие структуры. Издание второе, переработанное и дополненное. М.: Изд-во «Советское радио», 1973.

Другого или рефлексивное управление, т.е. скрытые, невидимые попытки передачи оснований для принятия решения одним из субъектов другому в требуемом направлении. С помощью техник рефлексивного управления осуществляется воздействие на субъекта, склоняющее его принять решение или выбрать модель поведения, которые заранее подготовлены или полностью контролируются управляющей стороной. Другими словами, речь идет о манипулировании общественным сознанием, которое чаще всего осуществляется с помощью таких информационных средств как пропаганда, провокация, обман, интриги, намеки, слухи. Сам В.А. Лефевр различал четыре основных способа рефлексивного управления, где могут происходить манипуляции [116]:

1) манипулирование посредством влияния: здесь возможно либо прямое склонение к тому или иному действию, либо инверсивное – через склонение к альтернативному выбору посредством формирования ложных посылок; пример последнего варианта – из сказки «Как братец кролик перехитрил братца Лиса»: пойманный Кролик трижды просит Лиса не бросать его в колючий терновый куст, но именно это Лис и делает в итоге, чего и добивался Кролик, т.к. там был его дом;

2) манипулирование путем изменения отношений: здесь возможно либо вступление в союз, либо в конфликт с противником ради достижения неразглашаемых целей;

3) управление через подсознание: здесь предполагается предварительное «изготовление» тех или иных мнений и/или желаний, закрепление их в сознании и их последующая целенаправленная активизация.

Важно подчеркнуть, что в информационном пространстве, особенно в Интернете, где поток обсуждаемых событий и новостей настолько велик и текуч, что проверка их истинности становится непростой аналитической

[116] Лефевр В.А. Лекции по теории рефлексивных игр. М.: «Когито-Центр», 2009.

задачей, рефлексивное управление включает в себя новые специфические инструменты.

Пример тому – утверждение в массовой политической коммуникации «*постправды»,* суть которой в том, что информации о событиях подается с акцентом на эмоциональное восприятие, что позволяет скрыть или исказить их объективную фактичность – итоге формируется политически ангажированное общественное мнение [117]. Иными словами, события воспринимаются как реальные, но, фактически, они такими не являются. В итоге, благодаря развитию цифровых медиа активно развивается *политика постправды*, агрессивно ориентированная на разрушение в массовом сознании границы между фактами, знаниями, мнениями и ценностями в целях получения политических преимуществ на внутреннем или международном рынке идей. Такая политика не является новостью, т.к. Х. Арендт еще в 1970-е гг. писала о «дефактуализации», свойственной миру политики [118], а Ж. Деррида в начале 1990-х гг. прямо делает вывод о перформативности медиа-правды, когда одно авторитетное или экспертное мнение тиражируется СМИ как единственно верное [119]. Особенностью современного момента являются лишь масштаб и изощренность политической лжи и цинизма, ставшие возможными благодаря невиданной силе кибервласти. В этой связи особое место в политике постправды занимают две категории инструментов влияния:

1) «фактоиды» (Н. Мэйлер), иными словами, события искусственно сконструированные в тех или иных политических целях и растиражированные в СМИ. По существу, фактоид инсценированное событие, но многократно воспроизведенное в медиапространстве оно воспринимается как реальное. Практический смысл создания «фактоидов»

---

[117] Word of the Year 2016 [Электронный ресурс] // Oxford Languages. URL: https://en.oxforddictionaries.com/word-of-the-year/word-of-the-year-2016 (дата обращения 15.01.2017).

[118] Arendt H. Lying in Politics: Reflections on the Pentagon Papers // Arendt H. Crises of the Republic. New York: Harcourt Brace & Co., 1972. P. 1-48.

[119] Derrida J. History of the Lie: Prolegomena // Derrida J. Without Alibi. Edited, translated, and with an Introduction by Peggy Kamuf. Stanford: Stanford University Press, 2002. P. 28-70.

хорошо отображает теорема У. Томаса, согласно которой, если люди воспринимают нечто как реальное, то они с этими установками живут и действуют;

2) «инфологемы» (В.З. Коган) – ложная или неполная информация, основанная на мифах, фейках, однако презентующая реальные события как вымысел, что весьма часто используется как эффективно работающий прием в политической пропаганде. Инфологемы обратны по смыслу фактоидам, но имеют столь же разрушительное влияние на публичную сферу; пример: война на Донбассе и ее освещение в российских и украинских СМИ.

Как эти и другие стратегии кибервласти реализуются через социальные сети в Интернете, будет показано далее.

Таким образом, национальная безопасность в современных условиях во все большей степени определяется капитализированием кибервласти. Страны, которые достигнут технологического и политического превосходства в киберпространстве, будут претендовать на мировое господство. Битва за кибервласть между державами будет важнейшей характеристикой ближайших лет развития международных отношений. Примером того, как использование кибервласти в качестве силового средства противостояния с Россией принесло весомый результат западной коалиции, стал государственный переворот на Украине в 2014 г., следствием которого стал приход к власти откровенно антироссийских политических сил, разрыв всех связей между нашими странами и установление прозападной государственной политики. Этого удалось добиться в результате применения широкого спектра силовых (не военных) средств политического принуждения, в частности, огромную роль сыграл Интернет и организованная кампания в социальных сетях, которым удалось решить важнейшие задачи:

– в области культуры (смена культурно-исторического кода);

– в образовании (воспитание в антироссийском духе);

– создание враждебных России социальных движений и общественных организаций.

Эффективная стратегия национальной безопасности в современных условиях киберпротивостояния должна, на наш взгляд, включать как минимум три компонента кибервласти:

1) структурная кибервласть, обеспечивающая развитие обозначенной нами национальной структуры киберпространства от физического до семантического уровней, включая необходимые элементы *киберзащиты*;

2) институциональная кибервласть, направленная на вовлечение человеческих, нормативных, экономических, технических и других ресурсов в область реализации Четвертой промышленной революции на основе внедрения киберфизических систем и искусственного интеллекта;

3) силовая кибервласть, включающая в себя все инструменты твердой, мягкой и гибридной силы для отстаивания и продвижения национальных интересов в международном киберпространстве, включая проведение *кибероперации*, создание сети СМИ и СМК, работу со специализированными международными организациями (ICANN, ITU), киберсообществами и отдельными инфлюенсерами.

Только в случае такого комплексного подхода к реализации национальной безопасности в области кибервласти можно рассчитывать на сохранение национального суверенитета и обеспечение *киберсдерживания* агрессивной политики других государств.

1.3. Кибервойна как проявление сложного информационно-политического насилия

С развитием процессов глобализации и доминированием цифровой составляющей в структуре современной социальной коммуникации войны и межгосударственные противоборства в мире приобрели совершенно новые направления и формы, порождая и новые концепции, и подходы к их

пониманию. Войны XXI века ведутся уже не только и не столько в воздухе, на море и на земле, но прежде всего в киберпространстве. Информация в современном мире становится универсальным средством достижения целей военного, политического и экономического характера. В особенности велика зависимость от информационных систем в сферах военного и государственного управления, а также в областях деятельности, которые связаны с функционированием потенциально опасных и критически важных объектов.

Использование интернета для атак компьютерных систем другого государства может нанести значительный ущерб его экономике и создать разлад в повседневной жизни страны. В книге Д. Туровского отмечается, что влияние специалистов по кибербезопасности усиливается ежегодно и повышается число средств слежения за гражданами[120]. Именно изменение типов угроз требует внимания к такому феномену как *кибервойна*.

Впервые термин «кибервойна» появился в научно-популярной статье писателя Дж. Поста 1979 г., в которой он описывал в духе киберпанка будущие войны машин против машин, где компьютеры, объединенные в сети, будут управлять ракетами, бомбами и заниматься шпионажем за противником[121]. Однако подлинным рождением современной концепции кибервойны можно считать статью 1993 г. известных американских аналитиков Дж. Арквиллы и Д. Ронфельдта «Кибервойна на подходе!», где описывалось, как военные хакеры будут в скором будущем вести не только разведывательную и шпионскую деятельность, но, прежде всего, активно заниматься кибератаками на компьютеры противника с целью разрушения его управленческой системы[122].

Новый этап интереса к идее кибервойн начался в конце 2000-х гг. в рамках обсуждения путей модернизации ведения войн и конфликтов на

---

[120]Туровский Д. Вторжение. Краткая история русских хакеров / Под ред. А. Горбачева. М.: Издательство Individuum, 2019. С. 31.

[121] Post J. Cybernetic War // Omni. 1979. No.5. P. 44-104.

[122] Arquilla J., Ronfeldt D. Cyberwar is Coming! // Comparative Strategy. 1993. Vol. 12 (2). P. 141-165.

международной арене в связи с активным ростом глобальной аудитории Интернета и социальных сетей, в частности. Таким образом, за последние четверть века были сформулированы многочисленные концепции и стратегии кибервойны, но всех их объединяет понимание того, что успех стратегических действий в киберпространстве не сводится к компьютеризации армии и систем вооружения. Цифровой век и сетевое общество породили новую форму информационно-политического насилия, которая потенциально охватывает пространство всей планеты и выходит за рамки обычного контекста межгосударственного вооруженного конфликта. И именно киберугрозы выходят сегодня на первый план для национальной безопасности любой страны, вовлекаемой в русло Четвертой индустриальной революции. Предлагая новые инструменты информационно-политического доминирования, кибервойна становится новой ареной, где происходит прорыв в эволюции глобальных конфликтов и отношений между государствами в целом, качественно меняя традиционное соотношение сил между ними и предоставляя негосударственным и/или ассиметричным игрокам невиданную ранее власть, позволяющую им играть важную роль в международных отношениях и бросать тем самым вызов региональным и глобальным державам.

Сегодня термин «кибервойна» активно используется в лексиконе специалистов по информационной безопасности, военных и политиков, однако среди них нет единого мнения относительно определения данного термина. Кибервойна может пониматься как синоним информационной войны, либо как ее конститутивный элемент, либо как ее разновидность[123]. Также некоторые выделяют кибервойны в отдельную категорию, связывая информационные войны сугубо с «операциями влияния», т.е. распространения дезинформации, компромата и пропаганды[124]. В любом случае кибервойны подразумевают активную борьбу за установление власти,

[123] Ventre D. Information Warfare. 2nd edition. London: ISTE Ltd and John Wiley & Sons Inc, 2016.

[124] Greenberg A. The Wired Guide to Cyberwar // Wired. 2019. 23d August. URL: https://www.wired.com/story/cyberwar-guide/ (дата обращения 31.08.2019).

влияния стратегического характера в киберпространстве, т.е. действия, направленные на ослабление противника в институциональном масштабе цифровыми средствами. Основными участниками кибервойн остаются национальные государства и их военные и секретные службы. В этом смысле кибервойну следует отличать от киберпреступности, т.е. взлома баз данных с целью извлечения прибыли и (промышленного) кибершпионажа, т.е. нелегального хакерства, но в интересах экономических игроков.

В целом можно выделить следующие основные точки зрения на природу современных кибервойн (Таб. 2.):

Критерий анализа	**Характеристика кибервойны**	**Источник**
Сущность кибервойны	Кибервойна – это ситуация конфликта между, по крайней мере, двумя политическими акторами, характеризующаяся враждебными намерениями и использованием кибератак против критически важной гражданской или военной инфраструктуры, с целью ослабить противника с точки зрения его обороноспособности или гражданского потенциала.	Liff A.P. Cyberwar: a New “Absolute Weapon”? The Proliferation of Cyber Warfare Capabilities and Interstate War” // Journal of Strategic Studies. 2012. Vol. 35 (3). P.401-428.
	Кибервойна представляет собой действия одного национального государства с проникновением в сети или компьютеры другого национального государства с целью разрушения или нанесения ущерба.	Clarke R. A., Knake R. K. Cyber War: The Next Threat to National Security and What to Do About It. New York: Harper Collins, 2010.
	Кибервойна – это противоправные и враждебные действия в киберпространстве, которые направлены против информационной инфраструктуры, информационных ресурсов и кибернетических систем для достижения определенной цели и осуществляемые с помощью программно-аппаратных средств воздействия	Антонович П.И. О современном понимании термина «кибервойна» // Вестник академии военных наук. 2011. № 2(35). С. 89-96.
Сравнение кибервойны и кинетической войны	Киберпространство – это не пространство прямого боестолкновения. Таким образом, кибервойна теряет фундамент для ведения классической войны и более не является театром военных действий, как это понимал Клаузевиц.	Libicki M. Why Cyberspace is not a Warfighting Domain // A Journal of Law and Policy for the Information Society. 2012. Vol. 8 (2). P. 325-340.

	Кибервойна сама по себе не может существовать. Это новое расширение конвенциональной войны, или ее составная часть. Чистая кибервойна, в которой используется только кибероружие, не эффективна. Будущие войны и столкновения будут смесью обычных или кинетических средств вооружения оружие и кибероружия, служащих для ослабления или усиления потенциала их пользователей.	Sommer P., Brown I. Reducing Systemic Cybersecurity Risk. Report for the OECD, Information Systems and Innovation Group. London: London School of Economics, 2011.
	Кибервойна – это техническое измерение информационной войны с использованием кибернетического потенциала против государства-противника и/или его общества; это такая же типичная война, но где, по крайней мере, один из компонентов базируется в компьютеризированном или цифровом поле.	Filiol É. Aspects opérationnels d'une cyberattaque: renseignement, planification et conduite // Ventre D. (ed.). Cyberguerre et guerre de l'information. Stratégies, règles, enjeux. Paris: Éditions Hermès Lavoisier, 2009. P. 319
	Ограниченная кибервойна, где информационная инфраструктура является одновременно целью, средствами и оружием атаки. Военные действия в физическом мире, если они есть, немногочисленны, но могут сопровождать кибератаку. Неограниченная кибервойна, которая больше не делает различий между гражданскими и военными целями, может сопровождаться последствиями в физическом мире, особенно с точки зрения летальности, а также иметь глубокие экономические и социальные разрушения.	Shimeall T., Williams Ph., Dunlevy C. Countering Cyber War // NATO Review, CERT Analysis Center of Carnegie Mellon University & NATO. 2001. Vol. 49 (4). P. 16-18.
Типологизация кибервойн	Современная информация и коммуникационные технологии породили феномен кибервойны, т.е. информационной войны, ведущейся в Интернете.	Trendle G. Cyberwar, "Internet Warfare in the Middle East" // The World Today. 2002. Vol. 58 (4). P. 7-8.
	Кибервойна – это комплекс скоординированных операций, осуществляемых в киберпространстве, с четко определенными целями с использованием цифровой информации и систем связи. Таким образом, кибервойна не включает в себя непосредственно идеи насилия, физическое уничтожение или смерть, но может способствовать этим явлениям.	Baud M. Cyberguerre: en quête d'une stratégie // Focus Stratégique. May 2013. No. 44. P. 47.

Характеристика практик кибервойны	Кибервойна чисто логически относится к военным действиям с целью разрушить, ослабить или нанести урон электронным ресурсам противника с помощью собственных компьютерных средств. Я лично предпочел бы, чтобы термин «информационные операции» относился бы ко всему спектру политических интервенций, начиная с кражи данных, обмана до причинения сбоев в работе электронных средств связи противника и их возможным уничтожением. Информационные операции в этом смысле делают неразличимым мирное время от войны.	Ventre D. An interview with Prof. Alan Chong (RSIS – Singapore) // Ecoles de Saint-Cyr Coëtquidan, Chair in Cyberdefense and Cybersecurity. 2013. Article No. III.2 URL: http://www.chaire-cyber.fr/IMG/pdf/article_3_2__chaire_cyberdefense.pdf (дата обращения 15.03.2020).
	Киберпространство имеет свои правила; например, в нем легко замаскировать свою идентичность и трудно предсказать или даже понять последствия (ущерб), вызванные киберстолкновением. Кибервойна – это всегда эксплуатация неопределенности.	Libicki M.C. Cyberdeterrence and Cyberwar // Rand Corporation monograph, 2009. P. 238. URL: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf (дата обращения 16.03.2020).
	Кибервойна состоит акций атаки и защиты внутри компьютерной сети (в более широком смысле, системы). Это определение специально исключает вредоносную эксплуатацию компьютерной сети, т.е. шпионаж, как отдельный феномен. Справедливо было бы сказать, что шпионаж – это не акт войны, т.к. не направлен на разрушение или сбой компьютерной системы.	Libicki M. Sub Rosa Cyber War // Czosseck Ch., Geers K. (eds) Cryptology and Information Security Series. Vol. 3. The Virtual Battlefield: Perspectives on Cyber Warfare. Amsterdam: IOS Press, 2011. P. 53-65.

Критика термина «кибервойна»	Нет единого определения того, что именно представляет собой кибервойну. Нападения на Эстонию в 2007, на Грузию в 2008 году, распространение вируса Stuxnet, современный шпионаж высокого уровня...все это может быть квалифицировано как кибервойна, включая и кибератаки, которые не имеют ничего общего с межгосударственными конфликтами, например, т.н. «хактивизм» или утечки информации в WikiLeaks, или поддержка революций Арабской весны 2011 года. Все это подразумевает, что понятие «кибервойна» больше не ограничено деятельностью национальных государств. Поэтому из-за отсутствия общего определения, большинство стран-членов ЕС стремятся избегать использования термина «кибервойна» в официальных документах, предпочитая нейтральные выражения, такие как «кибершпионаж», «кибератаки» или «киберзащита».	Klimburg A. Tirmaa-Klaar H. Cybersecurity and Cyberpower: Concepts, Conditions, and Capabilities for Cooperation for Action within the EU // Study for Directorate-General for external policies of the Union, European Parliarment. 2011. P. 11. URL: https://www.europarl.europa.eu/RegData/etudes/STUD/2011/433828/EXPO-SEDE_ET(2011)433828_EN.pdf (дата обращения 12.02.2020).

Таб. 2. Современные подходы к анализу природы кибервойны

Разносторонность подобных выводов, тем не менее, объединяет общее понимание невозможности сведения природы кибервойн к классическому пониманию военных действий в духе Клаузевица, где основным условием является открытая борьба с потенциальным летальным исходом для противника. Кибервойны – это всегда скрытое от глаз информационно-политическое насилие, ведущееся тайным образом и не имеющее прямых летальных последствий для «живой силы» противника. Стороны, находящиеся в конфликте, зачастую или не признают себя в состоянии войны, или отрицают факт, что были кем-то атакованы и понесли ущерб. Такое новое состояние войны возможно благодаря двум причинам: невидимость понесенного ущерба и невозможность или сложность юридического установления источника кибератаки.

Социологический анализ показывает, что подобная ситуация является отражением более глубоких социальных изменений. В этом смысле кибервойны наиболее ярким образом воплощают черты «текучей современности» (З. Бауман), которая определяется невозможностью проведения границы между войной и миром. Как указывает по этому поводу З. Бауман, низко-интенсивные, невидимые и закамуфлированные войны приводят к «оруэллизации» мирового порядка, когда антиутопический лозунг «Война – это мир» из романа Дж. Оруэлла «1984» превращается в новый – «Мир – это война». При этом сама война становится «текучим злом», которое более не укладывается в традиционные гуманистические определения добра и зла, а становится метаморфной, скользкой силой, сочетающей ложь, манипуляции и грубость[125].

Таким образом, в соответствии с описанными ранее стратегическими действиями в киберпространстве с нашей точки зрения *метаморфная природа* кибервойны, особенно в форме *сетевой войны* (подробнее см. в следующей главе), может включать в себя не только кибератаки, но и кибердавление и рефлексивное киберуправление. Каждый из элементов кибервойны обладает своим набором основных средств ведения войны в киберпространстве.

В рамках рефлексивного киберуправления происходит трансформация понимания кибервойны и изменение постановки задач для решения поставленных целей в противоборстве. Если при кибератаках главной задачей считается подавление элементов информационной инфраструктуры, то при рефлексивном киберуправлении осуществляется передача информационных потоков и их искажение, формирование дезинформации и ее распространение и пр.

Таким образом, при рефлексивном киберуправлении происходит манипулирование общественным сознанием, в частности, с целью

[125] Bauman Z., Donskis L. Liquid Evil. Cambridge, England: Polity Press, 2016.

формирования политической напряженности, дезинформация граждан о работе органов государственного управления. Это, в конечном счете, приводит к провоцированию столкновений религиозного, социально-политического и национального характера, подрыву авторитета власти, нанесению ущерба жизненно важным интересам государства в разных областях.

Примером может служить резко ухудшившиеся ситуации внутри государств Северной Африки и Ближнего Востока в 2010-2011 гг. После финансового кризиса 2008 г. американские СМИ развернули кампанию, ориентированную на «вещание» беспрецедентной критики внешней и внутренней политики представителей власти в указанных регионах. В кибернетическом пространстве населению регионов навязывалась идея о поддержке «народных революций» и «неизбежности перемен».[126] Исходя из этого, можно говорить о хорошо организованной кибернетической стратегической операции, направленной на вмешательство руководства США в управление государствами Северной Африки и Ближнего Востока.

Формирование в рамках рефлексивного киберуправления информационной монополии на основные события в конкретных регионах в сочетании с блокированием информационного потока противников приводит к получению информационного превосходства в киберпространстве. Таким образом, в настоящее время для достижения информационного превосходства в киберпространстве продолжаются активные действия по повышению эффективности т.н. «специальных информационных операций».

В политике США реализация рефлексивного киберуправления осуществляется по принципу «international public information» (международного общественного информирования), проводимого, в частности, с помощью социальных сетей. Среди инструментов

[126] Pincus W. Pentagon Reviewing Strategic Information Operations // The Washington Post. 2009. 27th December. URL: https://www.washingtonpost.com/wp-dyn/content/article/2009/12/26/AR2009122601462.html (дата обращения 29.08.2019).

рефлексивного киберуправления при проявлении «твердой силы» можно также выделить фальсификацию, имитацию, использование слухов, представление агрессора в качестве жертвы и пр. К примеру, при конфликте Южной Осети и Грузии 8 августа 2008 г. британский телеканал «Sky News» в новостных выпусках транслировал, что «Россия ведет обстрел территории Южной Осетии, которая входит в состав Грузии». Еще одним примером проявления «твердой силы» выступают многочисленные информационные потоки с выступлением очевидцев и «жертв» ведущихся боевых конфликтов: при конфликте между Южной Осетией и Грузией на телевидении Италии показывали старушку-грузинку, которая потеряла дом, в результате обстрела русскими солдатами; относительно Сирийского конфликта телеканал США неоднократно демонстрировал фото детей, которые пострадали от химического оружия.

Стратегия «наклеивания ярлыков» как инструмент рефлексивного киберуправления заключается в эксплуатации стереотипов и предрассудков граждан через наклеивание соответствующего «ярлыка». Стоит при этом подчеркнуть, что «ярлыком» выступает квалификация объекта как нечто, чего аудитория боится, находит отрицательным и пр.

В стратегии «принуждающая пропаганда» используются выражения и слова, которые имеют принуждающий характер. К примеру, в ноябре 2015 г. на севере Польши были расклеены листовки, пропагандирующие преимущества вхождения в состав Польши Украины.

В рамках настоящего исследования представляется интересным рассмотреть еще один инструмент ведения кибервойны в рамках рефлексивного киберуправления – «троллинг». Он представляет собой ряд целенаправленных действий в киберпространстве, а именно: обман, высмеивание, провоцирование с целью вызвать агрессию объекта троллинга. Этим занимаются специально проинструктированные команды интернет-пользователей, которые иногда называются «фабриками троллей». Обычно троллинг обостряет любую коммуникативную ситуацию.

Основы троллинга как инструмента ведения кибервойны в чем-то перекликаются с принципами военной пропаганды (Рис. 4.).

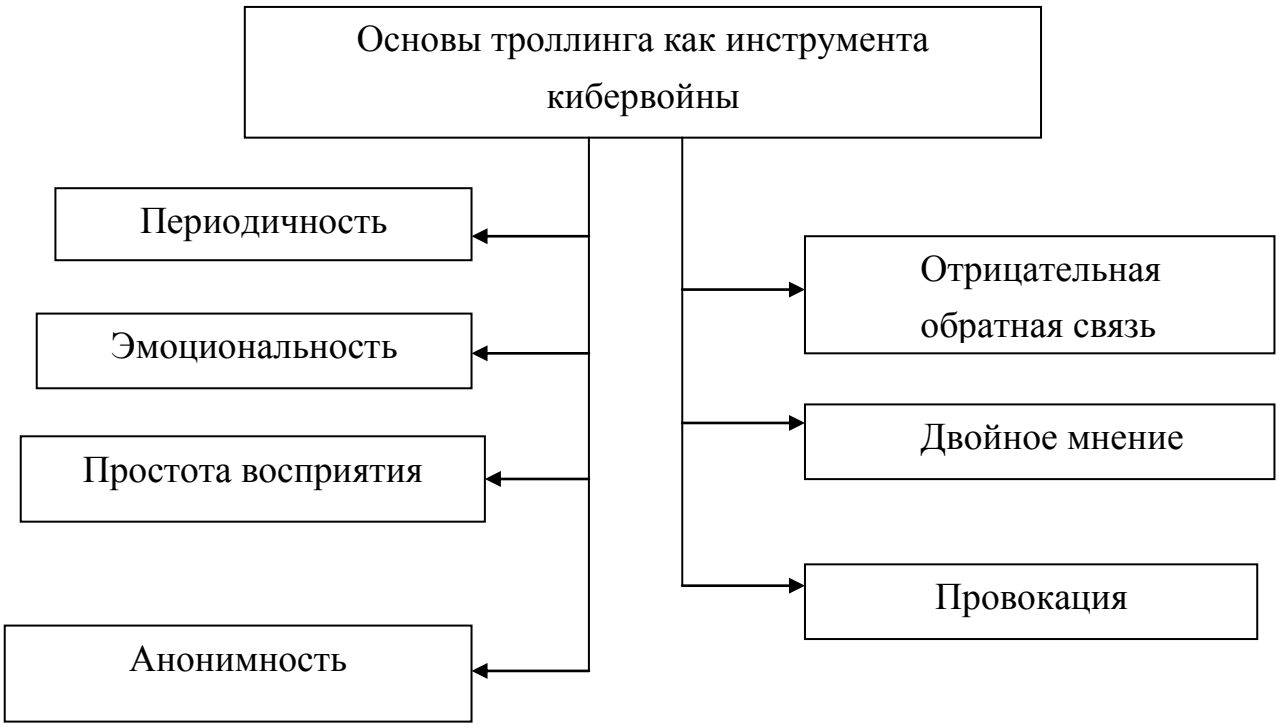


Рис. 4. Основные принципы троллинга как инструмента кибервойны

Во время президентства Барака Обамы появились так называемые «фабрики троллей». Ранними исследованиями фабрик троллей стали презентация методов сетевой пропаганды, подготовленная в 2012 г. Калифорнийской ассоциацией стоматологов, и книга 2014 г. журналистки Ш. Атткинсон о многочисленных нарушениях и скандалах внутри администрации Белого дома.[127]

Другой суперпак, American Bridge 21st Century, принадлежащий Дэвиду Броку, поддерживавшему семейство Клинтон долгие годы, потратил один миллион долларов на исправление комментариев пользователей в социальных сетях. Эту инициативу американские СМИ прозвали операцией троллей «Correct the Record». Суперпак сенатора Джеба

[127]Attkisson S. Stonewalled: My Fight for Truth Against the Forces of Obstruction, Intimidation, and Harassment in Obama's Washington. New York: Harper, 2014.

Буша Right to Rise USA был замечен в агрессивном троллинге сенатора Марко Рубио. Позже журналистское расследование выявило, что суперпак Джеба Буша финансировали китайцы, что стало в Америке причиной скандала.

В 2016 г. под кампанию Дональда Трампа был создан Great America Pac. Его основал специалист по политическому маркетингу, республиканец Эрик Бич, а крупнейшим донором стал израильско-американский бизнесмен, бывший директор студии Marvel Исаак Перлмуттер. Первым продуктом этого суперпака явилась реклама под названием «Враги» – в ролике бывший морской пехотинец Карл Хигби, спекулируя на массовом убийстве в ночном гей-клубе в Орландо в июне 2016 года, призывал ради защиты интересов США и борьбы с терроризмом голосовать за Трампа. На Хиллари Клинтон в выборах 2016 года работал суперпак Priorities USA Action, за которым стояли бывшие помощники Обамы Билл Бертон и Шон Свини. Они собрали 60 миллионов, и почти все эти деньги, согласно отчёту, были потрачены на «внутренние расходы». Демократам в борьбе с Трампом помогал и суперпак Women Vote!

Если суперпаки в основном дискредитируют конкурентов во внутренней политике, то для внешнего вещания созданы сотни структур, атакующих другие государства, если те не следуют политической линии Вашингтона. «Новым словом» здесь стали создание видимости борьбы с ложными (фейковыми) новостями и «работа по разоблачению проявлений авторитаризма». Ещё один ресурс под названием «Полиграф» имеет сайт на русском языке, где систематически критикуется, ставится под сомнение и опровергается информация, идущая из России.

Основными инструментами «мягкой силы» при осуществлении рефлексивного киберуправления можно считать формирование информационного поля вокруг государства, осуждение ведущими мировыми политиками действий политической системы, политического режима. Стоит

подчеркнуть особую роль деятельности НКО в части оказания такого информационного влияния.

Таким образом, существующие инструменты рефлексивного киберуправления направлены на смену парадигм восприятия и понимания обществом окружающего мира и ситуации в существующих политических и военных конфликтах.

И, наконец, третьим типом осуществления кибернетической войны считается оказание кибердавления, для чего используется «цифровая дипломатия»[128].

Также США являются активным игроком по использованию инструментов кибернетического давления «гибридной силы». Так, с 2006 г. США осуществляют реализацию проекта Digital Outreach Team, который направлен на ведение «войны идей». Основная цель ведения такой войны состоит в исследовании политических и общественных дискуссий в социальных сетях и блогах, а также дальнейшем широкомасштабном распространении и конструировании идей, ценностей и смыслов, которые требуются для формирования альтернативных моделей восприятия политической и социальной реальности.

Таким образом, современные процессы глобализации, происходящие в мировом пространстве, а также существующее военное и политическое противостояние в кибернетическом пространстве невозможны без системной работы в кибернетическом пространстве с использованием соответствующих инструментов борьбы.

Опираясь на стратегические действия в киберпространстве было предложено выделить в структуре кибернетической войны как формы информационно-политического насилия кибератаки, кибердавление и рефлексивное киберуправление. Каждый элемент кибервойны может

---

[128] Володенков С.В., Митева В.В. Сетевые информационные войны в современных условиях: основные акторы и стратегии // PolitBook. 2016. №3. С. 18-35.

использовать конкретный набор основных средств ведения войны в киберпространстве.

Если при кибератаках главной задачей считается подавление элементов информационной инфраструктуры, то при рефлексивном киберуправлении осуществляется передача информационных потоков и их искажение, формирование дезинформации и ее распространение и пр. В свою очередь, киберуправление предполагает исследование политических и общественных дискуссий в социальных сетях и блогах, а также дальнейшее широкомасштабное распространение и конструирование идей, ценностей и смыслов, которые требуются для формирования альтернативных моделей восприятия политической и социальной реальности.

Выводы к главе 1.

1) Дана характеристика современному цифровому киберпространству, раскрыта суть его дифференциации: мировые цифровые гиганты США и Китая влияют на характер междунарожных отношений и на международную безопасность. По нашему убеждению, в целях укрепления национальной безопасности, России необходимо создать свое собственное цифровое облако. Власть в киберпространстве имеет *ацентричный характер:* нет валидных критерией для определения общепринятого кибергегемона или «отстающих».

2) Киберпространство функционирует за счет синтеза агентства и актантов, последствия чего амбивалентны: с одной стороны, это благо для многих людей, получающих доступ к новому знанию; но с другой стороны, оно может быть использовано против людей – в нем инсцинируются страхи, формируется «постправда», что драматизирует их сознание.

3) Кибератаки позволяют конвертировать мифы, фейки, «постправду» в реальные экономические и политические капиталы. Используя

терминологию П. Бурдье, киберпространство является *цифровым полем,* на котором киберакторы ведут борьбу.

4) Киберизация производит новые сложные риски для международного порядка, угрожающие национальной безопасности.

5) Показаны две тенденции в области современных международных отношений: смещение суверенитета и власти государств в область киберпространства и нарастающая зависимость их от цифровых технологий, а также диффузия кибервласти между государственными и негосударственными акторами, что вместе ведет к размыванию и ослаблению национальной безопасности как таковой.

6) По своей природе политическая власть в киберпространстве отличается от «классической» власти, предполагающей, навязывание воли посредством права, авторитета или традиций (М. Вебер) или способность класса, владеющими основными средствами производства, осуществлять социально-политическое господство (К. Маркс, Ф. Энгельс). Ныне “собственники средств определения” смыслов (У. Бек) фактически владеют данной политической властью, она позволяет им выражать свои политические интересы. Соответственно, кибервласть представляет собой *сложную систему ресурсов, структурированных вокруг производства и обмена цифровой информации, а также контроля над ней*. Её сложность, в частности, проявляется в том, ресурсы оказывают *нелинейное действие*: сравнительно небольшие факторы могут быть весьма значимыми по своим воздействиям на социум. Вместе с тем, кибервласть постепенно трансформируется во властную *гегемонию*, т.е. супервласть, которая не ограничивается контролем над сугубо кибернетическими ресурсами, включающими в себя структурные уровни киберпространства, обозначенные нами в предыдущем параграфе, но также вбирает в себя человеческие, финансовые, экономические, символические, культурные и политические ресурсы, создаваемые или задействованные в этой системе.

7) «Цифровая дипломатия» подразумевает весьма широкий набор управленческих задач — и традиционных, и новых, но решаемых с помощью киберинструментов в режиме онлайн. В ситуации борьбы за кибервласть цифровая дипломатия включает в себя элементы кибердавления, т.е. стремится к неявному противостоянию с противником с целью создания благоприятных условий для реализации реальных политических действий в своих интересах.

8) Национальная безопасность в современных условиях во все большей степени определяется капитализированием кибервласти. Страны, которые достигнут технологического и политического превосходства в киберпространстве, будут претендовать на мировое господство. Битва за кибервласть между державами будет важнейшей характеристикой ближайших лет развития международных отношений.

9) Изменилась эффективность использования тех или иных инструментов насилия – они становятся информационно-цифровыми и надзорно-цифровыми. Для победы в настоящее время необходимо с помощью «игры» кодами сигнификациии принудить правящую элиту противника принять систему ценностей, интересов и норм, что возможно сделать не только с помощью военной силы, но, прежде всего, с помощью невоенных инструментов силовой политики – информационно-когнитивных средств, цифрового надзора, манипулирования общественного сознания с помощью симулякров и симуляций.

ГЛАВА 2. СОЦИАЛЬНЫЕ СЕТИ КАК СТРАТЕГИЧЕСКИЙ РЕСУРС КИБЕРВОЙНЫ

2.1. Социальные сети как фактор стратегической безопасности

Стратегическое значение онлайновых социальных сетей напрямую связано с формированием сетевого общества в целом. Как указывает создатель теории информационального общества М. Кастельс, «...новая коммуникационная система, все более говорящая на универсальном цифровом языке, одновременно интегрирует в глобальном масштабе производство и распространение слов, звуков и изображений в нашей культуре и приспосабливает их к персональным вкусам и настроениям индивидов. Интерактивные компьютерные сети растут по экспоненте, создавая новые формы и каналы коммуникации, формируя жизнь и формируясь жизнью в одно и то же время»[129]. В работе «Галактика Интернет» исследователь отмечает центральную роль Интернета в переходе к новому, «сетевому» обществу: «вообще-то сети – это достаточно старые формы материализации человеческой деятельности, однако в наши дни они обрели новую жизнь в результате превращения их в информационные сети, объединенные Интернетом»[130]. Таким образом, именно Интернет и онлайновые социальные сети в частности становятся технологическим и социальным базисом развития новой экономики, новой политики и ведения новых войн.

Именно эта принципиально новая роль интернета и социальных сетей в качестве инструмента силовой политики государств, обладающих, прежде всего, доминирующими возможностями в технологической области, является важнейшим фактором, который влияет на системную безопасность России.

---

[129] Кастельс М. Информационное эпоха: экономика, общество, культура. М.: Изд-во Высшей школы экономики, 2000. С. 26.

[130] Кастельс М. Галактика Интернет: Размышления об Интернете, бизнесе и обществе. Екатеринбург: У-Фактория, 2004. С. 13.

Само по себе понятие «социальная сеть», впервые введенное в социальную науку Дж. Барнсом в 1954 г., включает некий существующий и потенциальный круг знакомых человека и социальных связей между этими людьми[131]. В современном цифровом мире социальные сети – это платформа, онлайн-сервис или веб-сайт, предназначенные для построения, отражения и организации социальных связей людей.

Соответственно, если потенциальные участники такого круга расширяются до максимального числа (например, пользующихся в общении языком или заинтересованных в том или ином общении), то и влияние этих сетей в качестве ИО увеличивается: в случае создания общедоступного интернета для всех жителей Земли потенциальных объектов такого информационного воздействия станет столько же сколько и пользователей интернета.

Так, в настоящее время частные компании, структуры гражданского общества, часто при поддержке государства, ведут разработку и внедрение таких проектов, как:

– фонд Internet.org, созданный Facebook, стремится подключить к интернету более 5 млрд. человек и обеспечить доступ к Сети в удалённых районах;

– проекты сверхбыстрого интернета со скоростью до 10 Гб/сек и даже до 1,4 Тб/сек, реализуемые в рамках нескольких программ;

– проекты сетей обмена данными на основе дополняющих или альтернативных современному Интернету технологий[132].

---

[131] Джон Барнс, австрало-британский социальный антрополог, изучая классовую структуру в одном норвежском округе, пришел к выводу о необходимости выделения в социальной организации местных сообществ помимо административной и экономической систем еще и социальных сетей (networks): “Каждый человек имеет определенный круг друзей, а эти друзья имеют, в свою очередь, собственных друзей. Некоторые из друзей одного человека знают друг друга, другие – нет. Я нашел удобным говорить о такого рода полях как о сетях. Под этим мне видится система точек, некоторые из которых соединены между собой. Точками этой системы являются люди, а линии соединения этих точек указывают, какие люди взаимодействуют друг с другом» [Barnes J. A. Class and committees in a Norwegian Island Parish // Human Relations. 1954. Vol.7. P. 43]. Социальные сети, по Барнсу, отличаются тем, что не имеют координации, физических структур и границ, а также гораздо разнообразнее, чем родственные сети (web of kinship).

[132] Демидов О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества. М.: Алпина Паблишер, 2016. С. 16.

При этом, в отличие от сложившихся социальных структур, представляющих достаточно жесткий «каркас» устоявшихся социальных отношений, социальные сети относятся к числу гибких структур, или «мягких тканей», способных управлять малыми социальными взаимодействиями отдельных групп и даже личностей. Поэтому контролировать подобные связи практически невозможно, а влияние тех или иных сетей на эти группы всегда будет находиться у тех, кто управляет данной социальной сетью. Попытки ограничить или даже запретить те или иные социальные сети, предпринимаемые государственными институтами, как правило, малоэффективны – участники общения в Интернете находят массу обходных путей для обмена информацией.

Различают, как правило, два типа социальных сетей:

– личная или эгоцентрическая (personal, egocentric) сеть, имеющая центром конкретного пользователя. Пример: Рис. 5.

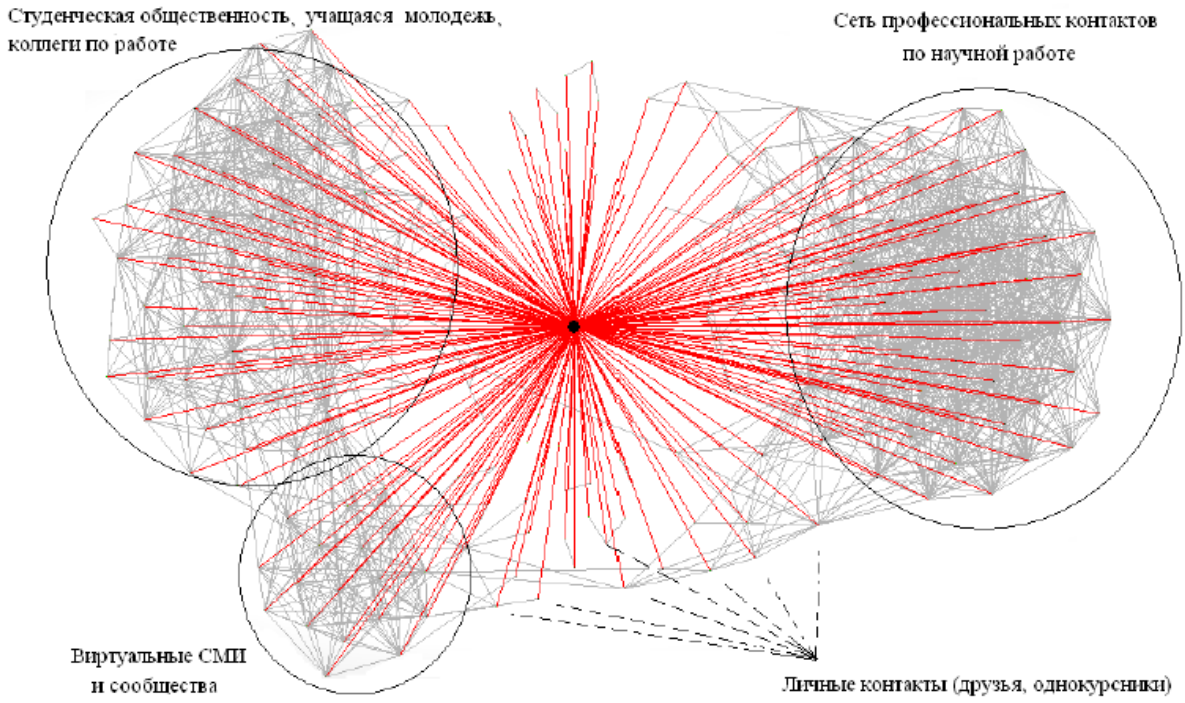


Рис. 5. Визуализация личного аккаунта в одной из онлайновых социальных сетей[133]

[133] Воронкин А.С. Социальные сети: эволюция, структура, анализ // Образовательные технологии и общество. 2014. № 1. С. 650-675. С. 669.

– целая или социоцентрическая (whole, sociocentric) сеть, объединяющая миллионы пользователей в горизонтальную гетерархическую структуру. Пример: Рис.6.

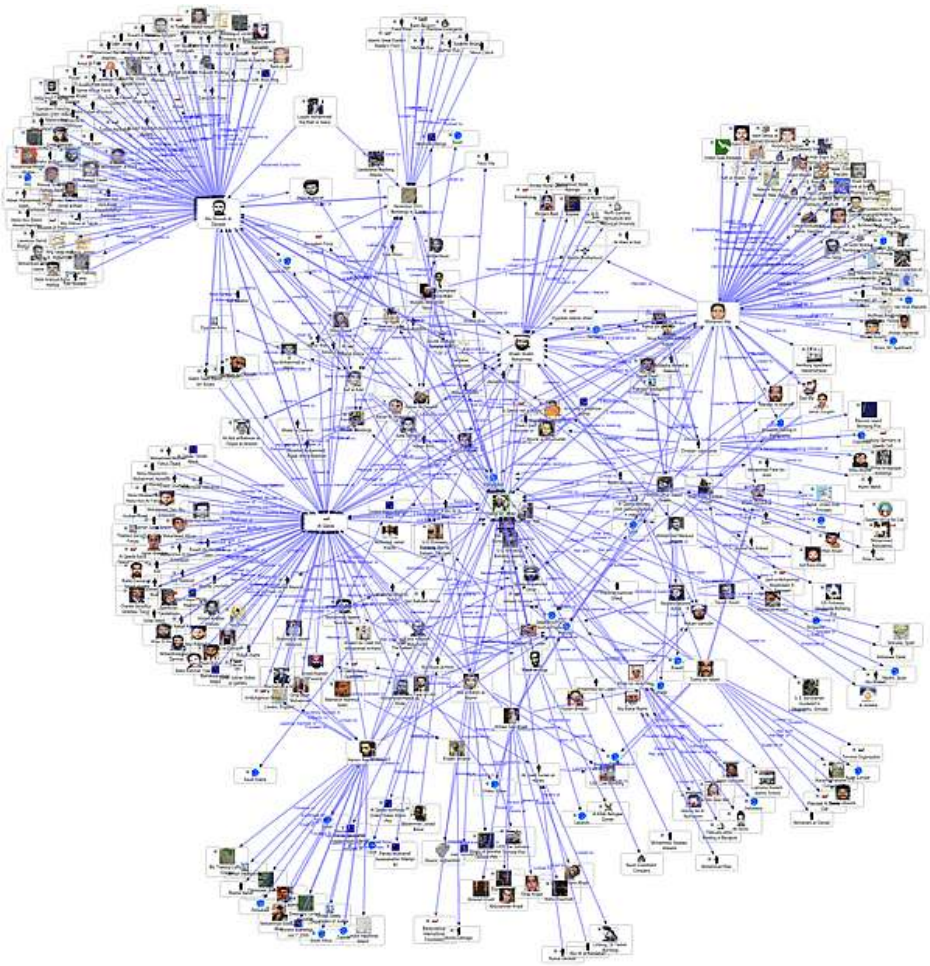


Рис. 6. Визуализация графов фрагмента онлайновой социальной сети[134]

С точки зрения противоборствующих акторов в военно-политической или иной международной области, любая из таких сетей является как средством силовой борьбы, так и потенциальным объектом воздействия.

Политическая сущность современных онлайновых социальных сетей не всегда очевидна. Это происходит потому, что политическая атрибутивность социальных сетей далеко не всегда очевидна. Более того, порой она тщательно скрывается теми, кто их контролирует. Сознательно и настойчиво

[134] Social Network Analysis [Электронный ресурс] // URL: https://researchimaginings.com/2015/03/02/social-network-analysis/ (дата обращения 04.03.2020).

создаётся ложное убеждение в том, что с политической точки зрения контролировать и использовать социальные сети невозможно. Это утверждение – искажение политической сущности социальных сетей, которые вполне успешно не только создаются, но и управляются (хотя и не всегда открыто и публично). Однако, политико-идеологические последствия развития интернета и, в частности, социальных сетей в полной мере отражает следующую тенденцию: политическая сущность социальных сетей не просто присутствует, но и делает их идеологическим средством влияния и, порой, политического принуждения.

Для характеристики политической природы социальных сетей как инструмента стратегического влияния используется понятие *сетевой войны*[135]. Последняя представляет собой не-военную разновидность кибервойны. Ее основная задача состоит в изменении (от модификации до трансформации) знания таргетированной аудитории о том, что эта аудитория знает о себе или об окружающем мире. Другими словами, это влияние на общественное мнение или мнение элит, а, возможно, и то, и другое. Конкретные тактики сетевых войн будут рассмотрены далее в работе, но в целом они включают в себя мягкие и гибридные методы работы с информацией – пропаганда, психологические кампании, политические и культурные диверсии, обман, препятствие работы местных СМИ, инфильтрация цифровых потокой в компьютерных сетях и базах данных, внедрение политического раскола и оппозиционных настроений среди пользователей. Если цели сетевой войны включают в себя т.н. CI3 (command, control, communication and intelligence), т.е. системы управления, то она становится частью кибервойны.

Дж. Арквилла и Д. Ронфельдт выделяют такие организационные черты сетевых войн:

---

[135] Arquilla J., Ronfeldt D. Networks and Netwars. The Future of Terror, Crime and Militancy. Santa Monica: Rand Corporation, 2001.

– участники сетевой войны представлены как индивидами, так и малыми группами;

– участники осуществляют дистанционное общение для координации своей деятельности и проведения операций;

– структура участников формально не определена; отсутствует иерархия и централизация.

Этот тип войны, по мнению авторов, максимально адаптирован к использованию такими аморфными группировками, как «хактивисты», представленные индивидуальными хакерами или международными хакерскими группами, состоящими из отдельных лиц, живущих вдалеке друг от друга на самых разных территориях и осуществляющих информационно-политическое насилие в стане противника.

Одним из наиболее ранних примеров разворачивания сетевой войны можно считать движение сапатистов в Мексике в 1994 г. Это леворадикальное движение, организованное т.н. Сапатистской армией национального освобождения (САНО) в интересах притесняемых мексиканских индейцев и бедняков, потерпев неудачу вооруженного восстания в начале 1994 г., прибегло к другой тактике, а именно использованию Интернета для мобилизации общественного мнения во всем мире в свою пользу в борьбе с экономической политикой мексиканского правительства. В итоге, САНО привлекло внимание лидеров и неправительственных организаций многих стран, институционализировалось и стало частью антиглобалистсткого движения. Главная инновация сапатистов в их политическом успехе была ставка на инструментализацию *симулякрной* природы медийного пространства. Как отмечает один из активистов движения Д. Гравина, «самое главное – это не само событие, а спектакль, который устраиваете по поводу этого события в медиа…мы пытались завернуть то, что с нами происходило, в театрально-поэтическую

обертку, это и есть идея Сапатиста»[136]. Революция в коммуникации серьезно изменила баланс сил от традиционных СМИ к интернет-аудитории. Это позволило сапатистской идее обрести успех, открывая новые каналы политического влияния и давая мощный импульс для политического участия обыкновенных граждан. В итоге, сапатизм от местечкового вооруженного движения с определенной иерархией внутри переродился в глобальный сетевой феномен информационной эпохи – с медийной инфраструктурой, политиками, организациями, акциями поддержки по всему миру.

Таким образом, концепция сетевой войны отражает трансформацию социальных отношений благодаря развитию новых цифровых коммуникационных сетей. Пример с движением сапатистов позволяет выделить некоторые важные характеристики нового типа информационно-политического влияния:

– правильный выбор стратегии коммуникации с аудиторией становится главным условием достижения целей;

– управление впечатлениями важнее реальных событий;

– использование ресурсов на одном направлении работы является залогом успеха (тактика «роения»);

– психо-социальное воздействие важнее физического разрушения;

– участниками сетевых войн могут быть совершенно разные акторы: политические деятели, террористы, революционеры, хактивисты, хакеры, преступники, пацифисты и т.п.;

– информационные технологии могут представлять реальную угрозу дестабилизации на государственном или институциональном уровне;

– сетевые войны неизбежны и не все общества/государства готовы к этому.

Социальные сети предоставляют огромные возможности для тех, кто их контролирует, для политико-силового использования в глобальном

[136] Meikle G. Networks of Influence: Internet Activism in Australia and beyond // G. Goggin (ed.) Virtual Nation: the Internet in Australia. Sydney: UNSW Press, 2004. P. 73-87.

противоборстве. Манипулятивные термины – один из способов насаждения массовых стереотипов. В частности, А.М. Цуладзе анализирует такой прием, как уловки. Они не всегда заметны невооруженным глазом, но очень действенны[137].

Таким образом, социальные сети стали мощным инструментом для сознательной политики дезинформации и искажения реальности, которые могут менять достаточно быстро и в глобальном масштабе информационно-когнитивный фон в стране и регионах. Мировые политические и культурно-духовные лидеры очень быстро осознали эти огромные возможности Интернета как фактора «силового принуждения»[138]. Более того, многие политики и учёные стали говорить о «неизбежности затяжного политического конфликта с Западом по поводу роли России на постсоветском пространстве...»[139].

Среди силовых средств противоборства, как показала практика последних двух десятилетий, особенно эффективными оказались именно информационно-психологические средства, используемые в онлайновых социальных сетях.

Причём, особенно важное значение в последние годы социальные сети приобретают в качестве информационного оружия, которому Л.В. Воронцов, например, предлагает следующее определение: «информационное оружие – это совокупность средств, методов и способов, специально созданных для нанесения ущерба информационной сфере, а также процессам и системам, функционирующим на основе информации»[140]. Ещё шире на функцию ИО рассматривает И.Н. Панарин, который определяет его, как «устройства и средства, предназначенные для нанесения противоборствующей стороне максимального урона в ходе информационной борьбы (путем опасных

---

[137] Цуладзе А.М. Политические манипуляции, или покорение толпы. М.: Книжный дом «Университет», 1999.

[138] Стратегическое сдерживание: новый тренд и выбор российской политики / А.И. Подберёзкин, М.В. Александров, К.П. Боришполец и др. М.: МГИМО-Университет, 2019. С. 511- 566.

[139] Мир 2035. Глобальный прогноз / под ред. акад. А.А. Дынкина / ИМЭМО РАН. М.: Магистр, 2017. С. 50.

[140] Манойло А.В. Государственная информационная политика в особых условиях. М.: МИФИ, 2003.

информационных воздействий)»[141]. Целью применения информационного оружия является причинение разрушительного воздействия на экономическую, политическую, социальную области функционирования государства, а также психологическое воздействие на население, цель которого чаще всего состоит в дестабилизации общества и программирования общественных настроений.

Особенностями ведения новых информационных войн является невероятная *метаморфность* самого применяемого оружия. Это обусловлено рядом его свойств (Рис. 7.):



Рис. 7. Характерные свойства информационного оружия [142]

[141] Панарин И.И. Типология информационной войны. М.: КСП, 2003.

[142] Систематизировано по: Гриняев С.Н. Поле битвы-киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны. М.: Харвест, 2004. С. 97-99.

Также важным свойством информационного оружия является его потенциальная превентивность. Этот потенциал используется сегодня в концепции глобального информационного лидерства США, которая известна также как «программирующее лидерство». Данная стратегия состоит в выдвижении эффективной информационной повестки дня, «то есть круга проблем, определяющих спектр и направленность совместных действий США с государствами – объектами данной стратегии, а затем в реализации заложенного в этой повестке потенциала в интересах Соединенных Штатов»[143]. Ярким примером реализации данной стратегии является информационный вброс в глобальный или региональный политический дискурс таких идей, как «борьба с терроризмом», «столкновение цивилизаций», «демократические ценности» и т. п., послужившие в свое время основой для последующего программирования реальных боевых операций в Югославии, Афганистане, Ираке, а также в арабских странах в рамках т.н. «Арабской весны», а также на постсоветстком пространстве (Грузия, Молдова, Украина). Благодоря информационному оружию возможно достигнуть те или иные цели посредством драматизации сознания противника. При этом сохраняются материальные ценности и окружающая среда. В этом эффективность информационного оружия. Более того, информационное оружие обладает высокими темпами модификации и совершенствования, которые превышают темпы развития средств защиты и противодействия ему.

Неслучайно, наиболее эффективно информационное оружие используется в тех странах, где уже имеет место социальная напряженность, недовольство граждан правительством, межнациональные и классовые конфликты. Как правило, в качестве каналов распространения информационного оружия используются именно социальные сети, которые обладают мгновенным доступом к максимально широкой аудитории. Так, по

[143] Троицкий М.А. Концепция "программирующего лидерства" в евроатлантической стратегии США // Pro et Contra. 2002. № 4. С.86-103.

данным ресурсов «We Are Social» и «Hootsuite» охват активных пользователей социальных сетей в мире и в России примерно равен – соответственно 49 и 48% населения[144].

Специалисты Министерства обороны РФ на конференции ООН по разоружению в 2019 году высказывали позицию, что правительство может продвигать идеи в Интернете с целью подорвать правительство другой страны – даже во имя демократической реформы – и это следует квалифицировать как «агрессию». Таким образом, российские власти считают правильным ввести ряд ограничений использования Интернета через международное законодательство, чтобы исключить свержение законного правительства. При этом США последовательно выступают против подобных усилий по ограничению интернет-общения. Дебаты по вопросам управления Интернетом и контроля над кибероружием имеют место и в Международном союзе электросвязи. Генеральный секретарь МСЭ Хамадун Туре считает целью развития Интернета достижение киберустойчивости, в том числе через международное сотрудничество в области ограничения распространения кибероружия и – в перспективе – полного разоружения в киберпространстве[145]. Однако, с социологической точки зрения ускоряющаяся рефлексивная модернизация и глобализация общества на основе новых технологий и экспертных знаний не дает шансов на решение этого вопроса в ближайшей перспективе, поскольку вопрос мирового распределения военной власти является одним из центральных столпов международных отношений в эпоху модерна и нынешнего радикального модерна, в частности. И стратегический потенциал Интернета и онлайновых социальных сетей, скорее всего, будет только возрастать в условиях ядерного сдерживания. Как указывает Э. Гидденс, «мир без войн – это утопия», ибо индустрия войны будет приобретать лишь все новые и

---

[144] Digital 2020 [Электронный ресурс] // URL: https://hootsuite.com/resources/digital-2020 (дата обращения 03.03.2020).

[145] Туре Х. Киберустойчивость: суть мира в киберпространстве // Индекс безопасности. №1 (104). Весна 2013. С. 207-212.

новые формы[146], поэтому власть и насилие будут существовать до тех пор, пока национальные государства и национальные интересы будут иметь вес на мировой политической арене.

2.2. Факторы политической мобилизации в социальных сетях

Использование социальных сетей сегодня активно способствует достижению тактических задач по мобилизации масс как движущей силы социальных движений и политических протестов. Многие исследователи, анализируя динамику различных массовых движений, говорят о том, что их успех напрямую связан с использованием разных политических тактик именно в социальных сетях.[147]

В контексте изучения проблемы информационно-политического насилия интересны классические исследования Т.Р. Гарра, который подробно изучает данный феномен в известной книге «Почему люди бунтуют»[148]. В его работе отмечается, что исследователями уделяется много внимания тому, как обиды и депривации граждан могут приводить к мобилизации протеста, а также процессу ее организации. На основе этого Гарр в своем исследовании источником насилия и агрессии видит относительную депривацию, под которой понимает схему восприятия группами граждан жизненных обстоятельств. Относительная депривация обусловливает формирование неудовлетворенности граждан и их фрустрации. Таким образом, если у граждан наблюдается расхождение между их потребностями в тех или иных благах и условиями их реализации, то у них формируется фрустрация, являющаяся одним из возможных факторов формирования политического насилия. Ссылаясь на Гарра, в рамках настоящего исследования под относительной депривацией автор будет понимать психологическую

[146] Гидденс Э. Последствия современности. М.: «Праксис», 2011. С. 200-203.

[147] Passy F., Monsch G.A. Do Social Networks Really Matter in Contentious Politics? // Social Movement Studies. 2014. Vol. 13 (1). P. 22-47.; Baumer D. C., Van Horn C. E. Politics and Public Policy: Strategic Actors and Policy Domains, 4th ed. Thousand Oaks, CA: SAGE Publications, Inc, 2014.

[148] Гарр Т. Почему люди бунтуют. СПб.: Питер, 2005.

неудовлетворенность граждан, которая выступает причиной будущих политических акций и протестов.

Помимо относительной депривации Гарр выделяет следующие основные факторы возможности политических протестов:

– баланс между протестными способностями граждан и способностью регулирования таких действий со стороны правительства;

– убежденность в оправданности и выгоде совершаемых протестных акций.

В своей работе Гарр использует термин «политическое насилие», под которым он понимает применение протестующими силовых акций или высказывание угрозы их применения с целью противостояния нежелательному курсу политики или выражения собственных политических интересов.

Однако, сегодня такого подхода явно недостаточно, поскольку в нем не учитывается высокий уровень влияния новых медиа, которые могут быть использованы для мобилизации людей без опоры на реальную депривацию.

В современных исследованиях нет единого мнения о том, как интернет и, в частности, социальные сети оказывают влияние на процессы политической мобилизации. Социальные сети на сегодняшний день предлагают новые возможности для осуществления коммуникации политического характера, расширяют доступ к такой информации, в настоящее время в социальных сетях осуществляется вовлечение пользователей в обсуждение публикаций, планов и деятельности современных политиков. В результате этого они дают возможность общаться с должностными лицами, получать сведения, которые способствуют участию граждан в политике.

Коммуникация в интернете характеризуется беспрецедентными скоростью и охватом аудитории. Кроме того в социальных сетях наблюдается меньшее количество посредников. Однако, некоторые исследователи полагают, что нет большой разницы между контактами

личного характера и получением информации с помощью социальных сетей[149].

К.А. Брянов и А.С. Шерстобитов исследовали основную роль коммуникативных и информационных технологий в ходе Арабской революции в Египте и Тунисе 2011 г. В рамках исследования ученые пришли к выводу, что современные социальные сети – это эффективный инструмент мобилизации граждан, а также инструмент распространения соответствующей информации.[150] В.А. Курочкин, в свою очередь, подчеркивает в своих исследованиях, что в современном обществе социальные сети пока не стали эффективным способом политического противостояния, так как политический дискурс в социальных сетях более «прост», имеет низкий уровень политизации и «виртуализации» активности.[151]

Социальные сети могут применяться для формирования «повестки дня», управления мнением общества и быть инструментом воздействия на других. Поэтому они могут выступать одним из ресурсов политической мобилизации. Так, К.А. Брянов и А.С. Шерстобитов в качестве примеров описывают координацию и организацию протестных акций в социальной сети «Вконтакте» во время избирательного периода в России 2011-2012 годов.[152] Они строят в своей работе «сетевые карты» – визуализацию отношений между группами социальной сети «Вконтакте» и устанавливают взаимосвязь между политической мобилизацией и сетевой активностью.

---

[149] Bimber B. The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism // Polity. 1998. Vol. XXXI. No. 1. P. 133-160.

[150] Шерстобитов А.С., Брянов К.А. Технологии политической мобилизации в социальной сети «ВКонтакте»: Сетевой анализ протестного и провластного сегментов // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: «Грамота», 2013. № 10 (36), часть I. С. 196-202.

[151] Курочкин А. В. Трансформация государственного суверенитета в условиях становления сетевого общества // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: «Грамота», 2012. № 2 (26). Ч. III. С. 95-99.

[152] Шерстобитов А.С., Брянов К.А. Технологии политической мобилизации в социальной сети «ВКонтакте»: Сетевой анализ протестного и провластного сегментов // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. Тамбов: «Грамота», 2013. № 10 (36), часть I. С. 196-202.

Данная взаимосвязь может быть представлена следующим алгоритмом (рис. 8.).

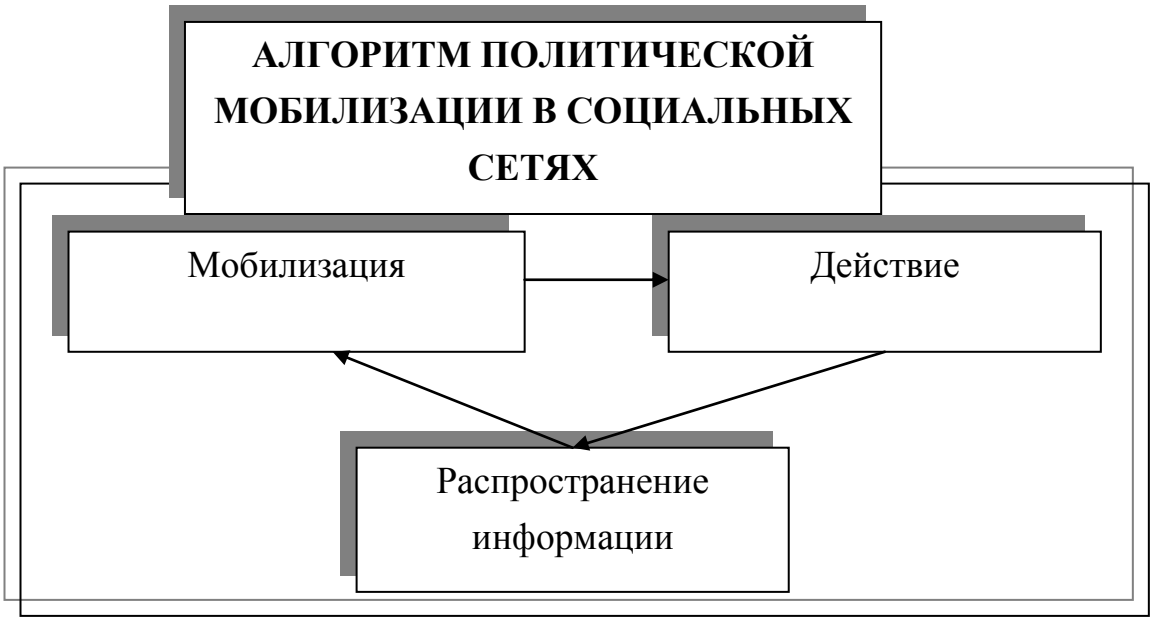


Рис. 8. Алгоритм политической мобилизации в социальных сетях по К.А. Брянову и А.С. Шерстобитову

Таким образом, ученые полагают, что при офлайн-активности участников социальных сетей мобилизация, в конечном счете, приводит к интенсификации сетевой коммуникации. Указанные ученые приводят в качестве примера основные данные об акциях протеста и их координации в социальных сетях «Вконтакте» и «Facebook» во время избирательного цикла 2011-2012 годов.

А. Шоу более детально классифицировал факторы политической мобилизации граждан в социальных сетях[153]:

1) Легкая доступность информации. Такая функция социальных сетей, как обмен мгновенными сообщениями позволяет быстро обмениваться политическими новостями и идеями.

[153] Shaw A. Role of Social Media in Social Mobilization (with Special Reference to Shahbag and Hokkolorob Movements) // Global Media Journal – Indian Edition [online]. 2016. Vol. 7 (1). URL: https://www.caluniv.ac.in/global-mdia-journal/COMMENT-2016-NOV/C-5-F.pdf (дата обращения 13.01.2019).

Так, доступность социальных сетей способствовала обмену информацией для жителей Гонконга с 26.09 по 31.12 2014 года во время движения «Occupy Central». За указанный период в Twitter было зафиксировано более 100 млн. сообщений, которые посвящались акциям протеста. Благодаря сетевому приложению «Instagram» происходило быстрое распространение фотографий с улиц, где были изображены люди, которые во время протеста укрывались от слезоточивого газа зонтиками. В результате массового «продвижения» таких фотографий протесты стали называть «Революцией зонтиков»[154].

2) Удобная среда для создания контента. Информационное пространство создается самими пользователями с помощью встроенных инструментов и может включать в себя картинки, видео, музыку, чаты, геолокацию и др.

3) Низкие финансовые издержки. В результате появления социальных сетей стало возможно более экономично осуществлять обмен мнениями, идеями и новостями. Согласно данным агентства «We Are Social» и сервиса Hootsuite только за 2018 г. прирост активных пользователей Интернета и социальных сетей в мире составил 9-10%, т.е. несколько сот миллионов людей (Рис. 9.). Все больше людей используют смартфоны и планшеты для доступа к социальным сетям. И благодаря большему количеству подключений юзеры получают больше свободы в использовании социальных сетей где бы он ни находились и что бы они ни делали.

[154] Leng S., Wertime D. Hong Kong's Protest, in Memes // Foreign Policy [online]. 2014. 29th September. URL: http://foreignpolicy.com/2014/09/29/hong-kongs-protest-in-memes/ (дата обращения 10.10.2019).

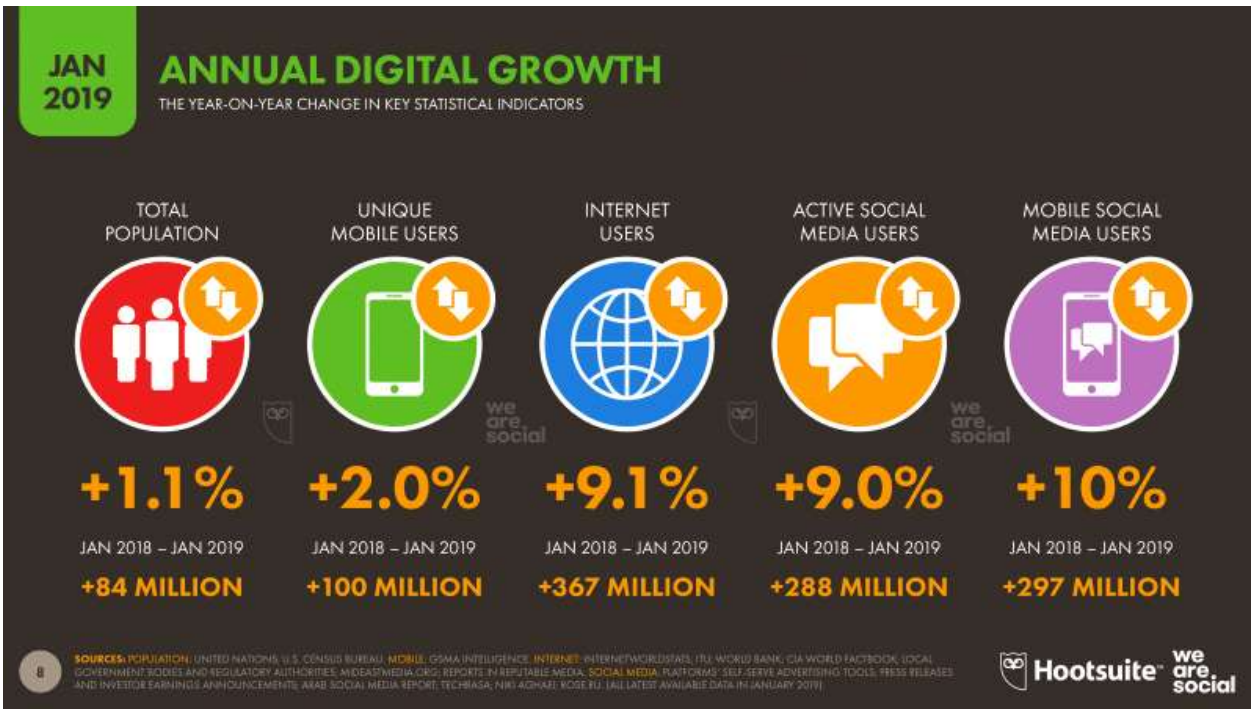


Рис. 9. Прирост пользователей Интернета и социальных сетей в мире с января 2018 г. по январь 2019 г.[155]

Свержение президента Филиппин в 2001 г. стало одним из самых ярких примеров такого фактора политической мобилизации, как низкие финансовые издержки. С помощью SMS-рассылки политическое движение «Народная власть II» организовало протестные демонстрации в Маниле. Граждан Филиппин в текстовых сообщениях призывали одеться в черную одежду и выйти на одну из центральных улиц. За 4 дня текстовой рассылки количество вышедших на улице «протестующих» составило 1 миллион человек.[156]

4) Общность интересов. Социальные сети позволяют пользователям находить людей, имеющих схожие с ними симпатии и антипатии, что способствует более плодотворному обмену политическими мнениями. В

[155] Вся статистика интернета на 2019 год – в мире и в России [Электронный ресурс] // WebCanape. 2019. 11 февраля. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/ (дата обращения 26.02.2019).

[156] Ушкин С.Г. Теоретико-методологические подходы к изучению сетевой протестной активности: от «умной толпы» к слактивизму // Мониторинг общественного мнения: экономические и социальные перемены. 2015. № 3. С. 3-11.

результате формирования таких групп интересов возможно объединение по политическим интересам.

5) Глобальная связь. Социальные сети предлагают быстрый способ связи между людьми в мире. Так, в исследованиях С. Гонсалес-Бэйлон отмечалась, что в мае 2011 г. в сервисе Twitter протестным выступлениям в Испании было посвящено более 500 тысяч твитов, которые были опубликованы более чем 100 тысячами пользователей.[157]

6) И, наконец, последним, но не менее важным фактором эффективности политической мобилизации в социальных сетях является то, что они предоставляют платформу для самовыражения и объединения простых людей вокруг общих интересов и проблем, а не только являются коммуникативной площадкой для экспертов и политических лидеров.

Так, к примеру, в России анонимный имиджборд «Двач» – известен вводом в активный оборот сленговых выражений, слов и картинок («мемов»), которые в то же время имеют отчетливое политическое значение. Благодаря данному сервису стал весьма популярен термин «ватник»[158].

Так же интересно, что протестный и скандальный характер той или иной группы в соцсети сам по себе способен привлечь большое количество людей. В 2009 г. Андерс Колдинг-Йоргенсен, психолог и преподаватель социальных медиа в Университете Копенгагена, в качестве эксперимента создал группу в Facebook, в которой провозглашался протест против сноса в Копенгагене известного Аистова фонтана (в реальности такого плана никогда не существовало). За небольшой промежуток времени группа набрала более 27 тыс. подписчиков, при этом мало кто удосужился проверить факт того, что фонтан действительно собираются сносить, хотя для этого достаточно было всего лишь почитать сообщения других участников группы. Но диалога в группе почти не происходило, площадка была использована в основном для

---

[157] Шарапов Р.И. Условия политической мобилизации в сети Интернет // Социодинамика. 2017. № 10. С. 1-8.

[158] Суманеев И. Reddit, Трамп и «Политач». Как социальные сети влияют на политику [Электронный ресурс] // НОЖ [сайт]. 26 декабря 2018. URL: https://knife.media/social-media-politics/ (дата обращения 11.11.2019).

выражения возмущения и негодования. Автор эксперимента сделал вывод, что судьба фонтана на самом деле мало интересовала людей, форум использовался для реализации потребности людей быть частью чего-то большого и важного[159]. В этом суть такого феномена как *слактивизм*, т.е. бесполезного цифрового активизма ради публичного эффекта самопрезентации. По замечанию профессора социологии Ш. Грасмак из Университета Темпл, участие в общественном движении объяснялось скорее «желанием подтвердить свою социальную ценность, слившись с ним, нежели тем, что это общественное движение соответствует идентичности каждого его участника»[160].

В рамках настоящего исследования интересен российский взгляд на проблему. В статье Р.И. Шарапова были выделены онлайн и офлайн факторы политической мобилизации масс[161]. Наиболее интересны в этом отношении именно офлайн-факторы, влияющие на политическую активность людей:

1) Уровень информационной свободы общества, который зависит от существующего политического режима. При росте авторитаризма доступ к Интернету может ограничиваться.

2) Доступность мобильных технологий Интернета. Мобильный телефон становится основным проводником в социальные сети и обмену информацией в них. В 2010 г. в социальной сети Facebook была создана «Страница Революции» для организации протестов в ходе Арабской весны. На персональные видеокамеры и мобильные телефоны записывались события протестных движений и выкладывались в Интернет. По данным арабских Social Media Report 2011, около 94 % населения Туниса получали

---

[159] Colding-Jørgensen A. Stork Fountain Experiment #1: Why Facebook groups are not democratic tools [online] // URL: http://virkeligheden.dk/2009/stork-fountain-experiment-1-facebook-groups-are-not-democratic-tools/ (дата обращения 12.11.2019).

[160] Hesse M. Facebook Activism: Lots of Clicks, but Little Sticks [online] // The Washington Post. 2009. 2nd July. URL: https://www.washingtonpost.com/wp-dyn/content/article/2009/07/01/AR2009070103936_2.html (дата обращения 17.10.2019).

[161] Шарапов Р.И. Условия политической мобилизации в сети Интернет // Социодинамика. 2017. № 10. С. 1-8.

политическую информацию из социальных сетей через телефон[162], в результате чего протестующие могли организовывать взаимосвязь, практически не подконтрольную цензуре. Как отмечал Дж. Бернарда, глава подразделения ZenithOptimedia, в настоящее время все больше пользователей интернета отмечают, что для них основными источниками развлечения и получения информации являются мобильные устройства. Становится очевидно, что мобильный интернет выступает в глобальном масштабе наиболее динамично растущим медиа.[163] Основными преимуществами использования мобильных приложений является возможность передавать местоположение пользователя. При организации протестных движений данная функция ускоряет и упрощает процесс координации граждан.

3) Уровень относительной депривации граждан. Примером могут служить политические протесты 2011-2012 гг. в России. Так, ВВП на душу населения в России в период 2000-2008 годов увеличился практически в два раза, однако финансовый кризис 2008 г. прервал рост экономики, снизив темпы роста валового внутреннего продукта на душу населения. Именно поэтому период бурного роста экономики не смог сформировать рост ожиданий у граждан, но мировое посткризисное восстановление способствовало повышению цен на продовольствие, что привело к разрыву между достижениями и ожиданиями людей к концу 2011 г., когда в России начались массовые акции протеста.[164]

4) Наличие объединяющей идеи. Так, перед событиями Арабской весны в международных СМИ начала разворачиваться жесткая критика политических режимов, начали распространяться идеи о недопустимости проявления силовых акций против протестующих. Накануне Арабской весны в 2010 г. в международных СМИ начали формироваться соответствующая

---

[162] Абоненты мобильной связи (на 100 человек) – Тунис (1960 – 2015) [Электронный ресурс] URL: http://data.trendeconomy.ru/indicators/Mobile_Phones/Tunisia (дата обращения 10.10.2019).

[163] Шарапов Р.И. Мобильный интернет как инструмент политической мобилизации // Известия Тульского государственного университета. Гуманитарные науки. 2017. № 1. С. 20-27.

[164] Свищёва А.Н. Относительная депривация в условиях финансово-экономического кризиса // Мониторинг общественного мнения: экономические и социальные перемены. 2016. №5. С. 183-202.

информационная поддержка этой идеи и идеологическая оправдание будущих протестов.

5) Наличие авторитетных лидеров общественного мнения, которые в сети являются проводниками политических лозунгов.

Таким образом, модель факторов политической мобилизации в социальных сетях будет выглядеть следующим образом (рис. 10.).



Рис. 10. Факторы политической мобилизации

Использование социальных сетей предоставляет возможность для осуществления прямых политических коммуникаций без воздействия традиционных институтов и СМИ. Таким образом, в социальных сетях многократно усиливается влияние политических кампаний. Социальные сети

способны не только привносить новую динамику в социальные движения, но и формировать культуру политического сопротивления. В результате этого, коллективные действия в социальных сетях способствуют популяризации виртуальных протестов на глобальных платформах, а также формированию основных политических событий без ограничений в пространстве и времени.

Исходя из этого, можно заключить, что социальные сети в политической мобилизации обладают революционным потенциалом, что подтверждается такими протестными акциями, как «Движение Хок Колороб», «Шахбагское движение», «Оккупай Уолл-стрит», «Арабская весна».

2.3. Травматизация сознания в социальных сетях как новая форма политического насилия: вызовы национальной безопасности

«Общество травмы» стало современной реальностью[165]. Травмы сознания, проявляющиеся в разрывах ценностей и норм, усвоенных в процессе социализации, проявляются как новая форма политического насилия, несущая вызовы национальной безопасности. Сложность вызовов травм проявляется в том, что они выступают как объективная деформированная реальность, так и культурно конструируются с определенными политическими целями[166]. В книге Дж. Александера *«Драма социальной жизни»* особый акцент сделан именно на культурном конструировании травм, которые выступают как новая и весьма сложная форма политического насилия. Социологом обосновывается форма манипуляции в виде «*драматизации сознания»* – процесса, приводящего к ломке прежних смыслов и ценностей и образованию *новых, политически*

[165] Тощенко Ж.Т. Общество травмы: между эволюцией и революцией (опыт теоретического и эмпирического анализа). Москва: Весь Мир, 2019.

[166] Штомпка П. Социальное изменение как травма // Социологические исследования. 2001. № 1; Штомпка П. Культурная травма в посткоммунистическом обществе // Социологические исследования. 2001. № 2; Alexander J.C. The Meaning of Social Life: A Cultural Sociology. New York: Oxford University Press, 2003; Alexander J.C. Trauma. A Social Theory. Cambridge: Polity Press, 2012.

заданных, что, по мнению автора, – квинтэссенция нынешнего модерна, основанного на производстве смыслов в социальных сетях. В современном мире «без драмы коллективные и личные смыслы не смогли бы поддерживаться, дьявол не мог бы быть идентифицирован, справедливость невозможно было бы достичь»[167]. Результатом социальной драмы является социальная травма сознания людей и их прежних жизненных миров. Драматизация сознания начинается с травмирования смыслов, обретенных индивидами в процессе социализации, которые замещаются новыми *мистифицированными, политически заданными представлениями* о смене ценностей. Посредством драмы в интернет-пространстве формируются политически востребованные смыслы, чья «драматургия пуста и цель которого – чистая мистификация. В спектаклизированных обществах модерна все перевернуто с ног на голову, ничто не приходит снизу вверх. Мы никогда не сможем быть активными, будучи драмопроизводящими агентами»[168]. При этом автор показывает и анализирует собственно механизм драматизации сознания. Когда в сетях актуальные социальные проблемы «входят в суматоху революционной социальной борьбы, они выступают как значимые символы. В то время как их материальность иллюзорна, они обладают фактической ценностью – этот вымысел реально используется. Для участников, равно как и наблюдателей, революционные конфликты воспринимаются как борьба на жизнь и смерть не между просто социальными группами, а между социальными представлениями, с одной стороны, священного, а с другой – нечестивого»[169]. Многие люди, полагающиеся на смыслы, производимые в интернет-пространстве и, в частности, в социальных сетях, могут и не осознавать, что их сознание травмируется – они принимают навязанные ценности, у них появляется готовность к жизни в новой мистифицированной реальности, представления

[167] Alexander J.C. The Drama of Social Life. Cambridge: Polity Press, 2017. P. 141.
[168] Там же. P. 2, 3.
[169] Там же. P. 40, 46.

о будущих свободе, счастье, которые не будут материализованы. Так, осуществляется целенаправленное производство симулякров и фейков.

В современном мире посредством драматизации сознания социальные сети дают возможность для осуществления соответствующих политических манипуляций, что может быть использовано государствами и другими различными политическими акторами. К примеру, в 2015 году мировые СМИ сообщили, что Агентство США по глобальным медиа (U.S. Agency for Global Media) собиралось создать медиадепартамент, в задачи которого будет входить «борьба с дезинформацией в росийской медиасфере» в социальных сетях «Вконтакте», «Одноклассники», а также русскоязычных сегментах Twitter и Facebook[170]. В рамках данного проекта предполагается распространять с помощью социальных сетей информацию, которая соответствует «большой прессе», а не сведениям из медиасферы России. Основной задачей такого проекта выступает разоблачение информации, предлагаемой российскими СМИ, распространение политической сатиры, т.е. создание определенных видеоматериалов, альтернативных медиапродуктам из России.

Именно поэтому на сегодняшний день социальные сети выступают новейшим способом и инструментом ведения информационных войн[171]. Г.И. Могилевская отмечает, что в настоящее время социальные сети перестали быть ресурсом для взаимных поздравлений, поиска утраченных связей или формой выражения своего мнения. На взгляд исследователя, социальные сети превратились в непосредственное оружие информационных войн, что обусловлено уникальной возможностью воздействия на сознание большой

[170] Американцы введут «информационные войска» в российские социальные сети. [Электронный ресурс] // Свободная пресса, 2015. URL: http://svpressa.ru/politic/news/118677/ (дата обращения 20.12.2019).

[171] Бутусов А.В. Социальные сети как инструмент политического противоборства и информационных войн // Вестник Тамбовского университета. Серия: Общественные науки, 2018. №13. С. 71-75.

аудитории, сосредоточенной на площадке определенного интернет-ресурса[172].

Исследователь информационной безопасности С.Н. Ненашев считает, что в настоящее время наиболее мощным видом противостояния в борьбе экономических и культурных систем выступает информационная война, основную роль в которой играют именно социальные сети[173]. Прежде всего, это обусловлено тем, что социальные сети предоставляют доступ к личной информации большого количества пользователей, а также позволяют оказывать воздействие на их мировоззрение.

Основными целями использования социальных сетей в качестве информационного оружия, на взгляд С.Н. Ненашева, выступают:

– распространение вредоносного софта для оказания технологического и информационного воздействия на пользователей;

– манипуляция коллективным сознанием, трансформация ценностей и навязывание поведенческих шаблонов для психологического и информационного воздействия.

Государства используют современные интернет-технологии для осуществления конкурентной борьбы во внешней политике. События последних лет (Арабская весна, Киевский майдан, Цветные революции и т.д.) свидетельствуют, что социальные сети несут потенциальную угрозу устойчивости политической системы, угрозу национальной безопасности государства. Развитие и продвижение социальных сетей переводит информационные войны на качественно новый уровень, увеличивая их эффективность, интенсивность и масштабность. На сегодняшний день с помощью социальных сетей могут совершаться преступления против политического строя, экономические преступления, продвигаться экстремистские идеи и взгляды, осуществляться вербовка в радикальные и

---

[172] Могилевская Г. И. Информационная война в социальных сетях [Электронный ресурс] // Молодой ученый, 2015. №15. С.871-873. URL: https://moluch.ru/archive/110/26957/ (дата обращения 15.11.2019).

[173] Массен Э. Соцсети – оружие массового поражения в информационной войне [Электронный ресурс]. URL: https://antisoc.ru/mneniya-uchenyih/kak-ispolzuyutsya-sotsialnyie-seti-v-informatsionnoy-voyne/ (дата обращения 22.12.2019).

террористические организации. Кроме того, с помощью социальных сетей внедряются и передаются шпионские программы[174].

Использование социальных сетей в качестве информационного оружия в кибервойне может иметь следующие направления (рис.11.).



Рис. 11. Основные направления использования социальных сетей в качестве информационного оружия

Рассмотрим их более подробно.

1) Политическая мобилизация.

На этапе современного развития IT-технологий социальные сети выступают одной из самых актуальных сфер политической мобилизации, так

[174] Гасанова М.М. Социальные сети в политике // Вестник Саратовского Государственного Социально-Экономического Университета. № 5 (59). Саратов, 2015. С. 215-218.

как в них определяются места проведения гражданских акций, осуществляется формирование информационной платформы для обмена мнениями и прочее. Социальную сеть с позиции технического подхода можно представить в качестве совокупности информационных, программных и аппаратных сервисов, которые поддерживают внутри данной сети определенные коммуникации[175]. Для понимания особой значимости и роли социальных сетей в политической мобилизации граждан требуется обратиться к ресурсному подходу, в рамках которого внимание акцентируется на возможностях акторов производить смыслы, их потенциале по привлечению сетевых и индивидуальных ресурсов для достижения конкретных политических целей. В рамках ресурсного подхода можно дифференцировать акторов, которые находятся в идентичных структурных позициях социальной сети по их сетевым и индивидуальным ресурсам: гендерным характеристикам, статусам, знаниям, капиталу и богатству.

В результате повышенной вовлеченности современного общества в цифровое пространство сетевое взаимодействие становится мощным инструментом субъектов политического мира для объединения граждан и их мобилизации в соответствующие политические процессы. Согласно исследованию ВЦИОМ, которое было проведено зимой 2018 г., около 45 % граждан в возрасте от 18 и более лет практически ежедневно обращаются к социальным сетям, хотя бы раз в неделю социальные сети используют 62 % опрошенных граждан. Стоит при этом подчеркнуть, что старшая возрастная группа лишь на 15 % вовлечена в социальные сети, 69 % россиян, использующих социальные сети, имеют возраст от 25 лет до 34 лет. И, наконец, 91 % российских граждан в возрасте от 18 лет до 24 лет в наибольшей степени вовлечены в мир социальных сетей[176].

---

[175] Римский В. Л. Коммуникация в социальных сетях как рациональный ответ граждан на условия ограничения их гражданской и политической активности // Социальные сети и виртуальные сообщества. М.: ИНИОН РАН, 2013. С. 132-146.

[176] ВЦИОМ. Социальные сети в России. Осень 2018. [Элетронный ресурс] URL: https://br-analytics.ru/blog/wp-content/uploads/2018/12/Sotsseti-Rossiya-osen-2018.pdf (дата обращения 10.09.2019).

Наиболее популярными социальными сетями в Российской Федерации считаются «Мой мир», «Twitter», «Instagram», «Viber», «WhatsApp», «Facebook», «Одноклассники», «Вконтакте» и «Skype» (Таб. 3.).

Социальные сети	**Кол-во сообщений, тыс.**	**Ежемесячная аудитория, тыс. человек**
Live Journal	4617	46
Twitter	59635	818
Мой мир	7216	99
Одноклассники	364000	15800
Instagram	304960	23740
Facebook	122760	2250
ВКонтакте	1096392	36453

Таб. 3. Активность российских граждан в социальных сетях, октябрь 2018 г.

Основной характеристикой социальных сетей в современном мире считается возрастная характеристика аудитории социальных сетей. Как уже отмечалось ранее, наибольшее количество пользователей социальных сетей – это молодые люди. Эта категория граждан является наиболее восприимчивой группой, которая в наибольшей степени поддается воздействию со стороны современных медиа-инструментов. В результате этого становится очевидно, что социальные сети выступают эффективным средством вовлечения современной молодежи в решение и обсуждение определенных проблем, политических вопросов, а также отстаивания ими своей политической позиции. А.В. Манойло отмечает по этому поводу, что современное молодое поколение активно ищет возможности для собственной социализации, повышения своего статуса в обществе, в результате чего они готовы принимать участие в рискованных акциях, в особенности в том случае, когда

организаторы таких акций обещают гарантированный и быстрый успех. Для поиска молодых граждан основной площадкой выступают именно социальные сети, где российское молодое поколение проводит много свободного времени[177].

Политические субъекты в социальных сетях используют разные средства и приемы воздействия на граждан, целью которых является управление эмоциями, настроениями и мнением граждан, а также изменение их привычных моделей поведения. Таким образом, в современных условиях социальные сети выступают особым пространством, в котором уровень эмоциональной и социальной напряженности групп балансирует в зависимости от политических потребностей акторов. В социальных сетях создаются определенные сообщества, как оппозиционных политических групп, так и групп в поддержку действующей власти.

Политическая мобилизация, проводимая в социальных сетях, осуществляется по следующей схеме:

1) описание проблемы, интересующей граждан;

2) вступление в группу;

3) обсуждение участниками группы основных тем;

4) развитие коммуникации и укрепление отношений внутри группы;

5) управление группой и активация действий участников за пределами кибернетического пространства[178].

Таким образом, в начале процесса мобилизации происходит формирование соответствующей информационной среды, которая наполнена идеями и сообщениями, транслирующимися для вовлечения граждан в диалог. Происходит открытое и свободное обсуждение определенных тем, в результате которого проявляется большая солидарность между участниками группы, т.е. происходит развитие горизонтальных связей.

---

[177] Манойло А.В. Убить котенка, или технологии конфликтной мобилизации в социальных сетях // Мировая политика. № 3. 2015. С. 1-12.

[178] Киняшева Ю.Б. Социальные сети как инструмент политической мобилизации граждан в современной России // Известия ТулГУ. Гуманитарные науки. 2018. №3. С. 3-10.

Расширение аудитории происходит на втором этапе, когда растет посещаемость группы и укрепляется внутригрупповая сплоченность. С этого момента происходит усиление концентрации точечной информации, которая содержит конкретную политическую идею, а затем и развитие коллективного мышления. В этот момент появляются участники группы, которые выполняют определенные роли (арбитры, модераторы, авторитетные пользователи и пр.), а также вводятся правила поведения, т.е. четко просматривается управление коммуникациями внутри группы.

На третьем этапе происходит управление группой, которое предполагает развитие согласованных и активных форм гражданского поведения, их выход за рамки киберпространства. На этом этапе можно наблюдать закрепление нужного «образа» в сознании граждан, развитие феномена «группового мышления», призывы к коллективным действиям, а также определение готовности участников к принятию участия в выступлениях, демонстрациях, митингах, и пр.

На четвертом этапе прослеживается взаимозависимость между развитием политических событий и организацией сетевого взаимодействия. Политические субъекты, принимая во внимание, что определенные политические решения гражданами воспринимаются достаточно негативно, начинают использовать в собственных интересах такие ситуации, тем самым, разжигая конфронтацию. Сообщества, созданные в социальных сетях, являются наиболее удобным и эффективным приемом влияния на общественные группы. Ярким примером может служить политическая мобилизация граждан, устроенная весной 2018 г., когда было создано более 200 публичных страниц в социальных сетях под названием «Митинг 26 марта – против коррупции» во «ВКонтакте». Во всех сообществах, которые были созданы в разных российских регионах и городах, наблюдался открытый диалог подписчиков, призывы к участию в протестном движении, а также комментарии к роликам «Против коррупции». В результате такой политической мобилизации в 82 городах Российской Федерации прошли

акции, численность участников в которых составила около 60 000 человек. Большинство митингов носили несанкционированный характер. Социальные сети были практически единственным способом распространения информации, что позволяет сделать вывод об эффективном использовании технологии политической мобилизации граждан в социальных сетях.

Таким образом, можно прийти к выводу, что в настоящее время социальные сети представляют эффективное политическое пространство, в котором происходит вовлечение гражданского общества в политический процесс. Прежде всего, эффективное использование социальных сетей для политической мобилизации граждан обусловлено низкими затратами на осуществление данного процесса и широким охватом аудитории. Именно поэтому можно предположить, что при недостаточном контроле и значительном потенциале социальных сетей заинтересованные сегменты политического пространства могут привести к дестабилизации политического устройства в государстве.

2) Вовлечение в экстремистские сообщества сконструированных политических смыслов «гуманизма».

Глобально функционирующие экстремистские организации используют социальные сети для вовлечения граждан в свою деятельность в значительной степени посредством целенаправленно сконструированных политических смыслов «гуманизма». Как отмечает У. Бек, новой реальностью современного мира стала «глобальная домашняя политика», квинтэссенция которой следующая: «протесты и проекты обычно оправдываются от имени “гуманизма” и “планеты”»[179].

В настоящее время в социальных сетях совершается деятельность 90 % экстремистских организаций в мире[180]. Функциональные возможности соцсетей позволяют террористическим организациям проводить вербовку и проявлять активность вне зависимости от географии проживания сетевых

[179] Beck U. Twenty Observations on a World in Turmoil. Cambridge: Polity Press, 2012.

[180] Лемеш К.И. Об опасности «социально-сетевого» экстремизма // Современные научные исследования и разработки. Т. 2. № 1(9). Астрахань. 2017. С. 378-379.

пользователей. Среди социальных сетей основными аренами для такой деятельности выступают «Twitter», «Facebook» и «ВКонтакте». Также для организации экстремистской деятельности получили широкое применение «YouTube», «Viber» и «WhatsApp»[181].

Внутри сообществ соцсетей пользователь имеет шанс столкнуться с «вредоносной» информацией[182]. В.Н. Лопатин отмечал, что к такой информации относятся:

1) посягательства на репутацию, доброе имя и честь гражданина;

2) пропаганда вражды и ненависти;

3) призывы к войне;

4) сведения, которые возбуждают религиозную, национальную, расовую, социальную вражду и ненависть[183].

Террористические и экстремистские сообщества рассматривают социальные сети как основной способ пополнения количества собственных сторонников[184]. Экстремистские сообщества пользуются возможностью анонимных действий на сайте. В результате этого группы экстремистов популяризируют собственную деятельность в интернете. Практически невозможно проследить каждое такое сообщество экстремистского характера. Согласно заключению Центра Визенталя за 2013 г., спецслужбы имеют возможность расследовать лишь 0,1-0,5 % публикаций в «Facebook» и «Twitter», за которыми могут скрываться криминальные группировки[185]. В настоящее время при этом в «Facebook» и «Twitter» не могут официально

---

[181] Борисов С.В. Сущность преступлений экстремистской направленности // Мировой судья. Москва. 2009. №4. С. 12-15.

[182] Жукова О.С., Иванченко Р.Б., Трухачев В.В. Информационный экстремизм как угроза безопасности Российской Федерации // Вестник Воронежского института МВД России. № 1. Воронеж. 2007. С. 53-55.

[183] Лопатин В.Н. Понятие и структура информационно-психологической безопасности // Право и политика. 2001. № 10. С. 44.

[184] Деева А.К., Коробейник В.А. Экстремистская деятельность в сети интернет // Профилактика и противодействие идеологии религиозно-политического терроризма и экстремизма в современной России: проблемы и перспективы: сб. ст. по материалам Всерос. научно-практ. конф., Белгород, 15 июня 2017 г. / НИУ БелГУ. Белгород, 2018. С. 63-65.

[185] Социальные сети как орудие экстремизма. [электронный ресурс] // Информационно-аналитический журнал "Политическое образование". URL: http://lawinrussia.ru/content/socialnye-seti-kak-orudie-ekstremizma (дата обращения 23.12.2019).

находиться только люди, состоящие в реестре National Sex Offenders Registry (реестр секс-преступников). Однако и такие ограничения законодательного уровня легко обходимы при использовании «косвенной пропаганды». Для остальных же преступных групп доступ в «Facebook» и «Twitter» доступен.

Так, в сентябре 2013 г. в Кении сомалийские исламисты «Аль-Шабаб» ворвались в торговый центр в г. Найроби. Несмотря на то, что специализированные службы были уверены в благоприятном исходе контртеррористической операции, было убито больше 100 человек в результате совершенного теракта. Основным обстоятельством, которое способствовало массовым убийствам граждан, стала трансляция события в социальных сетях «Facebook» и «Twitter». Кроме того, указанные социальные сети использовались для отслеживания исламистами актуальной информации о проведении контртеррористической операции, а также популяризации в интернете собственных экстремистских идей.

Еще одним примером использования данных социальных сетей для продвижения экстремистских идей могут служить массовые протесты в Тунисе в 2010 г., которые привели к тому, что был свергнут президент Зин аль-Абидин Бен Али.

Появилось понятие «Твиттер-революция», которое применяют, в частности, по отношению к революции 2011 г. в Египте, революции 2010-2011 гг. в Тунисе, сериям акций протеста 2009 г. в Иране, массовым беспорядкам 2009 г. в Кишиневе, и «Евромайдану» в Украине.

При исследовании влияния социальных сетей на вовлечение в экстремистские сообщества внимание нужно также уделить социальным сетям с функцией геопозиционирования. С помощью таких социальных сетей можно не только осуществлять коммуникации, но и отслеживать передвижения пользователей этих сетей. К примеру, в 2011 г. в разгар революции в Тунисе для подачи сигнала о нахождении в тюрьме или отделении полиции, а также для координации социальных движений

активисты экстремистской организации «Такриз» использовали социальную сеть «Foursquare».

Следовательно, главным образом политическая мобилизация осуществляется через мобильный интернет, а не стационарный. Это обусловлено тем, что передача актуальных видеоматериалов и фотоматериалов, возможность передачи местоположения снижают временные издержки политической мобилизации пользователей в части их объединения и координации. При этом функционал социальных сетей полностью фиксируется в мобильных версиях, что предоставляет участникам дополнительные удобство и скорость.

Таким образом, использование мобильного интернета и мобильного функционала социальных сетей наиболее выигрышно в сравнении со стационарным интернетом в широте охвата аудитории, а также скорости распространения информации. Именно эти условия считаются необходимыми для проведения эффективной политической мобилизации.

3) Кибершпионаж в социальных сетях.

Стоит подчеркнуть эффективность осуществления слежки за пользователями в социальных сетях. В книге американского журналиста Г. Гринвальда[186] описывается программа X-KEYSCORE, используемая американской спецслужбой АНБ. С помощью данной программы осуществляется сбор электронных данных, отслеживание интернет-активности граждан в реальном времени.

Е. Мессмер пишет, что кибершпионаж – это несанкционированное получение информации для получения военного, политического, экономического или личного превосходства, осуществляемого с использованием взлома или обхода системы компьютерной безопасности. Для осуществления кибершпионажа используется вредоносное программное

[186] Гринвальд Г. Негде спрятаться. Эдвард Сноуден и зоркий глаз Дядюшки Сэма // Пер. Т. Зверевич, С. Силинский. СПб.: «Питер», 2014. С. 320.

обеспечение, которое включает шпионские программы[187]. В последние годы в социальных сетях также осуществляется кибершпионаж со стороны сотрудников спецслужб для выявления антиправительственной, террористической или экстремистской деятельности[188]. Так, например, сотрудники ЦРУ с помощью программы Athena могут изменять удаленно настройки операционных систем, т.е. занося компьютерные вирусы, они могут выгружать файлы с зараженных устройств. Данная программа была разработана ЦРУ совместно с компанией Siege Technologies, она работает на компьютерах, в которых используется ПО Windows[189].

Что же касается мобильных устройств, то, как отмечалось выше, кибершпионаж возможен и в мобильном интернете. Так, в 2010 г. компании Google и Apple обвинялись в отслеживании GPS-данных телефонов и их передачи в штаб-квартиру. Однако, компания Apple смогла урегулировать данный конфликт, обновив прошивку iPhone, в результате чего было ограничено количество отслеживаний устройством.

К. Пирилло отмечает, что в последнее время кибершпионаж включает в себя исследование общественной активности на сайтах социальных сетей, в частности Twitter и Facebook[190]. При этом, стоит подчеркнуть, что акты кибершпионажа более распространены, чем акты кибервойны. В глобальном масштабе ведущей страной, которая проводит кампании кибершпионажа, выступает Китайская Народная Республика. Дж. Эванс в декабре 2007 г. отмечал о «нападках» со стороны китайских организаций на более, чем 300 британских компаний.

В контексте кибервойны интересны слова У. Лорда – главнокомандующего ВВС США, который отмечал, что Китай загрузил 10-20

---

[187] Messmer E. Cyber Espionage: A Growing Threat to Business. [Электронный ресурс] // PCWorld. 2008. URL: https://www.pcworld.com/article/141474/article.html (дата обращения 28.12.2019).

[188] Pirillo C. Five Ways the Government Spies on You. [Электронный ресурс] // The Lockergnome daily report. 2011. URL: https://lockergnome.com/2011/11/07/five-ways-the-government-spies-on-you/ (дата обращения 28.12.2019).

[189] Там же.

[190] Там же.

терабайт данных из NIPRNet министерства обороны[191], которые были украдены у Командования по разработке информационных систем армии США (Army Information Systems Engineering Command), Центра военно-морских систем (Naval Ocean Systems Center), Агентства по противоракетной обороне (the Missile Defense Agency)[192].

Таким образом, с помощью отслеживания таких сведений, можно разрабатывать стратегии по политической мобилизации, политическому маркетингу определенных политических групп или политиков либо осуществлять вовлечение граждан в экстремистские сообщества. Кроме того, с помощью кибершпионажа можно нанести урон самому государству и его инфраструктуре.

4) Троллинг в социальных сетях.

Троллинг может осуществляться на новостных сайтах, в чатах, порталах, социальных сетях, тематических форумах и так далее. Троллинг в социальных сетях, в качестве информационного оружия, может проявляться в соответствующих провокациях, обмане, интригах, инсинуациях, слухах в интернет-пространстве.

В современных исследованиях отмечается, что троллинг в качестве информационного оружия и формы социальной агрессии обладает специфическими особенностями, одной из которых считается возможность его существования исключительно в виртуальных сообществах. Кроме того, в троллинге наблюдается специфический механизм лавинообразной агрессии, распространяющейся мгновенно на аудиторию виртуального сообщества. Особенностью троллинга является невозможность вступить в визуальный или физический контакт жертвы с инициатором конфликтной

[191] NIPRNet (от англ. Non-classified Internet Protocol (IP) Router Network; с англ. - «Сеть маршрутизации неконфиденциального IP-трафика») - сеть, используемая для обмена не секретной, но важной информацией между «внутренними» пользователями, а также для обеспечения доступа к интернету.

[192] Carr J. Inside Cyber Warfare. Sebastopol, USA, 2010. P. 4.

ситуации[193]. В настоящее время тролли могут создавать в целом ряде сообществ напряжение с помощью использования проекции публичности в СМИ и их сталкивания между собой. Сценарии последних «фэйсбуковских» революций, на его взгляд, свидетельствуют о том, что троллинг превращается в востребованную профессию.

5) Астротурфинг.

В социальных сетях для вовлечения и манипуляции целевой аудиторией все чаще используется социоинженерная технология астротурфинг. Она представляет собой имитацию общественной поддержки или искусственное формирование общественного мнения с помощью масштабного комментирования.

На веб-форумах астротурфинг используется для вытеснения мнения реальных пользователей, а также создания в интернет-пространстве поддельных кампаний, которые создают у пользователей впечатление, что большинство людей выступают против чего-либо или требуют что-то конкретное.

Можно выделить несколько инструментов, которые свойственны астротурфингу:

1) «серфинг», т.е. для поднятия рейтинга определенной информации в социальных сетях осуществляется техническая «накрутка» счетчика просмотров;

2) распространение в виртуальном пространстве основных идей, которые будут ретранслированы или поддержаны большинством пользователей;

3) создание команд для размещения сообщений в новостях, форумах и чатах с целью осмеивания или продвижения определенных идей[194].

---

[193] Внебрачных Р.А. Троллинг как форма социальной агрессии в виртуальных сообществах // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». Ижевск.2012. №1. С. 36-39.

[194] Ашманов И. Под властью ментального вируса, или Как отличить вброс от новости [Электронный ресурс] // Интернет журнал «Фома». 2012. URL: https://foma.ru/pod-vlastyu-mentalnogo-virusa-ili-kak-otlichit-vbros-ot-novosti.html (дата обращения 01.01.2020).

К примеру, в 2008 г. газета «The Guardian» писала о том, что в Китайской Народной Республике насчитывается около 300 тыс. астротурферов, основной задачей которых является организация противостояния отрицательной информации о Китае[195].

В блоге Daily Kos (США) отмечается, что астротурфинговые компании, располагая информационными технологиями, оказывают мультиплицирующий эффект[196]. Программное обеспечение автоматически воспроизводит все окружение, которое должно быть у реального пользователя, с помощью автоматической многократной публикации постов осуществляется поддержка фальшивых аккаунтов.

В 2011 г. «The Guardian» писала также о разработке Минобороной США программного обеспечения для манипулирования настроениями пользователей социальных сетей с помощью создания фальшивых онлайн-пользователей, которые будут распространять проамериканскую пропаганду и оказывать интеллектуальное воздействие на пользователей. Данная операция была названа Operation Earnest Voice, OEV, тендер на разработку программы SMISC для которой был объявлен Минобороной США в 2011 г.

Перечисленные элементы способствуют тому, что астротурфинг используется в более глобальных инструментах, результатом которых является формирование в сознании пользователей новых целей, смыслов и ценностей. Идеи астротурфинга подхватываются другими пользователями и тиражируются многочисленной аудитории социальных сетей, именно поэтому повышается популярность его использования в геополитических отношениях.

6. Сокпаппетинг.

Еще одним методом манипулирования большим количеством людей в интернете является сокпаппетинг. По определению, сокпаппетинг

---

[195] Ашрафов Р. Сетевые миротворцы [Электронный ресурс] // Портал «Кремль.орг». 2008. URL: http://kreml.org/opinions/189135205 (дата обращения 01.01.2020).

[196] Васильев А.А. Манипуляция общественным мнением через виртуальные сообщества // Христианское чтение. СПб 2016. №5. С. 207-222.

представляет собой искусственное нагнетание ажиотажа в виртуальном пространстве с помощью интернет-ботов и клонов. С помощью специальных программ генерируются тысячи «фейковых» аккаунтов, которые используются для информационного воздействия на пользователей социальных сетей.

Так, в 2013 г., как пишет Б. Ктепи, один бот в социальных сетях мог с помощью 1,8 млн. персональных компьютеров мультиплицировать до 3 млн. ретвитов, лайков и кликов ежедневно[197].

Стоит при этом подчеркнуть, что часто профессиональными троллями создаются «сокпаппеты», которые создают искусственную накрутку голосов, эффект большинства, распространяют дезинформацию и так далее.

Так, к примеру, в 2011 г. компания Ntrepid (США) получила от Центрального командования США контракт на 2,76 млн. долларов для создания «фальшивых онлайн-пользователей», которые будут распространять необходимую политическую информацию в социальных сетях и манипулировать мнениями пользователями[198]. Проамериканская пропаганда велась на языках пушту, урду, персидском и арабском языке.

Также 11 сентября 2014 г. отчеты «сокпаппетов» указывали на взрыв в Луизиане химического завода. Многие СМИ публиковали данную новость, в том числе блогеры на YouTube и Twitter, однако американские власти заявили о том, что данное событие является обманом. Однако, многие отмечали, что данная информация была получена от офиса по управлению «сокпаппетингом», спонсируемой правительством. [199]

Кристофер Сноуден писал, что в 2012 г. Правительство ЕС и Великобритании финансировали благотворительные организации, основной целью которых было проведение кампаний и лоббирование политических

---

[197] Ktepi B. Deception in political social media // K. Harvey (ed). Encyclopedia of social media and politic. Vol. 4. Thousand Oaks, CA: SAGE Publications. P. 357-359.

[198] Fielding N., Cobain I. Revealed: US spy operation that social media. [Электронный ресурс] //The Guardian. 2011. URL: https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks (дата обращения 02.12.2019).

[199] Chen A. The Agency. [Электронный ресурс] // The New York Times. 2015. URL: https://www.nytimes.com/2015/06/07/magazine/the-agency.html (дата обращения 12.03.2020).

решений. Сноуден отмечает один пример политического решения, которое поддержали 73 % пользователей, называя эту кампанию «сокпаппетом»[200].

Таким образом, сокпаппетинг предполагает создание ботнетов или программ-роботов, целью которых считается имитация общения с живыми людьми и генерирование твитов, лайков и пр. Сокпаппеты за несколько месяцев могут создать себе репутацию, историю, а также завязать доверительные отношения с пользователями социальных сетей, оказывая информационное воздействие на них.

Выводы к главе 2.

1) Социальные сети стали мощным инструментом для сознательной политики дезинформации и искажения реальности, которые могут менять достаточно быстро и в глобальном масштабе информационно-когнитивный фон в стране и регионах. Социальные сети могут служить инструментом организации социальных протестов, формирования общественного мнения, вовлечения в экстремистские группировки и продвижения экстремистских идей.

2) Кибервойна представляет собой вид военных действий с использованием сети интернет, ориентированный на основные системы жизнеобеспечения и функционирования государства. Кибервойна может включать в себя кибератаки, кибердавление и рефлексивное киберуправление. Каждый из элементов кибервойны обладает своим набором основных средств ведения войны в киберпространстве.

3) При рефлексивном киберуправлении происходит манипулирование общественным сознанием, в частности, с целью формирования политической напряженности, дезинформация граждан о работе органов государственного

[200] Snowden C. Sock Puppets: How the government lobbies itself and why [Электронный ресурс] // IEA Discussion Paper No. 39.2012. URL: https://iea.org.uk/publications/research/sock-puppets-how-the-government-lobbies-itself-and-why (дата обращения 07.02.2020).

управления. Это, в конечном счете, приводит к провоцированию столкновений религиозного, социально-политического и национального характера, подрыву авторитета власти, нанесению ущерба жизненно важным интересам государства в разных областях.

4) Исходя из того, что «общество травмы» стало современной реальностью (Ж.Т. Тощенко), нами проанализированы *травмы сознания*, проявляющиеся в разрывах ценностей и норм, усвоенных в процессе социализации, которые проявляются как новая форма политического насилия, несущая вызовы национальной безопасности. Показано, что в социальных сетях осуществляется «драматизация сознания» и манипуляция им с помощью симулякров и фейков, представленных в виде тех или иных «гуманистических» и «планетарных ценностей». Конкретно проанализированы такие формы новейших манипуляций сознанием как троллинг в социальных сетях, астротурфинг, сокпаппетинг.

5) Другим глобальным явлением в виртуальном пространстве, управление которым может быть рассмотрено как информационное оружие, выступает троллинг в соцсетях. В последние годы в рамках активного информационного противоборства внутри государств и в межгосударственных отношениях троллинг начал перемещаться из интернет-пространства в реальность. Так, он трансформировался в форму политического протеста и разговорного развлечения.

6) В социальных сетях для вовлечения и манипуляции целевой аудиторией все чаще используется астротурфинг, результатом чего является формирование в сознании пользователей новых целей, смыслов и ценностей. Идеи астротурфинга подхватываются другими пользователями и тиражируются многочисленной аудитории социальных сетей, именно поэтому повышается популярность его использования в геополитических отношениях.

7) Сокпаппетинг, как одно из направлений информационного оружия социальных сетей, предполагает создание ботнетов или программ-роботов,

целью которых считается имитация общения с живыми людьми и генерирование твиттов, лайков и пр. Сокпаппеты за несколько месяцев могут создать себе репутацию, историю, а также завязать доверительные отношения с пользователями социальных сетей, оказывая информационное воздействие на них.

8) Вместе с тем, социальные сети могут служить эффективной платформой для политического маркетинга, на которой осуществляется формирование и продвижение положительного имиджа политика, формирование общественного мнения, преломление действительности через субъективное видение определенного политического субъекта.

ЗАКЛЮЧЕНИЕ

Проведенное исследование позволяет сделать следующие выводы и обобщения, которые в концентрированной форме сформулированы в виде положений, выносимых на защиту.

Нами дана характеристика современному дигитализированному киберпространству, квинтээсенция которого видится в следующем. Благодаря гетерархической природе сетевой, ацентричной организации, киберпространство представляет собой своеобразную ризому, будучи внеструктурным и нелинейным способом формирования целостности самых разнородных смыслов. В нем отсутствует единый центр, но есть множество кластеров тесных («сильных») связей различных акторов и множество удаленных («слабых») связей с другими кластерами, все вместе образующими единую глобальную сеть. Киберпространство может постоянно копироваться, множиться и воспроизводиться благодаря каскадам бифуркаций, что характерно для нелинейно развивающегося социума. Важнейшим следствием сетевой организации киберпространства следует считать его ацентричный характер с точки зрения распределения власти: не существует общепризнанного и общепринятого кибергегемона.

Последствия функционирования киберпространства, сочетающего человеческое агентство и актанты, амбивалентны. С одной стороны, оно создает множество возможностей для быстрого доступа к общественным благам, открывает новые пути и средства для всех людей участвовать в гражданском обществе, но, с другой стороны, это также создает уникальные возможности для самых различных акторов использовать киберпространство для развертывания мощных средств-актантов стратегического действия, ведения военных операций.

Кибератаки осуществляются главным образом ради конвертации виртуальных смыслов в реальные капиталы – экономического, политического, культурного, социально-психологического, военного

характера. Киберпространство следует оценивать, прежде всего, как цифровое поле борьбы киберакторов, от индивидов до государств, за капитализацию всех уровней своего участия в его структуре.

Киберизация носит характер риск-киберизации международного порядка, поскольку именно в киберпространстве на сегодняшний день зарождаются и проявляются самые неконтролируемые, рукотворные риски с разнообразными ненамеренными последствиями, угрожающими международному порядку.

Показаны и раскрыты две тенденции в области современных международных отношений: смещение суверенитета и власти государств в область киберпространства и нарастающая зависимость их от цифровых технологий, а также диффузия кибервласти между государственными и негосударственными акторами, что вместе ведет к размыванию и ослаблению национальной безопасности как таковой.

По своей природе политическая власть в киберпространстве отличается от «классической» власти, предполагающей, навязывание воли посредством права, авторитета или традиций (М. Вебер) или способность класса, владеющими основными средствами производства, осуществлять социально-политическое господство (К. Маркс, Ф. Энгельс). Ныне «собственники средств определения» смыслов (У. Бек) фактически владеют данной политической властью, она позволяет им выражать свои политические интересы. Соответственно, кибервласть представляет собой сложную систему ресурсов, структурированных вокруг производства и обмена цифровой информации, а также контроля над ней. Её сложность, в частности, проявляется в том, ресурсы оказывают нелинейное действие: сравнительно небольшие факторы могут быть весьма значимыми по своим воздействиям на социум. Вместе с тем, кибервласть постепенно трансформируется во властную гегемонию, т.е. супервласть, которая не ограничивается контролем над сугубо кибернетическими ресурсами, включающими в себя структурные уровни киберпространства, обозначенные нами в предыдущем параграфе, но

также вбирает в себя человеческие, финансовые, экономические, символические, культурные и политические ресурсы, создаваемые или задействованные в этой системе.

«Цифровая дипломатия» подразумевает весьма широкий набор управленческих задач – и традиционных, и новых, но решаемых с помощью киберинструментов в режиме онлайн. В ситуации борьбы за кибервласть цифровая дипломатия включает в себя элементы кибердавления, т.е. стремится к неявному противостоянию с противником с целью создания благоприятных условий для реализации реальных политических действий в своих интересах.

Национальная безопасность в современных условиях во все большей степени определяется капитализированием кибервласти. Страны, которые достигнут технологического и политического превосходства в киберпространстве, будут претендовать на мировое господство. Битва за кибервласть между державами будет важнейшей характеристикой ближайших лет развития международных отношений.

Изменилась эффективность использования тех или иных инструментов насилия – они становятся информационно-цифровыми и надзорно-цифровыми. Для победы в настоящее время необходимо с помощью «игры» кодами сигнификациии принудить правящую элиту противника принять систему ценностей, интересов и норм, что возможно сделать не только с помощью военной силы, но, прежде всего, с помощью невоенных инструментов силовой политики – информационно-когнитивных средств, цифрового надзора, манипулирования общественного сознания с помощью симулякров и симуляций.

Исследование социальных сетей выявило то, что они стали мощным инструментом для сознательной политики дезинформации и искажения реальности, которые могут менять достаточно быстро и в глобальном масштабе информационно-когнитивный фон в стране и регионах.

Кибервойна представляет собой вид военных действий с использованием сети Интернет, ориентированный на основные системы жизнеобеспечения и функционирования государства. Кибервойна может включать в себя кибератаки, кибердавление и рефлексивное киберуправление. Каждый из элементов кибервойны обладает своим набором основных средств ведения войны в киберпространстве.

При рефлексивном киберуправлении происходит манипулирование общественным сознанием, в частности, с целью формирования политической напряженности, дезинформация граждан о работе органов государственного управления. Это, в конечном счете, приводит к провоцированию столкновений религиозного, социально-политического и национального характера, подрыву авторитета власти, нанесению ущерба жизненно важным интересам государства в разных областях.

Показано, что в социальных сетях осуществляется «драматизация сознания» и манипуляция им с помощью симулякров и фейков, представленных в виде тех или иных «гуманистических» и «планетарных ценностей». Конкретно проанализированы такие формы новейших манипуляций сознанием как троллинг в социальных сетях, астротурфинг, сокпаппетинг.

СПИСОК ЛИТЕРАТУРЫ

Международные правовые акты, нормативные правовые акты региональных объединений государств

1. Аннан К. При большей свободе: к развитию, безопасности и правам человека для всех / К. Аннан. Доклад Генерального секретаря ООН на 59-й сессии Генеральной Ассамблеи ООН, 2005. – 40 с. [Электронный ресурс] URL: https://www.unisdr.org/files/resolutions/N0537567.pdf (дата обращения 01.02.2020).

2. Меры укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий // ОБСЕ, 1092-е пленарное заседание : решение № 1202, PC Journal No. 1092, 2016. [Электронный ресурс]. URL: http://www.osce.org/ru/pc/228521?download=true (дата обращения 14.11.2019).

3. Неизменная приверженность свободе и демократии. Довильская декларация «Группы семи» от 27 мая 2011 года. – Довиль, 2011. [Электронный ресурс]. URL: http://kremlin.ru/supplement/946 (дата обращения 21.03.2020).

4. Окинавская хартия Глобального информационного общества (принята главами государств и правительств «Группы восьми» 22 июля 2000 года). – Окинава, 2000. [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/3170 (дата обращения 11.12.2019).

5. Convention on cybercrime // Council of Europe. European Treaty Series – No. 185. – Budapest, 2001. [Электронный ресурс]. URL:http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (дата обращения 11.12.2019).

6. Cyber Security strategy of the European Union: An open, safe and secure Cyberspace // JOIN (2013). European Commission. – Brussels, 2013.

[Электронный ресурс]. URL: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security (дата обращения 21.08.2019).

7. Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks // Official Journal L 033 , 06/02/1999 P. 0001 - 0011 [Электронный ресурс]. URL: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999D0276:EN:HTML (дата обращения 21.08.2019).

8. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016. Concerning measures for a high common level of security of network and information systems across the Union, 2016. [Электронный ресурс] URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN (дата обращения 03.10.2018).

9. The Kananaskis Summit G8 Chair's Summary. – Kananaskis, 2002. [Электронный ресурс] URL: http://www.g8.utoronto.ca/summit/2002kananaskis/summary.html (дата обращения 14.07.2019).

10. WTO Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPs). – Marrakesh, 1994. [Электронный ресурс] URL: https://www.wto.org/english/docs_e/legal_e/27-trips_01_e.htm (дата обращения 25.04.2019).

Нормативные правовые акты Российской Федерации

11. Российская Федерация. Конституция Российской Федерации : [принята всенародным голосованием 12 декабря 1993 г.]. / Официальный интернет-портал правовой информации. – Москва. – URL:

http://publication.pravo.gov.ru/Document/View/0001201408010002 (дата обращения: 12.09.2019). – Текст : электронный.

12. Российская Федерация. Законы. О безопасности : Федеральный закон № 390-ФЗ (в редакции федеральных законов от 05.10.2015 № 285-ФЗ, от 06.02.2020 № 6-ФЗ) : [принят Государственной Думой 7 декабря 2010 года : одобрен Советом Федерации 15 декабря 2010 года]. / Официальный интернет-портал правовой информации. – Москва. – URL: http://pravo.gov.ru/proxy/ips/?docbody=&nd=102144301 (дата обращения: 07.11.2019). – Текст : электронный.

13. Российская Федерация. Законы. О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации: Федеральный закон № 164-ФЗ : [принят Государственной Думой 12 сентября 2008 года : одобрен Советом Федерации 19 сентября 2008 года]. / Официальный интернет-портал правовой информации. – Москва. – URL: http://pravo.gov.ru/proxy/ips/?searchres=&bpas=cd00000&a3=&a3type=1&a3value=&a6=&a6type=1&a6value=&a15=&a15type=1&a15value=&a7type=1&a7from=&a7to=&a7date=&a8=164&a8type=1&a1=%CE+%F0%E0%F2%E8%F4%E8%EA%E0%F6%E8%E8+%D1%EE%E3%EB%E0%F8%E5%ED%E8%FF+%EE+%F1%EE%F2%F0%F3%E4%ED%E8%F7%E5%F1%F2%E2%E5+%E3%EE%F1%F3%E4%E0%F0%F1%F2%E2++%F3%F7%E0%F1%F2%ED%E8%EA%EE%E2+%D1%EE%E4%F0%F3%E6%E5%F1%F2%E2%E0+%CD%E5%E7%E0%E2%E8%F1%E8%EC%FB%F5+%C3%EE%F1%F3%E4%E0%F0%F1%F2%E2+%E2+%E1%EE%F0%FC%E1%E5+%F1+%EF%F0%E5%F1%F2%F3%EF%EB%E5%ED%E8%FF%EC%E8+%E2+%F1%F4%E5%F0%E5+%EA%EE%EC%EF%FC%FE%F2%E5%F0%ED%EE%E9+%E8%ED%F4%EE%F0%EC%E0%F6%E8%E8&a0=&a16=&a16type=1&a16value=&a17=&a17type=1&a17value=&a4=&a4type=1&a4value=&a23=&a23type=1&a23value=&textpres=&sort=7&x=75&y=16 (дата обращения: 09.03.2019). – Текст : электронный.

14. Российская Федерация. Законы. О средствах массовой информации : Федеральный закон № 2124-1- ФЗ : [принят Верховным Советом России и подписан Президентом РСФСР 27 декабря 1991 года]. / Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) : официальный сайт. – Москва. – URL: https://rkn.gov.ru/mass-communications/smi-registation (дата обращения: 12.06.2019). – Текст : электронный.

15. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации : Федеральный закон № 149-ФЗ : [принят Государственной Думой 8 июля 2006 года : одобрен Советом Федерации 14 июля 2006 года]. / Официальный интернет-портал правовой информации. – Москва. – URL: http://pravo.gov.ru/proxy/ips/?docbody&nd=102108264 (дата обращения: 27.10.2019). – Текст : электронный.

16. Российская Федерация. Подзаконные акты. О государственной программе Российской Федерации "Информационное общество (2011-2020 годы)": Распоряжение Правительства Российской Федерации от 20 октября 2010 г. № 1815-р (в ред. Постановления Правительства Российской Федерации от 18.05.2011 г. N 399) / Официальный интернет-портал правовой информации. – Москва. – URL: http://pravo.gov.ru/proxy/ips/?doc_itself=&nd=102142714&page=1&rdk=13#I0 (дата обращения: 15.06.2019). – Текст : электронный.

17. Российская Федерация. Подзаконные правовые акты. О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена: Указ Президента Российской Федерации № 351 (в ред. Указов Президента РФ от 21.10.2008 № 1510, от 14.01.2011 № 38) : [издан Президентом Российской Федерации 17 марта 2008 года]. / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) : официальный сайт. –

Москва. – URL: https://digital.gov.ru/common/upload/UKAZ_351_1.pdf (дата обращения: 01.02.2020). – Текст : электронный.

18. Российская Федерация. Подзаконные правовые акты. О признании утратившим силу Указа Президента Российской Федерации от 5 февраля 2010 г. №146 «О Военной доктрине Российской Федерации»: Указ Президента Российской Федерации № 815: [издан Президентом Российской Федерации 25 декабря 2014 года]. / Официальный интернет-портал правовой информации. – Москва. – URL: http://publication.pravo.gov.ru/File/GetFile/0001201412260001?type=pdf (дата обращения: 03.02.2019). – Текст : электронный.

19. Российская Федерация. Правовые доктрины. Военная доктрина Российской Федерации : [утверждена Президентом Российской Федерации 25 декабря 2014 года, Пр-2976]. / Президент Российской Федерации: официальный сайт. – Москва. – URL: http://static.kremlin.ru/media/events/files/41d527556bec8deb3530.pdf (дата обращения: 04.04.2019). – Текст : электронный.

20. Российская Федерация. Правовые доктрины. Государственная программа Российской Федерации "Информационное общество (2011-2020 годы)" : [утверждена Постановлением Правительства Российской Федерации № 313 от 15 апреля 2014 года]. / Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации (Минкомсвязь России) : официальный сайт. – Москва. – URL: https://digital.gov.ru/ru/documents/4137 (дата обращения: 07.03.2020). – Текст : электронный.

21. Российская Федерация. Правовые доктрины. Доктрина информационной безопасности Российской Федерации : [утверждена Указом Президента Российской Федерации № 646 от 5 декабря 2016 года]. / Президент Российской Федерации: официальный сайт. – Москва. – URL: http://www.kremlin.ru/acts/bank/41460 (дата обращения: 04.04.2019). – Текст : электронный.

22. Российская Федерация. Правовые доктрины. Концепция внешней политики Российской Федерации : [утверждена Указом Президента Российской Федерации № 640 от 30 ноября 2016 г.]. / Президент Российской Федерации: официальный сайт. – Москва. – URL: http://www.kremlin.ru/acts/bank/41451 (дата обращения: 04.04.2019). – Текст : электронный.

23. Российская Федерация. Правовые доктрины. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года : [утверждены Президентом Российской Федерации 24 июля 2013 года, № Пр-1753]. / Совет Безопасности Российской Федерации : официальный сайт. – Москва. – URL: http://www.scrf.gov.ru/security/information/document114 (дата обращения: 15.09.2019). – Текст : электронный.

24. Российская Федерация. Правовые доктрины. Стратегия национальной безопасности Российской Федерации : [утверждена Указом Президента Российской Федерации N 683 от 31 декабря 2015 года]. / Президент Российской Федерации: официальный сайт. – Москва. – URL: http://www.kremlin.ru/acts/bank/40391/page/1 (дата обращения: 20.06.2018). – Текст : электронный.

25. Российская Федерация. Правовые доктрины. Стратегия национальной безопасности Российской Федерации до 2020 года: [утверждена Указом Президента Российской Федерации N 537 от 12 мая 2009 года]. / Президент Российской Федерации: официальный сайт. – Москва. – URL: http://www.kremlin.ru/supplement/424 (дата обращения: 20.06.2018). – Текст : электронный.

26. Российская Федерация. Правовые доктрины. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы : [утверждена Указом Президента Российской Федерации № 203 от 9 мая 2017 года]. / Президент Российской Федерации: официальный сайт. – Москва. –

URL: http://www.kremlin.ru/acts/bank/41919 (дата обращения: 24.01.2019). – Текст : электронный.

27. Российская Федерация. Правовые доктрины. Федеральной целевая программа "Электронная Россия (2002 – 2010 годы)" (с изменениями от 26 июля 2004 г.) : [утверждена Постановлением Правительства Российской Федерации N 65 от 28 января 2002 года]. / Министерство экономического развития Российской Федерации : официальный сайт. – Москва. – URL: http://old.economy.gov.ru/minec/activity/sections/fcp/doc1096611747891 (дата обращения: 11.03.2019). – Текст : электронный.

Нормативные правовые акты иностранных государств

28. Четырнадцать пунктов В.Вильсона об условиях мира (из его послания Конгрессу США). 8 января 1918 г. // Международная политика новейшего времени в договорах, нотах и декларациях. Под ред. проф. Ю.В. Ключникова и А.Сабанина. – Ч. II. – М.: Литиздат НКИД, 1926. – С. 108–110.

29. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities: US President Executive Order 13694 // Federal Register ,Vol. 80, No. 63, 2015. – 3 p.

30. Clinton Administration’s Policy on Critical Infrastructure Protection: Presidential Decision Directive 63 [Factsheet and White Paper] // USDA Office of Procurement and Property Management, Physical Security Program. – Washington D.C., 1998. – 14 p. [Электронный ресурс] URL: https://www.hsdl.org/?abstract&did=456517 (дата обращения 21.02.2018).

31. Critical Infrastructure Protection: US President Executive Order 13010 // Federal Register Vol. 61, No. 138. – Washington, D.C., 1996. – 6 p.

32. Department of Defense Strategy for Operating in Cyber Space. – U. S. Department of Defense, 2011. – 19 p. [Электронный ресурс] URL: https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf (дата обращения 12.07.2019).

33. Establishing the Office of Homeland Security and the Homeland Security Council: US President Executive Order 13228 // Federal Register, Vol. 66, No. 196, 2001. – 6 p.

34. Homeland Security : Presidential Directive Hspd-7 // Office of the President Press Secretary of the United States. – Washington, D.C., 2003. – 10 p. [Электронный ресурс] URL: https://www.energy.gov/sites/prod/files/HSPD-7.pdf (дата обращения 04.07.2019).

35. IT Strategic Plan: Fiscal Years 2011-2013 – Digital Diplomacy // US Department of State. – Washington, D.C., 2010. – 20 p. [Электронный ресурс] URL: https://2009-2017.state.gov/documents/organization/147678.pdf (дата обращения 09.04.2019).

36. National Security Strategy of the United States of America // SEAL of The President of the United States. – Washington, D.C, 2010. – 60 p. [Электронный ресурс]. URL: https://2009-2017.state.gov/documents/organization/147678.pdf (дата обращения 09.04.2019).

37. National Security Strategy of the United States of America // The White House Office. – Washington D.C., 2017. – 68 p. [Электронный ресурс] URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf (дата обращения 20.02.2018).

38. The Department of Defense Cyber Strategy // The Department of Defense of the United States – Washington, D.C., 2015. – 42 p. [Электронный ресурс] URL: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (дата обращения 17.12.2018).

39. The National Strategy for Homeland Security // The Department of Homeland Security of the United States. – Washington D.C., 2002. – 90 p. [Электронный ресурс]. URL: https://www.dhs.gov/sites/default/files/publications/nat-strat-hls-2002.pdf (дата обращения 20.03.2018).

40. The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets // Executive Office of the President of the United States. – Washington D.C., 2003. – 96 p. [Электронный ресурс] URL: https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (дата обращения 20.03.2018).

41. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 // One Hundred Seventh Congress of the United States of America AT THE FIRST SESSION; H.R. 3162. – Washington D.C., 2001. – 131 p. [Электронный ресурс] URL: https://www.congress.gov/107/bills/hr3162/BILLS-107hr3162enr.pdf (дата обращения 11.07.2019).

Монографии, учебники, учебные и справочные издания, словари

42. Актуальные проблемы противодействия терроризму и экстремизму: тематический сборник / Под ред. В.В.Красинского. – М., 2017. – 221 с.

43. Алексеева Т.А. Современная политическая мысль (XX–XXI вв.): политическая теория и международные отношения / Т.А. Алексеева. – М.: Аспект Пресс, 2015. – 623 с.

44. Алексеева Т.А. Современные политические теории / Т.А. Алексеева. – М.: РОССПЭН, 2000. – 343 с.

45. Алексеева Т.А., Минеев А.П., Лошкарёв И.Д., Ананьев Б.И. «Квантовый подход» к международным отношениям / Т.А. Алексеева, А.П. Минеев, И.Д. Лошкарёв, Б.И. Ананьев. – М.: Знание Сила, 2018. – 110 с.

46. Амелин В.Н. Социология политики / В.Н. Амелин. – М., 1992. – 61 с.

47. Антюхова Е.А. Публичная дипломатия: теория и практика / Е.А. Антюхова, Б.Х. Бахриев, К.П. Боришполец, Х.Р. Джаббари Насир, Е.С. Зиновьева, Т.В.Зонова, В.В. Каберник, М.М. Лебедева, Ю.А. Никитина, А.И.

Подберезкин, О.А. Тимофеева, М.В. Харкевич, Д.Д. Шебалин, Е.О. Шебалина ; под ред. Лебедевой М.М. – М: Аспект Пресс, 2017. – 272 с.

48. Банке Б., Бутенко В., Коцур О. Россия онлайн: влияние интернета на российскую экономику. Отчет [Электронный ресурс] / Б.Банке, В.Бутенко, О.Коцур. – The Boston Consulting Group, 2011. – 42 с. URL: http://img.rg.ru/pril/article/48/57/59/000111333.pdf (дата обращения 02.11.2019).

49. Баталов Э.Я. Политическая культура современного американского общества / Э.Я. Баталов. – М., 1990. – 154 с.

50. Бек У. Что такое глобализация? / У. Бек. – М.: Прогресс-Традиция, 2001. – 304 с.

51. Беляков А. В., Матвейчев О.А. Большая актуальная политическая энциклопедия / А.В. Беляков, О.А. Матвейчев и др. – М: Эксмо, 2009. – 412с.

52. Бжезинский З. Между двумя веками: роль Америки в эру технотроники / З. Бжезинский. – М.: Прогресс, 1972. – 308 с.

53. Богатуров А.Д. Очерки теории и политического анализа международных отношений / А.Д. Богатуров, Н.А. Косолапов, М.А. Хрусталев; научно-образоват. форум по междунар. отношениям. – М. 2002. – 380 с.

54. Богатуров А.Д., Хрусталев М.А., Косолапов И.А. Очерки теории и политического анализа международных отношений / А.Д. Богатуров, М.А. Хрусталев, И.А. Косолапов. – М.: НОФМО, 2002. – 380 с.

55. Бодрийяр Ж. К критике политической экономии знака / Ж. Бодрийяр – М.: Библион-Русская книга, 2003. – 272 с.

56. Боришполец К.П. Методы политических исследований: Учебное пособие для студентов вузов. 2-е изд. испр. и доп. / К.П. Боришполец. – М.: Аспект Пресс, 2010. – 230 с.

57. Бурдье П. Социальное пространство: поля и практики / П. Бурдье. – М.: Институт экспериментальной социологии, 2007. – 576 с.

58. Бурдье П. Социология социального пространства / П. Бурдье. – М.: Институт экспериментальной социологии, 2007. – 288 с.

59. Веселов В.А. Международная безопасность и контроль над вооружениями / В.А.Веселов.– М.: Макс-Пресс, 2005. – 201 с.

60. Гарр Т. Почему люди бунтуют / Т.Гарр. – СПб.: Питер, 2005. – 461 с.

61. Гидденс Э. Последствия современности. – М.: «Праксис», 2011. – 352 с.

62. Гнатюк О.Л. Основы теории коммуникации / О.Л. Гнатюк. – М. : КНОРУС, 2012. – 256 с.

63. Григорьев М.С., Игнатов В.С., Магеров В.М. Противодействие террористической пропаганде / М.С. Григорьев, В.С. Игнатов, В.М. Магеров. – М.: Фонд исследования проблем демократии, 2017. – 112 с.

64. Гринберг Т.Э. Политические технологии / Т.Э. Гринберг. – М. : Аспект Пресс, 2012. – 280 с.

65. Гринвальд Г. Негде спрятаться. Эдвард Сноуден и зоркий глаз Дядюшки Сэма. [пер. Т. Зверевич, С. Силинский]. / Г. Гринвальд. – СПб.: Питер, 2014. – 320 с.

66. Гриняев С.Н. Поле битвы – киберпространство: Теория, приемы, средства, методы и системы ведения информационной войны / С.Н. Гриняев. – М.: Харвест, 2004. – 448 с.

67. Деева А.К., Коробейник В.А. Экстремистская деятельность в сети интернет / А.К. Деева, В.А. Коробейник. // Профилактика и противодействие идеологии религиозно-политического терроризма и экстремизма в современной России: проблемы и перспективы: сб. ст. по материалам всерос. научно-практ. конф., Белгород, 15 июня 2017 г. / НИУ БелГУ. – Белгород, 2018. – 100 с. – С.63–65.

68. Демидов О. Глобальное управление Интернетом и безопасность в сфере использования ИКТ: Ключевые вызовы для мирового сообщества / О.Демидов. – М.: Алпина Паблишер, 2016. – 198 с.

69. Казаринова Н.В. Основы теории коммуникации / Н.В. Казаринова. – СПб.: Роза мира, 2006. – 224 с.

70. Кастельс М. Становление общества сетевых структур / М. Кастельс // Новая постиндустриальная волна на Западе: Антология. – М.: Academia, 1999. – С.494–505.

71. Киссинджер Г. Мировой порядок / Г. Киссинджер. – М.: АСТ, 2015 – 512 с.

72. Клаузевиц К. «О войне» / К. Клаузевиц. – М.: АСТ, 2019. – 352 с.

73. Козин В.П., Карякин В. В. Политика и стратегия США в геополитической динамике XXI века / Козин В.П., Карякин В. В. – М: Граница. 2014. – 368 с.

74. Кокошин А.А. Политико-военные и военно-стратегические проблемы национальной безопасности России и международной безопасности / А.А.Кокошин. – М.: Высшая школа экономики, 2013. – 261 с.

75. Конышев В.Н. Американский неореализм о природе войны: эволюция политической теории / В.Н.Конышев. – СПб: Наука, 2004 – 372 с.

76. Корконосенко С.Г. Социология журналистики / С.Г. Корконосенко и др. – М. : Аспект Пресс, 2004. – 421 с.

77. Кравченко С.А. Социология в 2-х тт. Т.1. Классические теории через призму социологического воображения / С.А. Кравченко. Учебник для академического бакалавриата. – М.: Юрайт, 2014. – 584 с.

78. Кравченко С.А. Социология в 2-х тт. Т.2. Новые и новейшие социологические теории через призму социологического воображения. Учебник для академического бакалавриата. – М.: Юрайт., 2014. – 636 с.

79. Кулагин В.М. Международная безопасность / В.М. Кулагин. – М.: Аспект Пресс, 2007. – 318 с.

80. Лебедева М.М. Мировая политика: учебник для бакалавров. Изд. 2-е., перераб. / М.М. Лебедева. – М.: Кнорус, 2013.– 254 с.

81. Лефевр В.А. Конфликтующие структуры. Издание второе, переработанное и дополненное / В.А. Лефевр. – М.: «Советское радио», 1973. – 158 с.

82. Лефевр В.А. Лекции по теории рефлексивных игр / В.А. Лефевр. – М.: «Когито-Центр», 2009. – 218 с.

83. Луман Н. Введение в системную теорию / Н.Луман. – М.: "Логос", 2007. – 360 с.

84. Луман Н. Социальные системы / Н.Луман. – СПб.: Наука, 2007. – 641 с.

85. Луман Н. Социальные системы. СПб.: Наука, 2007.

86. Маклюэн М. Галактика Гуттенберга: становление человека печатающего / М.Маклюэн. – М.: Академический проект: Фонд «Мир», 2005. – 496 с.

87. Маклюэн М. Понимание медиа: внешние расширения человека / М.Маклюэн. – М.: Канон-пресс, 2003. – 464 с.

88. Манойло А.В. Государственная информационная политика в особых условиях / А.В. Манойло. – М.: МИФИ, 2003. – 388 с.

89. Маркс К. Социология. Сборник. М.: «КАНОН-пресс-Ц», «Кучково поле», 2000.

90. Мелюхин И.С. Информационное общество: истоки, проблемы, тенденции развития / И.С. Мелюхин. – М. 1999. – 206 с.

91. Мир 2035. Глобальный прогноз / под ред. акад. А.А. Дынкина / ИМЭМО РАН. М.: Магистр, 2017. – 352 с.

92. Московичи С. Век толп / С. Московичи. – М., 1996. – 189 с.

93. Най Дж. Будущее власти: как стратегия умной силы меняет XXI век / Дж. Най. – М.: АСТ, 2014. – 444 с.

94. Некоторые аспекты анализа военно-политической обстановки: монография / под ред. А.И. Подберёзкина. – М.: МГИМО-Университет, 2014. – 874 с.

95. Никольсон Г. Дипломатическое искусство / Г. Никольсон. – М.: Книга по Требованию, 2013. – 118 с.

96. Панарин И.И. Типология информационной войны / И.И. Панарин. – М.: КСП, 2003. – 320 с.

97. Панарин И.Н. Технология информационной войны / И. Н. Панарин. – М.: КСП +, 2003. – 320с.

98. Панарин С.А. Безопасность как ценность и норма: опыт разных эпох и культур / С.А.Панарин. – СПб: Интерсоцис, 2012. – 296 с.

99. Парсонс Т. О понятии «политическая власть» // Антология мировой политической мысли. Т.2. М., 1997.

100. Парсонс Т. Система современных обществ / Т.Парсонс. – М.: Аспект Пресс, 1998. – 269 с.

101. Петровский В.Ф. Американская внешнеполитическая мысль. Критический обзор организации, методов и содержания буржуазных исследований в США по вопросам международных отношений и внешней политики / В.Ф.Петровский. – М.: «Международные отношения», 1976. – 336 с.

102. Подберезкин А.И. Национальный человеческий капитал т.3 / А.И. Подберезкин. – М.: МГИМО-Университет, 2011. – 848 с.

103. Подберезкин А.И. Проект долгосрочной стратегии национальной безопасности России с методологическими и методическими комментариями / А.И. Подберезкин, М.В. Харкевич, М.В. Александров, О.Е. Родионов. – М : МГИМО-Университет, 2016. – 88 с.

104. Подберезкин А.И. Стратегия национальной безопасности России в XXI веке / А.И. Подберезкин. – М: МГИМО-Университет, 2016. – 338 с.

105. Подберезкин А.И., Александров М.В. Мир в XXI веке: прогноз развития международной обстановки по странам и регионам: монография; под ред. М.В. Александрова, О.Е. Родионова; МГИМО, Центр военно-политических исследований / А.И. Подберезкин, М.В. Александров. – М., 2018. – 768 с.

106. Попов В.Д. Тайны информационной политики (социокоммуникативный психоанализ информационных процессов) / В.Д. Попов. – М: РАГС, 2007. – 301 с.

107. Попов И.М., Хамзатов М.М. Война будущего: Концептуальные основы и практические выводы. Очерки стратегической мысли / И.М. Попов, М.М.Хамзатов. – М.: Кучково поле, 2016. – 832 с.

108. Почепцов Г.Г. Имиджелогия / Г.Г. Почепцов. – М. : Рефл-бук, 2001. – 704 с.

109. Почепцов Г.Г. Информационные войны/ Г.Г. Почепцов. – М. : Рефл-бук, 2000. – 576 с.

110. Проблемы информационной безопасности в международных военно-политических отношениях; под ред. А.В. Загорского, Н.П. Ромашкиной. – М.: ИМЭМО РАН, 2016. –183 с.

111. Роговский Е. США: информационное общество. Экономика и политика / Е. Роговский. – М.: Международные отношения, 2008. – 408с.

112. Сазанов В.М. Социальные сети – публичная сфера / В.М.Сазанов. – М.: Лаборатория СВМ, 2012. – 225 с.

113. Сетов Н.Р. Политический реализм: теория и метод / Н.Р. Сетов. – М.: Издательство Московского университета, 2013. – 184 с.

114. Системный мониторинг глобальных и региональных рисков: Арабский мир после Арабской весны / Отв.ред. А.В. Коротаев, Л.М. Исаев, А.Р.Шишкина. – М.: ЛЕНАНД, 2013. – 430 с.

115. Стратегическое сдерживание: новый тренд и выбор российской политики / А.И. Подберёзкин, М.В. Александров, К.П. Боришполец и др.; под ред. К.П.Боришполец, О.Е.Родионова. – М.: МГИМО-Университет, 2019. – 656 с.

116. Тоффлёр Э. Третья волна / Э. Тоффлёр под ред. П.С. Гуревича. М.: АСТ, 1999. – 784 с.

117. Тощенко Ж.Т. Общество травмы: между эволюцией и революцией (опыт теоретического и эмпирического анализа) / Ж.Т. Тощенко. – М: Весь Мир, 2019. – 344 с.

118. Тощенко Ж.Т. Общество травмы: между эволюцией и революцией (опыт теоретического и эмпирического анализа) / Ж.Т. Тощенко. – Москва: Весь Мир, 2020. – 352 с.

119. Туровский Д. Вторжение. Краткая история русских хакеров / Д.Туровский. – М.: Издательство Individuum, 2019. – 296 с.

120. Уткин А.И. Новый мировой порядок / А.И.Уткин. – М.: Алгоритм, Эксмо, 2006. – 640 с.

121. Фененко А.В. Современная международная безопасность: Ядерный фактор / А.В. Фененко. – М: Аспект Пресс, 2013. – 573 с.

122. Фуко М. Воля к истине: по ту сторону власти, знания и сексуальности / М. Фуко. – М.: Касталь, 1996. – 448 с.

123. Фуко М. Интеллектуалы и власть: Избранные политические статьи, выступления и интервью. М.: Праксис, 2002. – 384 с.

124. Хабермас Ю. Вовлечение другого. Очерки политической теории / Ю.Хабермас. – СПб.: Наука. 2001. – 417 с.

125. Харрис Ш. Кибервойн@: пятый театр военных действий / Ш. Харрис. – М.: Альпина нон-фикшин, 2016. – 392 с.

126. Хрусталев М.А. Методология прикладного политического анализа / М.А.Хрусталев. – М.: Проспект, 2010. – 158 с.

127. Хрусталев М.А. Методология прикладного политического анализа: учебное пособие / М.А. Хрусталев / Московский гос. ин-т междунар. отношений (ун-т) МИД России, Инновационная образовательная прогр. – М.: Проспект, 2010. – 158 с.

128. Цветкова Н.А. Cultural Imperialism: международная образовательная политика США в период «холодной войны» / Н.А. Цветкова. – СПб.: СПбГУ, 2007. – 195 с.

129. Чугунов А.В. Развитие информационного общества: теории, концепции и программы: учебное пособие / А.В. Чугунов. – СПб.: Ф-т филологии и искусств СПбГУ, 2007. – 98 с.

130. Шаклеина Т.А. Россия и США в мировой политике / Т.А. Шаклеина. – М.: Аспект Пресс, 2012. – 272 с.

131. Шваб К. Четвертая промышленная революция / К. Шваб. – М.: «Эксмо», 2016. – 230 р.

132. Шершнёв И. Л. Общественная дипломатия России в глобализирующемся мире / И.Л. Шершнёв. – М.: МосГУ, 2011. – 303 с.

133. Щекотихин В. М., Королёв А. В., Королёва В. В. Информационная война. Информационное противоборство: теория и практика / В. М. Щекотихин, А. В. Королёв, В. В. Королёва и др. – М : Акад. ФСО России, 2011. – 999 с.

134. Acquisti A., Gross R. Information Revelation and Privacy in Online Social Networks (The Facebook case) / A.Acquisti, R.Gross // Pre-proceedings version. ACM Workshop on Privacy in the Electronic Society (WPES), 2005. – 11 p.

135. Alexander J. C. The Meaning of Social Life: A Cultural Sociology / J.C. Alexander. – New York: Oxford University Press, 2003. – 296 p.

136. Alexander G., Bennett A. Case studies and theory development in the social sciences / G. Alexander, A. Bennett. – Cambridge: The MIT Press, 2005. – 352 p.

137. Alexander J. C. The Civil Sphere. Oxford University Press, 2006.

138. Alexander J.C. The Drama of Social Life / J.C. Alexander. – Cambridge: Polity Press, 2017. – 189 p.

139. Alexander J.C. The meaning of social life: a cultural sociology / J.C. Alexander. – Oxford: Oxford University Press, 2003. – 296 p.

140. Alexander J.C. Trauma: A Social Theory / J.C. Alexander. – Cambridge: Polity Press, 2012. – 232 p.

141. Attkisson S. Stonewalled: My Fight for Truth Against the Forces of Obstruction, Intimidation, and Harassment in Obama's Washington / S. Attkisson. – New York: Harper, 2014. – 434 p.

142. Bauman Z., Donskis L. Liquid Evil / Z. Bauman, L. Donskis. – Cambridge: Polity Press, 2016. – 170 p.

143. Baumer D.C., Van Horn C.E. Politics and Public Policy: Strategic Actors and Policy Domains, 4th ed. / D.C.Baumer, C.E. Van Horn. – CA: SAGE Publications, Inc, 2014. – 416 p.

144. Beck U. Twenty Observations on a World in Turmoil / U.Beck. – Cambridge: Polity Press, 2012. – 162 p.

145. Beck U. World at Risk / U. Beck. – Cambridge: Polity Press, 2010. – 269 p.

146. Braidotti R. The Posthuman / R. Braidotti. – Cambridge: Polity Press, 2015. – 180 p.

147. Carr J. Inside cyber warfare / J. Carr. – Sebastopol, CA: O'Reilly Media, 2010. – 234 p.

148. Castells M. The Information Age: Economy, Society and Culture. Vol.I: The Rise of the Network Society. 2-nd ed. / M. Castells. – Cambridge MA / Oxford UK: Blackwell Publishers, 2010. – 657 p.

149. Castells M. The Information Age: Economy, Society and Culture. Vol.II: The Power of Identity / M. Castells. – Malden MA/ Oxford UK: Blackwell Publishers, 1996. – 584 p.

150. Castells M. The Internet Galaxy: Reflexions on the Internet, Business, and Society / M.Castells. – Oxford: Oxford University Press, 2002. – 292 p.

151. Davis P., Cragin K. Social science for counterterrorism: putting the pieces together / P. Davis , K. Cragin. – RAND Corporation, 2009. – 540 p. [Электронный ресурс]. URL: https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG849.pdf (дата обращения 04.02.2020)

152. Davis P., Larson E., Haldeman Z., Oguz M., Rana Y. Understanding and influencing public support for insurgency and terrorism / P.Davis, E. Larson , Z. Haldeman , M. Oguz, Y.Rana. – RAND Corporation, 2012. – 270 p. [Электронный ресурс]. URL: https://www.rand.org/content/dam/rand/pubs/monographs/2012/RAND_MG1122.pdf (дата обращения 03.03.2020).

153. Davis P., O'Mahony A. A computational model of public support for insurgency and terrorism: a prototype for more-general social-science modeling. / P. Davis, A. O'Mahony. – RAND Corporation, 2013. – 110p. [Электронный ресурс]. URL: https://www.rand.org/content/dam/rand/pubs/technical_reports/TR1200/TR1220/RAND_TR1220.pdf (дата обращения 14.08.2019).

154. Deleuze G., Guattari F. A Thousand Plateaus / G.Deleuze, F.Guattari. – Minneapolis: University of Minnesota Press, 1987. – 629 p.

155. Emerson R.M. Power-Dependence Relations // American Sociological Review № 27, 1962.

156. Fuchs C. Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook, and MySpace by Students in Salzburg in the Context of Electronic Surveillance / C. Fuchs. – Salzburg/Vienna: Forschungsgruppe "Unified Theory of Information" – VereinzurForderung der Integration der Informationswissenschaften, 2009. – 145 p.

157. Grauman B. Cyber Security: The Vexed Question of Global Rules. An independent report on cyber-preparedness around the world. Brussels, 2012. [Электронный ресурс] URL: https://pdfs.semanticscholar.org/5259/62263586710d90abbb3584236ff835cc5f0f.pdf?_ga=2.152765370.26273978.1588134073-398395631.1585861038 (дата обращения 11.07.2019).

158. Jaynes E., Bretthorst L. Probability theory: the logic of science / E.Jaynes, L. Bretthorst. – Cambridge, UK: Cambridge University Press, 2003. – 758 p.

159. Jordan T. Cyberpower: The Culture and Politics of Cyberspace and the Internet / T. Jordan. – London: Routledge, 1999. – 254 p.

160. Kelly J., Etling B. Mapping Iran's online public: politics and culture in the Persian blogosphere / J. Kelly, B. Etling. – Cambridge, USA: Harvard Law School, 2008. – 36 p.

161. Kelly J., Etling B., Faris R. Mapping the Arabic blogosphere: politics, culture and dissent / J. Kelly, B. Etling, R. Faris. – Cambridge, USA: Harvard Law School, 2009. – 62 p.

162. Kremer J.F., Muller B. (eds). Cyberspace and International Relations: Theory, Prospects and Challenges / J.F. Kremer, B. Muller. – Heidelberg: Springer, 2014. – 284 p.

163. Latour B. The Pasteurization of France / B. Latour. – Cambridge, MA: Harvard University Press, 1988. – 273 c.

164. Latour B., Woolgar S. Laboratory Life: The Construction of Scientific Facts / B. Latour, S. Woolgar. – Princeton: Princeton University Press, 2013. – 296 p.

165. Mosco V. Becoming Digital. Toward a Post-Internet Society / V. Mosco. –Bingley: Emerald Publishing Limited, 2017. – 227 p.

166. Nye J.S. The future of power / J.S.Nye // Public Affairs, 2011. – 320 p.

167. Nye J.S., Jr. Soft Power: The Means to Success in World Politics / J.S. Nye, Jr. – New York: Public Affairs, 2004. – 192 p.

168. Nye J.S., Jr. The Future of Power / J.S. Nye, Jr.– New York: Public Affairs, 2011. – 320 p.

169. Perrow Ch. Normal Accidents: Living with High Risk Technologies / Ch. Perrow. – New Brunswick, NJ: Rutgers University Press, 1999. – 464 p.

170. Preparing for the Future of Artificial Intelligence. – Washington: Executive Office of the President National Science and Technology Council Committee on Technology, 2016. – 48 p.

171. Report on the 5th Science and Technology Basic Plan. – Tokyo: Council for Science, Technology and Innovation, Cabinet Office, Government of Japan, 2015. – 23 p.

172. Richards H., Pherson R. Structured analytic techniques for intelligence analysis / H. Richards, R. Pherson. – Washington, DC: CQ Press, 2011. – 384 p.

173. Snowden C. Sock puppets: How the government lobbies itself and why. // Discussion Paper No.39. – Institute of Economic Affairs, 2012. – 39 p. [Электронный ресурс] URL: https://iea.org.uk/publications/research/sock-puppets-how-the-government-lobbies-itself-and-why (дата обращения 17.01.2020).

174. Turkle S. Alone Together: why we expect more from technology and less from each other / S Turkle. – New York: Basic Books, 2011. – 384 p.

175. Urry J. Climate Change and Society / J. Urry. – Malden: Polity Press, 2011. – 166 p.

176. Urry J. Global Complexity / J. Urry. – Cambridge: Polity Press, 2003. – 172 p.

177. Vanderburg W.H. Our War on Ourselves / W.H. Vanderburg. – Toronto: University of Toronto Press, 2011. – 400 p.

178. Ventre D. Information Warfare. 2nd edition / D.Ventre. – London: ISTE Ltd and John Wiley & Sons Inc, 2016. – 352 p.

179. Williamson J. In defense of objective Bayesianism / J. Williamson. – Oxford, UK: Oxford University Press, 2010. – 200 p.

Диссертации и авторефераты

180. Батуева Е.В. Американская концепция угроз информационной безопасности и ее международно-политическая составляющая : дис. канд. полит. наук: 23.00.04 / Е.В. Батуева. – Москва, 2015. – 207 с.

181. Биккулов А.С. Интернет как средство массовой коммуникации : дис. канд. социол. наук: 22.00.06 / А.С. Биккулов. – Санкт-Петербург, 2003. – 217 с.

182. Карякина К.А. Особенности журналистского и пользовательского контента в интернете: автореф. дис. канд. филол. наук: 10.01.10 / К.А. Карякина.– Москва, 2011. – 36 с.

183. Лещенко А.М. Социальные сети как механизм конструирования коммуникации в современном обществе : дис. канд. философ. наук: 09.00.11 / А.М. Лещенко. – Пятигорск, 2011. – 158 с.

184. Михеев А.Н. Принятие внешнеполитических решений в условиях развития новых информационных технологий: роль международных неправительственных организаций: дис. канд. полит. наук: 23.00.04 / А.Н. Михеев. – Москва, 2005. – 195 с.

185. Шеремет А.Н. Интернет как средство массовой коммуникации: социологический анализ: дис. канд. социол. наук: 22.00.06 / А.Н. Шеремет. – Екатеринбург, 2003. – 167 с.

186. Щербаль С.С. Технологии политической пропаганды в избирательных кампаниях российских партий: на примере парламентских выборов: автореф. дис. канд. полит. наук: 23.00.02 / С.С. Щербаль. – Краснодар, 2012. – 23 с.

Статьи в научных периодических изданиях и сборниках

187. Атанесян А.В. “Бархатная революция” в армении: потенциал, достижения и риски политико-протестной активности // Полис. Политические исследования. 2018. № 6. – С.80-98.

188. Большова Н.Н. “Пегида” как пример массовых протестных движений, возникших в Европе под влиянием миграционного кризиса // Полис. Политические исследования. 2016. № 3. – С.123-137.

189. Бондаренко С.В. Виртуальные сетевые сообщества девиантного поведения // Погосян Л.А., Бондаренко С.В., Черноус В.В. Профилактика девиантного поведения молодёжи Дона и Юга России. – Ростов-на-Дону: СКНЦ ВЩ, 2003. – С. 54-88.

190. Бондаренко С.В. Особенности создания и функционирования публичных площадок «электронной демократии» // Полис № 5, 2011. – С. 164-178.

191. Борисов С.В. Сущность преступлений экстремистской направленности // Мировой судья. №4. 2009. – С. 12-15.

192. Бутусов А.В. Социальные сети как инструмент политического противоборства и информационных войн // Вестник Тамбовского университета. Серия: Общественные науки. №13. 2018. – С. 71-75.

193. Васильев А.А. Манипуляция общественным мнением через виртуальные сообщества // Христианское чтение. –№5. 2016. – С. 207-222.

194. Внебрачных Р.А. Троллинг как форма социальной агрессии в виртуальных сообществах // Вестник Удмуртского университета. Серия «Философия. Психология. Педагогика». №1. 2012. – С. 36-39.

195. Володенков С.В., Митева В.В. Сетевые информационные войны в современных условиях: основные акторы и стратегии // PolitBook. 2016. №3. – С. 18-35.

196. Воронина И.А. Первые публикации Народного комиссариата по иностранным делам (1917-1918 гг.) // Международная жизнь. – 2003. N 2. – С. 115-122.

197. Воронкин А.С. Социальные сети: эволюция, структура, анализ // Образовательные технологии и общество. № 1. 2014. – С. 650-675.

198. Гасанова М.М. Социальные сети в политике // Вестник Саратовского Государственного Социально-Экономического Университета. № 5 (59). 2015. – С. 215-218.

199. Голубев Д.С. Факторы вероятности трансграничного распространения внутригосударственных вооруженных конфликтов // Полис. Политические исследования. 2019. № 2. – С.41-58.

200. Егоров Е. Россия в зеркале упражнений НАТО над Украиной / Дипломатика, 2012. № 4. – С. 180-182.

201. Ефимов Е.Г., Кузнецов А.А. Виды кризисного потенциала социальных Интернет-сетей как региональных социально-экономических систем // Инновационный потенциал современного региона проблемы региональной безопасности и внутрирегиональной интеграции на постсоветском пространстве, всерос. научн.-практ.конф. – Волгоград: ФГОУ ВПО ВАГС, 2011. – С. 144-145.

202. Жукова О.С., Иванченко Р.Б., Трухачев В.В. Информационный экстремизм как угроза безопасности Российской Федерации // Вестник Воронежского института МВД России. № 1. 2007. – С. 53-55.

203. Зинченко Ю.П. Виртуализация реальности: от психологического инструментария к новой субкультуре // Человек как субъект и объект медиапсихологии : сб. науч. ст. – М.: МГУ, 2011. – С. 231-278.

204. Киняшева Ю.Б. Социальные сети как инструмент политической мобилизации граждан в современной России // Известия ТулГУ. Гуманитарные науки. №3. 2018. – С. 3-10.

205. Коробенков А. Цифровая система управления производством – важный шаг к "Индустрии 4.0" [Электронный ресурс] // Технологии в

электронной промышленности. № 7. 2016. – P.50-52. URL: https://controleng.ru/wp-content/uploads/11_91.pdf (дата обращения 12.04.2020).

206. Коротаев А.В., Шишкина А.Р., Балтач А.А. Относительная депривация как фактор социально-политической дестабилизации: опыт количественного анализа // Полис. Политические исследования. 2019. № 2. – С.107-122.

207. Коротаев А.В., Шишкина А.Р., Исаев Л.М. Арабская весна как триггер глобального фазового перехода? // Полис. Политические исследования. 2016. № 3. – С.108-122.

208. Коротаев А.В., Шишкина А.Р., Лухманова З.Т. Волна глобальной социально-политической дестабилизации 2011-2015 гг.: количественный анализ // Полис. Политические исследования. 2017. № 6. – С.150-168.

209. Кравченко С.А. Спираль усложнения насилия: востребованность гуманистической политики // Политические исследования, 2019. № 5. –С. 43-55.

210. Кравченко С.А., Подберезкин А.И. Диагностика доверия к безопасности России в условиях нового знания о рисках и уязвимостях // Гуманитарий Юга России, 2017. Т. 23. №1. – С. 27-41.

211. Крутских А. К политико-правовым основаниям глобальной информационной безопасности // Международные процессы, 2007. № 1 (5). – С.28-37.

212. Кузнецова Ю.М. Картина мира и современные технологии: «легкость бытия» в интернете // Человек как субъект и объект медиапсихологии : сб. науч. ст. – М.: МГУ, 2011. – С. 437-467.

213. Кулагин В. Глобальная или мировая безопасность // Международные процессы. 2007. Т. 5. № 2. – С. 38-51.

214. Кулагин В.М. Мир в XXI веке: многополюсный баланс сил или глобальный pax democratica? (Гипотеза «демократического мира» в контексте альтернатив мирового развития) // Полис, 2000. № 1. – С. 23-37.

215. Курочкин А. В. Трансформация государственного суверенитета в условиях становления сетевого общества // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – Тамбов: «Грамота», 2012. № 2 (26). Ч. III. – С. 95-99.

216. Ланцов С.А., Усмонов Ф.И. Проблемы безопасности в теории международных отношений: сравнительный анализ основных направлений [Электронный ресурс] // Журнал ПОЛИТЭКС, 2008. Т.4.№2.– С.151-163. URL: https://cyberleninka.ru/article/n/problemy-bezopasnosti-v-teorii-mezhdunarodnyh-otnosheniy-sravnitelnyy-analiz-osnovnyh-napravleniy/viewer (дата обращения 04.02.2020).

217. Лебедева М.М., Харкевич М.В., Зиновьева Е.С., Копосова Е.Н. Архаизация государства: роль современных информационных технологий // Полис. Политические исследования. 2016. № 6. – С.22-36.

218. Лемеш К.И. Об опасности «социально-сетевого» экстремизма Современные научные исследования и разработки. Т. 2. № 1(9). 2017. – С. 378-379.

219. Луман Н. Риск и опасность // Отечественные записки. № 2(53). 2013. – С. 19-51.

220. Манойло А.В. Современные политические конфликты: право на вмешательство // Полис. Политические исследования. 2017. № 6. – С.178-188.

221. Манойло А.В. Убить котенка, или технологии конфликтной мобилизации в социальных сетях // Мировая политика. № 3. 2015. – С. 1-12.

222. Мациевский Ю.В. В ловушке гибридности: политический режим в Украине после революции 2014 года // Полис. Политические исследования. 2018. № 1. – С.96-115.

223. Мирошниченко И.В., Морозова Е.В. Сетевая публичная политика: контуры предметного поля // Полис. Политические исследования. 2017. № 2. – С.82-102.

224. Могилевская Г.И. Информационная война в социальных сетях // Молодой ученый. №15. 2015. – С. 650-654.

225. Носетти Ж. Кремль «ВКонтакте»: власть и интернет в России [Электронный ресурс] // IFRI - Russie.Nei.Visions №59.2011. URL: http://www.pircenter.org/kosdata/page_doc/p2734_1.pdf (дата обращения 08.01.2020).

226. Ознобищев С.К. “Новая холодная война”: воспоминания о будущем // Полис. Политические исследования. 2016. № 1. – С.60-73.

227. Палитай И.С. Трансформация образов власти и политических лидеров Великобритании под влиянием Brexit (на материалах европейских и американских СМИ за 2014-2017 гг.) // Полис. Политические исследования. 2018. № 2. – С.150-162.

228. Петухов В.В., Петухов Р.В. Запрос на перемены: причины актуализации, ключевые слагаемые и потенциальные носители // Полис. Политические исследования. 2019. № 5. – С.119-133.

229. Подберезкин А.И. От «стратегии противоборства» к «стратегии управления» // Вестник МГИМО-Университета, 2017. – № 1(52). – С. 7-20.

230. Примаков Е.М. ООН: вызовы времени // Россия в глобальной политике. 2004. № 5. [Электронный ресурс] URL: https://globalaffairs.ru/articles/oon-vyzovy-vremeni/ (дата обращения 15.01.2020).

231. Радина Н.К. Цифровая политическая мобилизация онлайн-комментаторов материалов СМИ о политике и международных отношениях // Полис. Политические исследования. 2018. № 2. – С.115-129.

232. Радина Н.К., Крупная Д.А. Цифровое политическое участие: эффективность электронных петиций негосударственных онлайн-платформ (на материале change.org) // Полис. Политические исследования. 2019. № 6. – С.113-127.

233. Римский В. Л. Коммуникация в социальных сетях как рациональный ответ граждан на условия ограничения их гражданской и

политической активности // Социальные сети и виртуальные сообщества. – М.: ИНИОН РАН, 2013. – С. 132-146.

234. Росс А., Скотт Б. Социальные СМИ: причина, следствие и реагирование // Официальный сайт НАТО. 2011. [Электронный ресурс] URL: http://www.nato.int/docu/review/2011/Social_Medias/21st-century-statecraft/RU/index.htm (дата обращения 27.03.2020).

235. Русакова О., Грибовод Е. Информационно-коммуникативные компоненты «мягкой силы» // Международные процессы. 2019. Том 17. № 1 (56). – С.62-72.

236. Рябченко Н.А., Малышева О.П., Гнедаш А.А. Управление политическим контентом в социальных сетях в период предвыборной кампании в эпоху постправды // Полис. Политические исследования. 2019. № 2. – С.92-106.

237. Свищёва А.Н. Относительная депривация в условиях финансово-экономического кризиса // Мониторинг общественного мнения: экономические и социальные перемены. 2016. №5. – С. 183-202.

238. Симония Н.А., Торкунов А.В. Новый мировой порядок: от биполярности к многополюсности // Полис. Политические исследования. № 3. 2015. – С. 27-37.

239. Смирнов А. Новейшие киберстратегии США – преамбула войны? // Международные процессы. 2018. Том 16. № 4 (55). – С.181-192.

240. Соловей В.Д. Цифровая мифология и избирательная кампания Дональда Трампа // Полис. Политические исследования. 2017. № 5. – С.122-132.

241. Соловьев Э.Г. Террористические организации как субъект международных отношений в меняющемся мире // Актуальные проблемы американистики: Материалы десятого международного научного семинара "Россия, НАТО и США в антитеррористической коалиции". – Н.Новгород, 2004. – С.173.

242. Стадник И., Цветкова Н. Политика кибербезопасности США: эволюция восприятия угроз // Международные процессы. 2018. Том 16. № 3. – С.157-169.

243. Тихонова С.В. Социальные сети: проблемы социализации интернета // Полис. Политические исследования. 2016. № 3. – С.138-152.

244. Троицкий М.А. Концепция "программирующего лидерства" в евроатлантической стратегии США // Pro et Contra. № 4. 2002. – С.86-103.

245. Туре Х. Киберустойчивость: суть мира в киберпространстве // Индекс безопасности. №1 (104). Весна 2013. – С. 207-212.

246. Ушкин С.Г. Теоретико-методологические подходы к изучению сетевой протестной активности: от «умной толпы» к слактивизму // Мониторинг общественного мнения: экономические и социальные перемены. 2015. № 3. – С. 3-11.

247. Хрусталев М.А. Диверсионно-террористическая война как военно-политический феномен // Международные процессы. 2003. № 2. – С. 60-61.

248. Цыганков П.А. Эволюция классических парадигм в западной теории международных отношений // Общественные науки и современность, 2004. № 2. – С.119-130.

249. Чернобай А. Роль социальных сетей в мобилизации протестных настроений на Ближнем Востоке и в Северной Африке в январе-марте 2011 года // Идеологические аспекты военной безопасности. 2011. № 1. – С. 40-47.

250. Шарапов Р.И. Мобильный интернет как инструмент политической мобилизации // Известия Тульского государственного университета. Гуманитарные науки. 2017. № 1. – С. 20-27.

251. Шарапов Р.И. Условия политической мобилизации в сети Интернет // Социодинамика. 2017. № 10. – С. 1-8.

252. Шариков П. Информационный суверенитет и вмешательство во внутренние дела в российско-американских отношениях // Международные процессы. 2018. Том 16. № 3. – С.170-188.

253. Шарков Ф.И. Визуализация политического медиапространства // Полис. Политические исследования. 2016. № 5. – С.97-107.

254. Шерстобитов А. С., Брянов К. А. Технологии политической мобилизации в социальной сети «ВКонтакте»: Сетевой анализ протестного и провластного сегментов // Исторические, философские, политические и юридические науки, культурология и искусствоведение. Вопросы теории и практики. – Тамбов: «Грамота», 2013. № 10 (36), часть I. – С. 196-202.

255. Штомпка П. Культурная травма в посткоммунистическом обществе // Социологические исследования . 2001. № 2. – С. 3-12.

256. Штомпка П. Социальное изменение как травма // Социологические исследования. 2001. № 1. – С.6-16.

257. Шульц Э. Современные протестные акции в развитых странах как форма радикальной мобилизации // Международные процессы. 2018. Том 16. № 3. – С.100-112.

258. Ясперс К. Современная техника // Новая технократическая волна на Западе. – М.: Прогресс, 1986. – С. 119-121.

259. Arendt H. Lying in Politics: Reflections on the Pentagon Papers // Arendt H. Crises of the Republic. – New York: Harcourt Brace & Co., 1972. – P. 1-48.

260. Arquilla J., Ronfeldt D. Cyberwar is Coming! // Comparative Strategy, 1993, Vol. 12 (2). – P. 141-165.

261. Bimber B. The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism // Polity. 1998. Vol. XXXI. No 1. – P. 133-160.

262. Boyd D.M., Ellison N.B. Social network sites: definition, history,and scholarship // Journal of computer-mediated communication. 2008. – № 13. – P.210-230.

263. Castells M. The new public sphere: global civil society, communication networks and global governance // The Annals of the American Academy of Political and Social Science. 2008. –№ 616. – P. 78-93.

264. Cowan G., Arsenault A. Moving from monologue to dialogue to collaboration: The Three Layers of Public Diplomacy // Annals of the American Academy of Political and Social Science. 616. 2008. – P. 10-30.

265. Derrida J. History of the Lie: Prolegomena // Derrida J. Without Alibi. Edited, translated, and with an Introduction by Peggy Kamuf. – Stanford: Stanford University Press, 2002. – P. 28-70.

266. Fielding N., Cobain I. Revealed: US spy operation that social media // The Guardian. March 17, 2011. [Электронный ресурс] URL: https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks (дата обращения 06.09.2019).

267. Genest C., Zidek J. Combining probability distributions: a critique and an annotated bibliography // Statistical Science. – Vol. 1. №. 1, 1986. – P. 114-135.

268. Giddens, A. Modernity and Self-identity: Self and Society in the Late Modern Age. Cambridge: PolityPress, 1991.

269. Hall I., Smith F. The struggle for soft power in Asia: Public diplomacy and regional competition // Asian Security. Vol. 9(1). 2013. – P. 1-18.

270. Harmon C. Public diplomacy's next challenge // The Quarterly Journal, 2008. – P. 142-144.

271. Khaleghi B. Multisensor data fusion: A review of the state-of-the-art // Information Fusion.Vol.41. - No.1. 2013. – P. 28-44.

272. Ktepi B. Deception in political social media // ed. K. Harvey. Encyclopedia of social media and politic. 2014. Vol. 4. – Thousand Oaks, CA: SAGE Publications. – P. 357-359.

273. List C, Polak B. Introduction to Judgment Aggregation // Journal of Economic Theory. – Vol. 145. – №. 2. 2010. – P. 441-466.

274. Nye J. The Pros and Cons of Citizen Diplomacy // New York Times. 04.10. 2010. [Электронный ресурс] URL: https://www.nytimes.com/2010/10/05/opinion/05iht-ednye.html (дата обращения 03.12.2019).

275. Passy F., Monsch G.A. Do Social Networks Really Matter in Contentious Politics? // Social Movement Studies. 2014. Vol. 13 (1). – P. 22-47.

276. Post J. Cybernetic War // Omni, 1979. No.5. – P. 44-104.

277. Public Diplomacy: Strengthening U.S. Engagement with the World. A Strategic Approach for the 21st Century / Office of the Under Secretary of State for Public Diplomacy and Public Affairs 2/26/2010. – 33 p.

278. Ronfeldt D., Arquilla J. Noopolitik: A new paradigm for public diplomacy // Routledge Handbook of Public Diplomacy. / Nancy Snow, Philip M. Taylor. – NY: Rougledge, 2009. – P. 352-362.

279. Rowland J., Rice M., Shenoi S. Whither Cyberpower? // International Journal of Critical Infrastructure Protection. Vol. 7 (2). 2014. – P. 124-137.

280. Satopaa V., Baron J., Foster D., Mellers B., Tetlock P., Ungar L. Combining multiple probability predictions using a simple logit model // International Journal of Forecasting. – Vol. 30. – №. 2. 2014 – P. 344-356.

281. Shane S. Former F.B.I. Agent Sues, Claims Retaliation Over Misgivings in Anthrax Case // New York Times, April 9. 2015. [Электронный ресурс] URL: https://www.nytimes.com/2015/04/09/us/ex-fbi-agent-claims-retaliation-for-dissent-in-anthrax-inquiry.html (дата обращения 12.05.2018).

282. Shannon C. A Mathematical Theory of Communications // Bell Systems Technical Journal. – Vol. 27.1948. – P. 623-656.

283. Sheldon J. Deciphering Cyberpower // Strategic Studies Quarterly. 2011. – P.95-112.

284. Takahashi T. MySpace or Mixi? Japanese engagement with SNS (social networking sites) in the global age // New media & society. – XX(X). 2010. – P. 1-23.

285. Urry J. Mobilities. Cambridge: Polity Press, 2008.

Интернет ресурсы

286. Абдуллин Р. Арабская революция 2.0. Интернет как фактор изменений на Ближнем Востоке [Электронный ресурс] // Центр Азия -

4.05.2011. URL: https://centrasia.org/newsA.php?st=1304453040 (дата обращения: 16.02.2020).

287. Американцы введут «информационные войска» в российские социальные сети [Электронный ресурс] // Свободная пресса - 14.04.2015. URL: http://svpressa.ru/politic/news/118677/ (дата обращения: 14.09.2019).

288. Ашманов И. Под властью ментального вируса, или как отличить вброс от новости [Электронный ресурс] // Сайт журнала «Фома» - 01.10.2012. URL: https://foma.ru/pod-vlastyu-mentalnogo-virusa-ili-kak-otlichit-vbros-ot-novosti.html (дата обращения: 15.09.2019).

289. Ашрафов Р. Сетевые миротворцы [Электронный ресурс] // Портал «Кремль. org» - 13.08.2008. URL: http://kreml.org/opinions/189135205 (дата обращения: 19.11.2018).

290. Белоусов В.В. Социальные Интернет-сети как политическое оружие и инструмент конкурентной борьбы [Электронный ресурс] // Капитал страны - 18.04.2011. URL: http://www.kapital-rus.ru/articles/article/183584/ (дата обращения: 22.02.2019).

291. Вся статистика интернета на 2019 год – в мире и в России // WebCanape. 2019. 11 февраля. [Электронный ресурс] URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/ (дата обращения 26.02.2019).

292. Выходы политиков в сеть: и Ельцин был не первым [Электронный ресурс] URL: http://www.temadnya.ru/spravka/07mar2001/306.html (дата обращения 25.01.2018).

293. Габуев А., Черненко Е. Пользователи протеста: Возможны ли сегодня революции без Twitter и Facebook [Электронный ресурс] // Газета Коммерсант - 09.03.2011. URL: https://www.kommersant.ru/doc/1597287 (дата обращения: 01.04.2020).

294. Гунеев С. МИД России "лайкнул" твит Трампа об ухудшении отношений Москвы и Вашингтона [Электронный ресурс] // информационное

агентство Sputnik - 16.07.2018. URL: https://ru.sputnik.md/world/20180716/20583797/trump-twiter-declaration-mfa-replika.html (дата обращения: 16.07.2018).

295. Зиновьева Е.С. «Цифровой Вестфаль»? [Электронный ресурс] // официальный сайт МГИМО(У) МИД России, 26 марта 2013. URL: https://mgimo.ru/about/news/experts/236588/ (дата обращения 03.04.2018).

296. Лихтман Б. Китай готовится к кибервойне [Электронный ресурс // Infox: Новые новости. 23.10.2009. URL: http://www.infox.ru/hi-tech/internet/2009/10/23/Kitay_gotovitsya_k_k.phtml. (дата обращения 29.08.2019).

297. Макконелл Б. Сетевое сообщество и роль государства [Электронный ресурс] // Россия в глобальной политике - 07.05.2016. URL: http://globalaffairs.ru/number/Setevoe-obschestvo-i-rol-gosudarstva-18027 (дата обращения: 17.03.2020).

298. Маковейчук А.В. Социальные сети как новый механизм продвижения интересов субъектов политической деятельности в молодёжной среде [Электронный ресурс] // Connect universum - 15.05.2012. URL: http://connect-universum.tsu.ru/blog/connectuniversum2012_ru/41.html (дата обращения: 30.05.2019).

299. Массен Э. Соцсети – оружие массового поражения в информационной войне [Электронный ресурс] // Сайт "Антисоцсеть". URL: https://antisoc.ru/mneniya-uchenyih/kak-ispolzuyutsya-sotsialnyie-seti-v-informatsionnoy-voyne/ (дата обращения: 12.03.2020).

300. Медведев Д. А. Пользователи интернета могут изменить мир [Электронный ресурс] // Актуальные комментарии - 08.09.2011. URL: http://actualcomment.ru/medvedev_polzovateli_interneta_mogut_izmenit_mir.html (дата обращения: 19.12.2019).

301. ОДКБ будет активно бороться с киберпреступностью [Электронный ресурс] // Сайт Организации Договора о коллективной

безопасности. 21.12.2011. URL: http://www.odkb-csto.org/news/detail.php?ELEMENT_ID=558 (дата обращения 29.08.2019).

302. Россия внесла в ГА ООН проект резолюции по информационной безопасности [Электронный ресурс] // Известия - 17.10.2018. URL: https://iz.ru/801609/2018-10-17/rossiia-vnesla-v-ga-oon-proekt-rezoliutcii-po-informatcionnoi-bezopasnosti (дата обращения: 05.11.2019).

303. Социальные сети в России. Осень 2018 [Электронный ресурс] // Brand Analytics. URL: https://br-analytics.ru/blog/wp-content/uploads/2018/12/Sotsseti-Rossiya-osen-2018.pdf (дата обращения: 05.04.2019).

304. Суманеев И. Reddit, Трамп и «Политач». Как социальные сети влияют на политику [Электронный ресурс] // НОЖ [сайт] – 26.12.2018. URL: https://knife.media/social-media-politics/ (дата обращения 11.11.2019).

305. Твиттер страница А.А. Навального [Электронный ресурс]. URL: https://twitter.com/navalny (дата обращения: 03.05.2020).

306. Твиттер страница В.В. Мальцева [Электронный ресурс]. URL: https://twitter.com/vvmaltsev (дата обращения: 05.04.2020).

307. Твиттер страница Д.А. Медведева [Электронный ресурс]. URL: https://twitter.com/medvedevrussia (дата обращения: 03.05.2020).

308. Твиттер страница Дональда Трампа [Электронный ресурс]. URL: https://twitter.com/realdonaldtrump (дата обращения: 03.05.2020).

309. Твиттер страница Министерства иностранных дел России [Электронный ресурс]. URL: https://twitter.com/mid_rf (дата обращения: 03.05.2020).

310. Шитов А. "Объявление войны через Twitter?" Блогосфера в США обсуждает тезисы Трампа [Электронный ресурс] // информационное агентство ТАСС - 11.04.2018. URL: http://tass.ru/mezhdunarodnaya-panorama/5116004 (дата обращения: 17.12.2019).

311. Colding-Jørgensen A. Stork Fountain Experiment #1: Why Facebook groups are not democratic tools [Электронный ресурс] // URL:

http://virkeligheden.dk/2009/stork-fountain-experiment-1-facebook-groups-are-not-democratic-tools/ (дата обращения 12.11.2019).

312. Greenberg A. The Wired Guide to Cyberwar [Электронный ресурс] // Wired. 2019. 23d August. URL: https://www.wired.com/story/cyberwar-guide/ (дата обращения 31.08.2019).

313. Hesse M. Facebook Activism: Lots of Clicks, but Little Sticks [Электронный ресурс] // The Washington Post. 2009. 2nd July. URL: https://www.washingtonpost.com/wp-dyn/content/article/2009/07/01/AR2009070103936_2.html (дата обращения 17.10.2019).

314. Kreisler H. Identity and Change in the Network Society. Conversation with Manuel Castells [Электронный ресурс] // Conversations with History, Institute of International Studies, UC Berkeley, 08.05.2001. URL: http://globetrotter.berkeley.edu/people/Castells/castells-con4.html (дата обращения 15.05.2019).

315. Leng S., Wertime D. Hong Kong's Protest, in Memes [Электронный ресурс] // Foreign Policy. 2014. 29th September. URL: http://foreignpolicy.com/2014/09/29/hong-kongs-protest-in-memes/ (дата обращения 10.10.2019).

316. Lüfkens M. Twiplomacy Study 2018 [Электронный ресурс] // twiplomacy.com [сайт], 10.10. 2018. URL: https://twiplomacy.com/blog/twiplomacy-study-2018/?source=post_page (дата обращения: 12.06.2019).

317. Messmer E. Cyber Espionage: A Growing Threat to Business [Электронный ресурс] // PCWorld [сайт] – 21.01.2008. URL: https://www.pcworld.com/article/141474/article.html (дата обращения: 01.02.2019).

318. Monitoring The WSIS targets. A mid-term review [Электронный ресурс] // World Telecommunication / ICT Development Report 2010. URL:

https://www.itu.int/dms_pub/itu-d/opb/ind/D-IND-WTDR-2010-PDF-E.pdf (дата обращения: 11.09.2019).

319. Nasser H. Civil Society 2.0 [Электронный ресурс] //Open Democracy - 19.10.2016. URL: https://www.opendemocracy.net/north-africa-west-asia/heba-al-nasser/civil-society-20 (дата обращения: 28.03.2020).

320. Pincus W. Pentagon Reviewing Strategic Information Operations [Электронный ресурс] // The Washington Post. 2009. 27th December. URL: https://www.washingtonpost.com/wp-dyn/content/article/2009/12/26/AR2009122601462.html (дата обращения 29.08.2019).

321. Pirillo C. Five Ways the Government Spies on You [Электронный ресурс] // The lockergnome daily report [сайт] – 07.11.2011. URL: https://lockergnome.com/2011/11/07/five-ways-the-government-spies-on-you/ (дата обращения: 09.08.2019).

322. Press G. A Very Short History of Big Data [Электронный ресурс] // Forbes.com. [сайт], 09.05.2013. URL: https://www.forbes.com/sites/gilpress/2013/05/09/a-very-short-history-of-big-data/#92208b965a18 (дата обращения: 21.05.2019).

323. Shafer G., Dempster A.P. Dempster-Shafer Theory [Электронный ресурс]. URL: http://www.glennshafer.com/assets/downloads/articles/article48.pdf (дата обращения: 17.10.2019).

324. Shaw A. Role of Social Media in Social Mobilization (with Special Reference to Shahbag and Hokkolorob Movements) [Электронный ресурс] // Global Media Journal – Indian Edition. 2016. Vol. 7 (1). URL: https://www.caluniv.ac.in/global-mdia-journal/COMMENT-2016-NOV/C-5-F.pdf (дата обращения 13.01.2019).

325. Stuxnet: война 2.0 [Электронный ресурс] // Хабр [сайт], 12 октября 2010. URL: https://habr.com/ru/post/105964/ (дата обращения 18.08.2019).

326. The future of the internet. A virtual counter-revolution [Электронный ресурс] // The Economist, 02.09.2010. URL: http://www.economist.com/node/16941635 (дата обращения: 04.09.2019)

327. The world in 2010 [Электронный ресурс] // ICT Facts and Figures. 2010. International Telecommunication Union. URL: http://www.itu.int/ITU-D/ict/material/FactsFigures2010.pdf (дата обращения: 07.09.2019).