

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКАЯ АКАДЕМИЯ НАРОДНОГО ХОЗЯЙСТВА И
ГОСУДАРСТВЕННОЙ СЛУЖБЫ ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ
ФЕДЕРАЦИИ»

СРЕДНЕРУССКИЙ ИНСТИТУТ УПРАВЛЕНИЯ – ФИЛИАЛ

На правах рукописи

ЦАРИК Владимир Станиславович

**Формирование системы противодействия «российской информационной
угрозе» на Западе (2014-2019 гг.):
концептуальный и институциональный аспекты**

ДИССЕРТАЦИЯ

на соискание ученой степени кандидата политических наук

5.5.4 – Международные отношения, глобальные и региональные
исследования

Научный руководитель:

кандидат политических наук, доцент

Малахова Оксана Владимировна

Орел – 2023

Содержание

Введение	3
Глава 1. Конструирование «российской информационной угрозы» в западной политологической мысли	38
1.1. Формирование представления о «российской информационной угрозе» в западном политическом пространстве в 2007-2013 гг.	38
1.2. Дискурс о «гибридной войне» как концептуальная основа противодействия «российской информационной угрозе»	49
1.3. Развитие представления о «российской информационной угрозе» в рамках теории «гибридной войны»	79
Выводы по главе 1	100
Глава 2. Становление институциональной инфраструктуры западной системы противодействия «российской информационной угрозе» после украинского кризиса (2014-2016 гг.)	106
2.1. Формирование политико-институциональных рамок информационного противодействия России западными межгосударственными объединениями	107
2.2. Особенности реагирования на «российскую информационную угрозу» органами власти государств Запада	149
Выводы по главе 2	177
Глава 3. Развитие институционального измерения западной системы противодействия «российской информационной угрозе» после президентских выборов в США (2017-2019 гг.)	183
3.1. Развитие механизмов противодействия «российской информационной угрозе» в США после избрания Д. Трампа	184
3.2. Выстраивание и укрепление институциональной инфраструктуры противодействия «российской информационной угрозе» в европейских государствах	219
3.3. Эволюция институциональных механизмов информационного противодействия России на уровне западных межгосударственных объединений	242
Выводы по главе 3	269
Заключение	274
Список литературы	287

Введение

Актуальность исследования. В 2014-2021 гг. в западном публичном пространстве регулярно звучали обвинения России в применении деструктивных методов информационного влияния, которым приписывали экстраординарную, практически экзистенциальную, угрозу национальной безопасности и общественной стабильности государств Запада. Эти обвинения получили не только значительный медийный резонанс, но и экспертно-академическое обоснование, а, с течением времени, и политическое оформление, превратившись в одну из не подлежащих сомнению констант западного дискурса и немаловажную составляющую общего конфронтационного курса в отношении нашей страны, развёрнутого Западом после кризиса 2014 г. На базе данных обвинений была выстроена целая система противодействия «российской информационной угрозе», состоящая из формальных и полужформальных государственных и международных механизмов, а также целой сети внегосударственных структур и инструментов, чьей функцией являлось выявление и нейтрализация якобы распространяемых российским руководством дезинформации, пропаганды и «фейковых новостей».

Это была не классическая информационная война, понимаемая как действия по нанесению ущерба противнику с помощью информационных средств воздействия, например, дезинформации госаппарата или деморализации населения. Это явление иного порядка, связанное не столько с воздействием собственно на политическую систему и общество Российской Федерации, сколько с закреплением определённых идеологем и установок в отношении нашей страны в западном политическом пространстве. Фактически, конструирование образа России как абсолютного деструктора, ведущего «гибридную агрессию» против либерального миропорядка, и создание специальных органов, призванных её отражать, в корне изменили порядок формирования политики Запада, его институтов и государств в отношении России, сложившийся в постбиполярный период и представлявший собой, пусть

и не очень устойчивый, баланс между ограниченно кооперативными подходами традиционных российских партнёров в Европе и конфронтационным дискурсом, продвигаемым Великобританией и рядом новых членов НАТО и ЕС из числа государств Центрально-Восточной Европы. По мере оформления системы противодействия «российской информационной угрозе» антироссийский конфронтационный дискурс приобрёл качество магистрального вектора политического курса Запада в отношении России. Благодаря этому, на момент начала специальной военной операции (СВО) на Украине и перехода геополитической конфронтации с РФ в «горячую» фазу, Запад уже выстроил полноценный механизм подавления любых положительных в отношении России позиций, позволивший в относительно сжатые сроки добиться разрыва кооперативных связей с Россией в экономической, научной и культурной плоскостях, несмотря на объективные потери от такого разрыва для собственной экономики и безопасности.

Для российской дипломатии и политической науки формирование подобной системы информационного противодействия стало неожиданным и довольно серьёзным вызовом, который нельзя недооценивать, игнорировать или списывать сугубо на внутривнутриполитическую конъюнктуру некоторых западных стран. Однако приходится констатировать, что к настоящему моменту этот вызов так и не получил должного академического осмысления и политического ответа, соответствующего его значимости для реализации национальных интересов России и её внешнеполитического курса. Это обуславливает необходимость комплексного изучения процесса инициирования, формирования и эволюции системы противодействия «российской информационной угрозе» на Западе во всех её аспектах и проявлениях, в систематизации имеющихся фактических данных для понимания механизмов функционирования данной системы и её деструктивных эффектов для статуса и авторитета России на международной арене. Это позволит, в том числе, сформировать адекватную оценку текущего положения дел во взаимодействии с коллективным Западом с учётом целей и задач СВО и возможностей договорных путей достижения этих целей.

Под «российской информационной угрозой» в данной работе подразумевается не конкретный термин из западной политической риторики, а совокупность действий в информационной сфере, в которых обвиняли Россию, её политическое руководство и граждан в западном медиапространстве после 2014 г. и которые расценивались как угроза политической стабильности и либерально-демократическому порядку. В неё входят так называемая «российская пропаганда», деструктивная работа «русских хакеров», ботов и троллей, «российское вмешательство» во внутренние политические процессы в западных странах и ведущаяся Россией «кибервойна со свободным миром».

Масштабность исследуемого феномена обусловила необходимость сфокусироваться на наиболее важных, на наш взгляд, его компонентах, а именно концептуальном и институциональном аспектах западной системы противодействия «российской информационной угрозе» на её государственном и межгосударственном уровнях. В то же время практический аспект её функционирования и задействованные в ней внегосударственные механизмы остались за рамками данной работы и могут стать предметом дальнейших исследований этой крайне актуальной и интересной проблематики.

Степень научной разработанности темы. Несмотря на многочисленные публикации по темам, затрагиваемым в данной работе («гибридная война», политическое использование информационных технологий, возвращение к открытой политике «сдерживания» России и др.), сама по себе проблема становления на Западе системы противодействия «российской информационной угрозе» практически не изучалась в том ключе, в котором она сформулирована в данном исследовании, причём как в западной академической науке, так и в российской. В большинстве академических источников «гибридная война» и обусловленные ею формы информационного противоборства рассматриваются как самостоятельные, объективно существующие, онтологически независимые элементы политической реальности, сущностные и содержательные аспекты которых нуждаются в отдельном изучении. В них не допускается возможность использования данного концепта в политическом и академическом дискурсе не

для отображения или описания, а для создания соответствующей политической реальности, задания необходимых концептуальных рамок, в которых практические факты, события и процессы будут неизбежно работать на поддержание концепта и его объективацию вне зависимости от воли акторов.

В настоящем исследовании изучаются этапы, уровни и субъекты процесса конструирования «российской информационной угрозы» в западном публичном пространстве, исходя из понимания того, что данный процесс имел целенаправленный, проектный характер и продвигался как на официальном, так и в экспертно-академическом дискурсивном поле. По этой причине, опираясь на широкий массив разнообразных источников, диссертант не столько использует содержательную часть их утверждений для развития на их основе собственных научных выводов, уточняющих или опровергающих предложенное ими описание, сколько рассматривает их как материал для отслеживания развития определённого дискурса, который стал частью проекта формирования «российской информационной угрозы».

Указанные источники можно ранжировать по нескольким признакам. Главный – характер публикации: академические работы, экспертные и аналитические материалы различных негосударственных организаций (НГО), публикации в СМИ и на различных Интернет-ресурсах. Особое место занимают специфические «псевдоэкспертные» источники – оформленные в академическом стиле статьи и доклады не в регулярных, периодических рецензируемых научных журналах, а в специальных тематических сборниках и выпусках, издаваемых под эгидой и при финансовой поддержке структур НАТО и ЕС, политизированными неправительственными организациями, партийными структурами западных стран. Возможность западного истеблишмента мобилизовать ресурсы для быстрого создания большого массива текстов с однотипными выводами, вводимых в экспертное пространство под видом научных (хотя они не проходят стандартного процесса анонимного рецензирования), а затем их тиражирования и популяризации в СМИ, обязательного регулярного воспроизводства в политическом дискурсе, создаёт

предпосылки для более лёгкого управления долгосрочным политическим курсом соответствующих стран и закрепления его желательных элементов через сконструированный в обществе и политическом классе консенсус.

Другой признак – авторство материалов (западное и украинское, российское). Возможно также ранжирование работ в зависимости от занимаемой автором позиции в пропаганде симпатий либо антипатий к России, предлагаемых им мер разрешения противоречий. При этом в некоторых случаях работы, написанные в нейтральном или пророссийском ключе, также играли немалую роль в конструировании «российской информационной угрозы», если они исходили из объективного характера «гибридной войны» и поддерживали нарратив о том, что Россия на самом деле ведёт подобного рода «войну» в отношении Запада.

Ключевую роль в становлении дискурса о «российской информационной угрозе» сыграла серия широко растиражированных публикаций от имени экспертов различных НГО, где вбрасывались основные месседжи с отточенными запоминающимися формулировками и с нужной идеологической подпиткой. На первом этапе основной поток публикаций был посвящён тематике «гибридной войны», имеющей информационную составляющую среди прочих, но постепенно акцент переводился на собственно «информационную угрозу» со стороны России, которая, однако, по-прежнему рассматривалась как составляющая «гибридной агрессии», что позволяло обострить восприятие «угрозы».

Тезис о «войнах нового поколения», будто бы инициированных Москвой, был подробно раскрыт в апреле 2014 г. в работе Я. Берзиньша¹; расстановка нужных акцентов была проведена в статье П. Померанцева² и «аналитическом» докладе А. Илларионова на заседании Парламентской ассамблеи НАТО в

¹ Bērziņš J. Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy / Bērziņš J. // National Defence Academy of Latvia Center for Security and Strategic Research Policy Paper. April 2014, no 02. 13 p. URL: <https://www.sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf> (дата обращения: 11.11.2020)

² Pomerantsev P. How Putin Is Reinventing Warfare / P. Pomerantsev // Foreign Policy. 2014, May 5. URL: <https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/> (дата обращения: 11.11.2020).

Вильнюсе³. После отождествления этого явления с понятием «гибридные войны», возникшим в недрах американской стратегической мысли⁴, концепцию «российской гибридной войны» как целостного многоаспектного действия (с упором на «некинетическую» составляющую) развивал М. Галеотти⁵.

Одновременно с разработкой концепта «российской гибридной агрессии» и в тесном взаимодействии с ним развивалось и представление об информационной составляющей этой «агрессии», якобы представляющей не меньшую угрозу, чем любые другие враждебные действия. Первыми акцентировали внимание на «информационной угрозе» России как составляющей «гибридной войны» И. Даржевская в мае 2014 г.⁶, П. Померанцев и М. Вайс в сентябре 2014 г. и позднее⁷. Установочными либо часто

³ Illarionov A. Speech by Mr. Andrei Illarionov at NATO Parliamentary Assembly. Committee on Economics and Security. 31 May 2014 / A. Illarionov // Livejournal.com. 11 июня 2014. URL: <https://aillarionov.livejournal.com/696630.html> (дата обращения: 11.11.2020)

⁴ См., в частности: Mattis J. Future Warfare: The Rise of Hybrid Wars / J. N. Mattis, F. Hoffman // U.S. Naval Institute, Proceedings Magazine, November 2005, Vol. 132, No. 11. P. 30-32; Hoffman F. G. Conflict in the 21-st Century. The Rise of Hybrid Wars / F. G. Hoffman. Arlington: Potomac Institute for policy studies, 2007. 72 p.; Hoffman F. G. Further Thoughts on Hybrid Threats / F. G. Hoffman // Small Wars Journal. 2009. March 02. URL: <http://smallwarsjournal.com/jml/art/further-thoughts-on-hybrid-threats> (дата обращения: 11.11.2020); Hoffman F. G. Hybrid Warfare and Challenges / F. G. Hoffman // Joint Forces Quarterly. 2009. Issue 52. p. 34-39. URL: <http://smallwarsjournal.com/documents/jfghoffman.pdf> (дата обращения: 11.11.2020); Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present / W. Murray, P.M. Mansoor (eds.). Cambridge: Cambridge University Press, 2012. 321 p.; Gates R. A Balanced Strategy: Reprogramming the Pentagon for a New Age / R. A. Gates // Foreign Affairs. 2009. Vol. 8, Issue 1. p. 28-40. URL: <https://www.comw.org/qdr/fulltext/0901gates.pdf> (дата обращения: 11.11.2020); Glenn R. W. Thoughts on “Hybrid” Conflict / R. W. Glenn // Small Wars Journal. 2009. URL: <http://smallwarsjournal.com/mag/docs-temp/188-glenn.pdf> (дата обращения: 11.11.2020); Glenn R. W. All Glory Is Fleeting. Insights from the Second Lebanon War / R. W. Glenn. Santa Monica, Ca Rand: National Defense Research Institute, 2012. 97 p. URL: <https://www.rand.org/pubs/monographs/MG708-1.html> (дата обращения: 11.11.2020); Sadowski D. Beyond the “Hybrid” Threat: Asserting the Essential Unity of Warfare / D. Sadowski, J. Becker // Small Wars Journal. 2010. January 7. URL: <http://smallwarsjournal.com/blog/journal/docs-temp/344-sadowski-et-al.pdf> (дата обращения: 11.11.2020); De Wijk R. Hybrid Conflict and the Changing Nature of Actors / R. De Wijk // The Oxford Handbook of War / Y. Boyer, J. Lindley-French (eds.). Oxford: Oxford University Press, 2012. P. 359-373.

⁵ Galeotti M. ‘The ‘Gerasimov doctrine’ and Russian Non-Linear War’ / M. Galeotti // In Moscow’s shadows. 2014. 6 July. URL: <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/> (дата обращения: 11.11.2020); Galeotti M. I’m Sorry for Creating the ‘Gerasimov Doctrine’ / M Galeotti // Foreign Policy. 2018. 5 March. URL: <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/> (дата обращения: 11.11.2020); Galeotti M. Controlling Chaos: How Russia Manages Its Political War in Europe / M. Galeotti // European Council on Foreign Relations Brief. August 2017. URL: https://ecfr.eu/wp-content/uploads/ECFR228_-_CONTROLLING_CHAOS1.pdf (дата обращения: 11.11.2020); Galeotti M. Hybrid war or gibridnaya voyna? Getting Russia’s non-linear military challenge right / M. Galeotti. Mayak Intelligence, 2016. 100 p.; Galeotti M. The mythical ‘Gerasimov Doctrine’ and the language of threat / M. Galeotti // Critical Studies on Security. 2018. Vol. 7, Issue 2. P. 157-161.

⁶ Darczewska J. The Anatomy of Russian Information Warfare. the Crimean Operation, a Case Study / J. Darczewska // OSW Point of View Number 42. May 2014. URL: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf (дата обращения: 11.11.2020)

⁷ Pomerantsev P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. / P. Pomerantsev, M. Weiss // A Special Report presented by The Interpreter, a project of the Institute of Modern Russia. URL:

встречающимися в тематике информационных войн авторами стали М. Л. Яйтнер и П. Маттсон, К. Жиль, Дж. Шерр, Н. Попеску, А. Полякова⁸. Кроме того, большую роль сыграли несколько тематических сборников, подготовленных специально созданными авторскими коллективами при НАТО либо в ассоциированных с ним структурах и неправительственных «мозговых центрах», специальные расследования, заказанные американским сенатом⁹. В

https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev_The_Menace_of_Unreality.pdf (дата обращения: 11.11.2020); Lucas E. Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe / E. Lucas, P. Pomerantsev // A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute. August 2016. 70 p. URL: <https://li.com/wp-content/uploads/2016/08/winning-the-information-war-full-report-pdf.pdf> (дата обращения: 11.11.2020); Weiss M. The Baltic elves taking on pro-Russian trolls / M. Weiss // The Daily Beast. 2016. 21 March. URL: <https://www.thedailybeast.com/the-baltic-elves-taking-on-pro-russian-trolls> (дата обращения: 11.11.2020).

⁸ Jaitner M. Applying Principles of Reflexive Control in Information and Cyber / M. L. Jaitner, MAJ. H. Kantola // Journal of Information Warfare. 2016. Vol 15, No. 4. P. 27-38; Jaitner M. L. Russian Information Warfare: Lessons from Ukraine / M. L. Jaitner // Russian Aggression against Ukraine / K. Geers (ed.). Tallinn: NATO CCD COE Publications, 2015. P. 87-94. URL: https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf (дата обращения: 11.11.2020); Jaitner M. Russian Information Warfare of 2014. / M. Jaitner // 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace / M. Maybaum, A.-M. Osula, L. Lindström (Eds.). Tallinn: NATO CCD COE Publications, 2015. P. 39-52; Giles K. Countering Russian Information Operations in the Age of Social Media / K. Giles // Council on Foreign Relations. November 21, 2017. URL: <https://www.cfr.org/report/countering-russian-information-operations-age-social-media> (дата обращения: 11.11.2020); Giles K. "Information Troops" – a Russian Cyber Command? / K. Giles // 2011 3rd International Conference on Cyber Conflict. C. Czosseck, E. Tyugu, T. Wingfield (Eds.). Tallinn, Estonia, 2011, P. 45-60; Giles K. Countering Russian Information Operations in the Age of Social Media / K. Giles // Council on Foreign Relations. November 21, 2017, 28.07.2018. URL: <https://www.cfr.org/report/countering-russian-information-operations-age-social-media> (дата обращения: 11.11.2020); Giles K. The Next Phase of Russian Information Warfare / K. Giles // Tallinn: NATO Strategic Communications Centre of Excellence. 2015. 16 p. URL: <https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles> (дата обращения: 11.11.2020); Sherr J. Russia: managing contradictions / J. Sherr // America and a Changed World: A Question of Leadership / R. Niblett (ed.). London: Chatham House/Wiley Blackwell, 2010. P. 162-184. URL: https://www.chathamhouse.org/sites/default/files/public/Research/Americas/us0510_sherr.pdf (дата обращения: 11.11.2020); Popescu N. Russia's Soft Power Ambitions / N. Popescu // Centre for European Policy Studies. Policy Brief. 2006 October, No. 115. 4 p. URL: <http://aei.pitt.edu/11715/> (дата обращения: 11.11.2020); Fried D. Democratic Defense Against Disinformation / D. Fried, A. Polyakova // Atlantic Council – Eurasia Center. February 2018. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/> (дата обращения: 11.11.2020); Polyakova A. The Future of Political Warfare: Russia, the West, and the Coming Age of Global Digital Competition / A. Polyakova, S. Boyer // Brookings – Robert Bosch Foundation Transatlantic Initiative. arch 2018. 24 p. URL: <https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/> (дата обращения: 11.11.2020); Polyakova A. The Kremlin Trojan Horses. Russian Influence in Greece, Italy, and Spain / A. Polyakova, M. Kounalakis, A. Klapsis et al. // Atlantic Council – Eurasia Center. November 2017. 36 p. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlin-s-trojan-horses-2-0/> (дата обращения: 11.11.2020)

⁹ NATO's Response to Hybrid Treats. / G. Lasconjarias and J. A. Larsen (eds.). Rome: NATO Defense college, 2015. URL: https://www.files.ethz.ch/isn/195405/fp_24.pdf (дата обращения: 11.11.2020); Hacks, leaks and disruptions – Russian cyber strategies / N. Popescu, S. Secriery (Eds.) // EU ISS Chaillot papers. 2018. No. 148. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (дата обращения: 11.11.2020); A Civil-Military Response to Hybrid Threats / E. Cusumano, M. Corbe (eds.). Palgrave Macmillan, Springer, 2018. 320 p.; Information Sharing in Military Operations / I. Goldenberg, J. Soeters, W. H. Dean (eds.). Springer, 2017. 274 p.; Information warfare. The pattern of aggression / I. Chifu, O. Nantoi (eds.). Bucharest: The Publishing House of the Institute of Political Sciences and International Relations "Ion I. C. Brătianu" of the Romanian Academy, 2016. 554 p.; DiResta R. The Tactics & Tropes of the Internet Research Agency. Report on the Internet Research Agency commissioned by the U.S. Senate Intelligence Committee / R. DiResta, K. Shaffer, D. Ruppel et al. New Knowledge, 2018. URL: <https://www.yonder-ai.com/resources/the-disinformation-report/> (дата обращения: 11.11.2020)

этих разноплановых сборниках обычно освещались сразу многие аспекты рассматриваемой проблемы, что позволяло черпать из них идеи для специализированных публикаций по тем или иным *аспектам*.

Многие академические работы по данной тематике, которые стали издаваться позже (примерно с середины 2015 г.), опирались на тезисы упомянутых установочных текстов и развивали их; масштабность подобной публикационной активности обеспечивалась, в том числе, авторами-военнослужащими США и союзников по НАТО, стран-претендентов на членство в страны НАТО; те же идеи повторялись в магистерских дипломных работах западных военных и гражданских ВУЗов¹⁰. Не имея познавательной ценности, не сообщая никакого нового научного результата, этот поток текстов, тем не менее, создавал общее впечатление о «российской гибридной войне» и «российской информационной агрессии» как о самоочевидной истине, неопровержимом явлении. В этом же русле написаны работы украинских авторов, наиболее показательной из которых является статья Е. Магды¹¹. В концептуальном плане они следуют общей западной тенденции, но антироссийский настрой выражают в более концентрированной форме.

В то же время, наряду с текстами, повторяющими и перефразирующими установочные материалы с раздуванием «российской угрозы», некоторые академические работы могли включать содержательный разбор того или иного

¹⁰ Raugh D. L. "Is the Hybrid Threat a True Threat?" / D. L. Raugh // Journal of Strategic Security. 2016. Vol. 9, No. 2. P. 1-13. URL: <https://scholarcommons.usf.edu/jss/vol9/iss2/2/> (дата обращения: 11.11.2020); Shakarian P. The 2008 Russian Cyber Campaign against Georgia / P. Shakarian // Military Review. November-December 2011, P. 62-68; Thiele R. D. The New Colour of War – Hybrid Warfare and Partnerships / R. D. Thiele // ISPSW Strategy Series: Focus on Defense and International Security. Oct 2015. Issue No. 383; Banasik M. Russia's Hybrid War / M. Banasik // Science & Military. 2016. No. 2. P. 39-47; M. Banasik. A Changing Security Paradigm. New Roles for New Actors – The Russian Approach / M. Banasik // Connections. 2016. Vol. 15, No. 4, 2016, P. 31-43; M. Banasik. Russia's Hybrid War in Theory and Practice / M. Banasik // Journal on Baltic Security. 2016. Vol. 2, Issue 1. P. 157-182; Veljovski G. The danger of "hybrid warfare" from a sophisticated adversary: the Russian "hybridity" in the Ukrainian conflict / G. Veljovski, N. Taneski, M. Dojchinovski // Defense & Security Analysis. 2017. Vol. 33, Issue 4. P. 292-307.; Wiśniewski J. Ukrainian Crisis – Example of a Hybrid War (General Lessons) / J. Wiśniewski // Zeszyty Naukowe AON. 2015. No. 4 (101). P. 175-187; Jones K. M. Cyber war: the next frontier for NATO. Master's Thesis / K. M. Jones // Monterey, California: Naval Postgraduate School, March 2015. URL: <https://calhoun.nps.edu/handle/10945/45201> (дата обращения: 11.11.2020); Danyk Y. Hybrid War High-tech, Information and Cyber Conflicts / Y. Danyk, T. Maliarchuk, Ch. Briggs // Connections. Spring 2017. Vol. 16, No. 2. P. 5-24; Mölder H. Information Warfare as the Hobbesian Concept of Modern Times – The Principles, Techniques, and Tools of Russian Information Operations in the Donbass / H. Mölder, V. Sazonov // The Journal of Slavic Military Studies. 2018. Vol. 31, No. 3. P. 308-328.

¹¹ Магда Е. Гибридная агрессия России в Украине: уроки для Европы / Е. Магда // Wschód Europy • Восток Европы • East of Europe. 2016. Vol 2, No. 2. С. 85-95.

аспекта информационного противоборства, либо нетривиальные рекомендации относительно использования различных технологий противостояния, как то: «вмешательство» РФ в выборы¹², особенности российской пропаганды на

¹² Blackwill R. D. Containing Russia. How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge / R. D. Blackwill. Ph. H. Gordon // Council on Foreign Relations (CFR). Council Special Report No. 80. January 2018, 43 p. URL: https://cdn.cfr.org/sites/default/files/report_pdf/CSR80_BlackwillGordon_ContainingRussia.pdf (дата обращения: 11.11.2020); Limonier K. Guerre hybride russe dans le cyberspace / K. Limonier, C. Gérard // Hérodote 2017/3, N°166-167, P. 145-163.; Wehner M. Hacking, propaganda and electoral manipulation. Moscow's information war on the West / M. Wehner // Eurozine. 21 July 2017. URL: <https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/> (дата обращения: 11.11.2020); Robets J. Q. Maskirovka 2.0: Hybrid Threats, Hybrid Response / J. Q. Roberts // Joins Special Operations University. Center for Special Operations Study and Research. December 2015; Brattberg E. Russian Election Interference. Europe's Counter to Fake News and Cyber Attacks / E. Brattberg, T. Maurer // Carnegie Endowment for International Peace. May 2018. 54 p. URL: https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf (дата обращения: 11.11.2020); Gude K. Russia's 5th Column / K. Gude // Center for American Progress. March 2017. 37 p. URL: <https://www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-column/> (дата обращения: 11.11.2020); Shuya M. Russian Cyber Aggression and the New Cold War / M. Shuya // Journal of Strategic Security. 2018. Vol. 11, No. 1. P. 1-18; Jurczyszyn L. Russia's Attempts to Influence the Presidential Election in France / L. Jurczyszyn // The Polish Institute of International Affairs, Bulletin. No. 20 (960), 28 February 2017. 2 p.; Bergmann M. War by Other Means. Russian Active Measures and the Weaponization of Information. War by Other Means / M. Bergmann, C. Kenney // Center for American Progress. Posted on June 6, 2017. 45 p. URL: <https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/> (дата обращения: 11.11.2020)

Украине¹³, деятельность СМИ и соцсетей¹⁴, включая *Russia Today*¹⁵, российские возможности в части мягкой силы¹⁶, боты и тролли¹⁷, кибератаки¹⁸ и др. Хотя

¹³ Kruk K. Analyzing the Ground Zero. What Western Countries Can Learn from Ukrainian Experience of Combating Russian Disinformation / K. Kruk // European Values Kremlin Watch Report. 11.12.2017. 24 p. URL: <https://www.europeanvalues.net/wp-content/uploads/2017/12/Analyzing-the-Ground-Zero..pdf> (дата обращения: 11.11.2020); Cyber War in Perspective: Russian Aggression against Ukraine / Kenneth Geers (Ed.) // NATO CCD COE Publications, Tallinn 2015, 175 p.; Richet J.-L. Cybersecurity Policies and Strategies for Cyberwarfare Prevention / J.-L. Richet. GI Global. 2015. 496 p.; MCINTOSH S. E. International Institutions, and the Russian People: Three Aspects of Russia's Current Information Campaign in Ukraine / S. E. McIntosh // Journal of Slavic Military Studies. 2015. No. 28. P. 299–306; Mulford J. P. Non-State Actors in the Russo-Ukrainian War / J. P. Mulford // Connections. Spring 2016. Vol. 15, No. 2. P. 89–107; Pasitselska O. Ukrainian crisis through the lens of Russian media: Construction of ideological discourse / O. Pasitselska // Discourse & Communication. 2017. Vol. 11, No. 6, P. 591–609.; Words and Wars: Ukraine facing Kremlin propaganda // K.: KIC, 2017. – 124 p.; Golovchenko Y. State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation / Y. Golovchenko, M. Hartmann, R. Adler-Nissen // International Affairs. 2018. Vol. 94, Issue 5. P. 975–994.

¹⁴ Lankina T. 'Russian Spring' or 'Spring Betrayal'? The Media as a Mirror of Putin's Evolving Strategy in Ukraine / T. Lankina, K. Watanabe // Europe-Asia Studies. 2017. Vol. 69, No. 10. P. 1526–1556; Huhtinen A.-M. Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere / A.-M. Huhtinen, J. Rantapelkonen // Journal of Information Warfare. 2016. Vol. 15, No. 4. P. 50–67; Khaldarova I. Fake News. The narrative battle over the Ukrainian conflict / I. Khaldarova, M. Pantti // Journalism Practice. 2016. Vol. 10, Issue 7. 01 June 2016. P. 891–901.; Roman N. Information wars: Eastern Ukraine military conflict coverage in the Russian, Ukrainian and U.S. newscasts / N. Roman, W. Wanta, I. Buniak // The International Communication Gazette. 2017. No. 79 (4). P. 357–378.; Nygren G. Journalism in the Crossfire. Media coverage of the war in Ukraine in 2014 / G. Nygren, M. Glowacki, J. Hök et al. // Journalism Studies. 2018. Vol. 19, Issue 7. P. 1059–1078.; Watanabe K. Measuring news bias: Russia's official news agency ITAR-TASS' coverage of the Ukraine crisis / K. Watanabe // European Journal of Communication. 2017. Vol. 32, No. 3. P. 224–241; Szostek J. Nothing Is True? The Credibility of News and Conflicting Narratives during "Information War" in Ukraine / J. Szostek // The International Journal of Press/Politics. 2018. Vol. 23 (1). P. 116–135.; Szostek J. The Power and Limits of Russia's Strategic Narrative in Ukraine: The Role of Linkage / J. Szostek // Perspectives of Polytics. June 2017. Vol. 15, No. 2. P. 379–395; Russian Social Media Influence. Understanding Russian Propaganda in Eastern Europe / T. C. Helmus, E. Bodine-Baron, A. Radin et al. // RAND Corporation Report. 2018. No. RR-2237-OSD. 148 p. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf (дата обращения: 11.11.2020); Pasitselska O. Ukrainian crisis through the lens of Russian media: Construction of ideological discourse / O. Pasitselska // Discourse & Communication. 2017. Vol. 11, No. 6. P. 591–609; Fedor J. "We need more clips about Putin, and lots of them:" Russia's state-commissioned online visual culture / J. Fedor, R. Fredheim // The Journal of Nationalism and Ethnicity. 2017. Vol. 45, Issue 2. P. 161–181.

¹⁵ Yablokov I. Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT) / I. Yablokov // Politics. 2015. Vol. 35, No. 3–4. P. 301–315; Limonier K. La stratégie d'influence informationnelle et numérique de la Russie en Europe / K. Limonier, M. Audinet // Hérodote 2017/1. N°164. P. 123–144. URL: <https://www.cairn.info/revue-herodote-2017-1-page-123.htm> (дата обращения: 11.11.2020); Nimmo B. Sputnik: Propaganda in a New Orbit / B. Nimmo // Information Warfare Initiative. January 2016. Center for European Policy Analysis (CEPA). Paper No. 2. URL: <https://silo.tips/download/propaganda-in-a-new-orbit> (дата обращения: 11.11.2020); Nelson E. Measuring RT's Impact on YouTube / E. Nelson, R. Orttung, A. Livshen // Russian Analytical Digest No. 177, 8 December 2015. 14 p. URL: <https://www.files.ethz.ch/isn/195347/RussianAnalyticalDigest177.pdf> (дата обращения: 11.11.2020); Kragh M. Russia's strategy for influence through public diplomacy and active measures: the Swedish case / M. Kragh, S. Åsberg // Journal of Strategic Studies. 2017. Volume 40, Issue 6. P. 773–816. Rawnsley G. D. To Know Us is to Love Us: Public Diplomacy and International Broadcasting in Contemporary Russia and China / G. D. Rawnsley // Politics. 2015. Vol. 35, No. 3–4. P. 273–286.

¹⁶ Hudson V. 'Forced to Friendship?' (Mis-)Understandings of Soft Power and the Implications for Audience Attraction in Ukraine / V. Hudson // Politics. August 2015. Vol. 35, No. 3. P. 330–346.; Keatinga V. Ch. Conservative soft power: liberal soft power bias and the 'hidden' attraction of Russia / V. Ch. Keatinga, K. Kaczmarek // Journal of International Relations and Development. 2017. Vol. 22, No. 2. P. 1–27.; Kochis D. Countering Russian Propaganda Abroad / D. Kochis // The Heritage Foundation. Issue Brief. No. 4286. October 21, 2014. 4 p. URL: <http://report.heritage.org/ib4286> (дата обращения: 11.11.2020); Gerber T. P. Does Russian Propaganda Work? / T. P. Gerber, J. Zavisca // The Washington Quarterly. 2016. Vol. 39, No. 2. P. 79–98; Rotaru V. Forced Attraction?, Problems of Post-Communism. How Russia is Instrumentalizing Its Soft Power Sources in the "Near Abroad" / V. Rotaru // Problems of Post-Communism. 2018. Vol. 65, Issue 1. P. 37–48.; Laruelle M. L'idéologie comme instrument du soft power russe. Succès, échecs et incertitudes / M. Laruelle // Hérodote 2017/3 (N°166–167). P. 23–35; Waggson Ch. Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare / Ch. Waggson, M. Hellman // CMS. 2018, Vol. 56, No. 5. P. 1161–1177; Slobodchikoff, Roots of Russian Soft Power: Rethinking Russian National

Identity / M. O. Slobodchikoff, G. D. Davis // Сравнительная Политика. 2017. Т. 8, № 2. С. 19-36.; Wilson J. L. Russia and China Respond to Soft Power: Interpretation and Readaptation of a Western Construct / J. L. Wilson // Politics. 2015. Vol. 35, No. 3-4. P. 287–300.; Kiseleva Y. Russia's Soft Power Discourse: Identity, Status and the Attraction of Power / Y. Kiseleva // Politics. 2015. Vol. 35, No. 3-4. P. 316–329; Rutland P. The limits of Russia's 'soft power' / P. Rutland, A. Kazantsev // Journal of Political Power. 2016. Vol. 9, No. 3, P. 395–413; Sergunin A. Understanding Russia's Soft Power Strategy / A. Sergunin, L. Karabeshkin // Politics. 2015. Vol. 35, No. 3-4. P. 347–363.

¹⁷ Zelenkauskaitė A. "Information Warfare" and Online News Commenting: Analyzing Forces of Social Influence Through Location-Based Commenting User Typology / A. Zelenkauskaitė, M. Balduccini // Social Media + Society. July 1, 2017. Vol. 3, Issue 3. URL: <https://journals.sagepub.com/doi/full/10.1177/2056305117718468> (дата обращения: 11.11.2020); Boyte K. J. An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine / K. J. Boyte // Journal of Information Warfare. 2017. Vol. 16, No. 1. P. 88-111; Abrams S. Beyond Propaganda Soviet Active Measures in Putin's Russia / S. Abrams // Connections. Winter 2016. Vol. 15, No. 1. P. 5-31; Huhtinen A.-M. Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere / A.-M. Huhtinen, J. Rantapelkonen // Journal of Information Warfare. 2016. Vol. 15, No. 4. P. 50-67; Wehner M. Hacking, propaganda and electoral manipulation. Moscow's information war on the West / M. Wehner // Eurozine. 21 July 2017. URL: <https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/> (дата обращения: 11.11.2020); Russian Social Media Influence. Understanding Russian Propaganda in Eastern Europe / T. C. Helmus, E. Bodine-Baron, A. Radin et al. // RAND Corporation, 2018. 148 p. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf (дата обращения: 11.11.2020); Connell M. Russia's Approach to Cyber Warfare / M. Connell, S. Vog // CNA Analytic Solutions. March 2017. URL: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf (дата обращения: 11.11.2020); Shallcross N. J. Social Media and Information Operations in the 21st Century / N. J. Shallcross // Journal of Information Warfare. 2017. Vol. 16, No. 1. P. 1-12; Nyst C. State-Sponsored Trolling. How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns / C. Nyst, N. Monaco // Digital Intelligence. Institute for the Future. 2018. URL: https://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf (дата обращения: 11.11.2020); Paavola J. Understanding the Trolling Phenomenon: The Automated Detection of Bots and Cyborgs in the Social Media / J. Paavola, T. Helo, H. Jalonen et al. // Journal of Information Warfare. 2016. Vol. 15, No. 4. P. 100-111; Weiss M. The Baltic elves taking on pro-Russian trolls / M. Weiss // The Daily Beast. 2016, 21 March. URL: <http://www.thedailybeast.com/articles/2016/03/20/the-baltic-elves-taking-on-pro-russian-trolls.html> (дата обращения: 11.11.2020)

¹⁸ Boyte K. J. A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare / K. J. Boyte // International Journal of Cyber Warfare and Terrorism. April-June 2017. Vol. 7, Issue 2. P. 54-70.; Kozłowski A. Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan / A. Kozłowski // European Scientific Journal. February 2014. Special edition. Vol. 3. P. 237–245; Fitton O. Cyber Operations and Gray Zones Challenges for NATO / O. Fitton // Connections. Spring 2016. Vol. 15, No. 2. P. 109-119.; Maurer T. Cyber Proxies and Their Implications for Liberal Democracies / T. Maurer // The Washington Quarterly. 2018. Vol. 41, No. 2. P. 171-188.; Geers K. (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine / K. Geers (Ed.) // NATO CCD COE Publications, Tallinn 2015, 175 p.; Deibert R. J. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war / R. J. Deibert, R. Rohozinski, M. Crete-Nishihata // Security Dialogue. 2012. No. 43 (1). P. 3–24.; The Fog of Cyber Defence / J. Rantapelkonen, M. Salminen (eds.) // National Defence University. Department of Leadership and Military Pedagogy Publication Series 2 Article Collection. No. 10. Helsinki, 2013. 236 p. URL : https://www.cyberwar.nl/d/20130200_The_Fog_of_Cyber_Defence_NDU_2013.pdf (дата обращения: 11.11.2020); Nocetti J. Géopolitique de la cyber-conflictualité / J. Nocetti // Politique étrangère. 2018. No. 2. P. 15-28; Limonier K. Guerre hybride russe dans le cyberspace / K. Limonier, C. Gérard // Hérodote 2017/3 (No. 166-167). P. 145-163; Wehner M. Hacking, propaganda and electoral manipulation. Moscow's information war on the West / M. Wehner // Eurozine. 21 July 2017 URL: <https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/> (дата обращения: 11.11.2020); Ashmore W. C. Impact of Alleged Russian Cyber Attacks / W. C. Ashmore // Baltic Security & Defence Review. 2009. Vol. 11. P. 4-40. URL: https://www.baltdefcol.org/files/files/documents/Research/BSDR2009/1_Ashmore_-_Impact_of_Alleged_Russian_Cyber_Attacks.pdf (дата обращения: 11.11.2020); Bryant W. D. International Conflict and Cyberspace Superiority. Theory and practice / W. D. Bryant. London: Routledge, 2017. 250 p.; Tikk E. International Cyber Incidents: Legal Considerations / E. Tikk, K. Kaska, L. Vihul // Cyber Defence Centre of Excellence (CCD COE). Tallinn, Estonia. 2010. 132 p.; Valeriano B. International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain / B. Valeriano, R. C. Maness // The Oxford Handbook of International Political Theory / Ch. Brown, R. Eckersley (eds.). Oxford: Oxford University Press, 2018. P. 259-272.; Shakarian P. Introduction to Cyber-Warfare. A Multidisciplinary Approach / P. Shakarian, J. Shakarian, A. Ruef. Waltham: Elsevier Inc., 2013. 337 p.; Kostyuk N. Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? / N. Kostyuk, Y. M. Zhukov // Journal of Conflict Resolution. 2019. Vol. 63, No. 2. P.317-347.; Kostyuk N. Hacking Power Grids: New Tactic of War or Wave of the Future? / N. Kostyuk // Russia Matters. 2017. 3 November. URL: <https://www.russiamatters.org/analysis/hacking-power-grids-new-tactic-war-or-wave-future> (дата обращения: 11.11.2020); Valeriano B. Persistent Enemies and Cyberwar:

интерпретация происходящего в этих работах обычно исходит из презумпции агрессивности России, они поднимают большой массив объективных фактов, позволяющих изучить характер информационного противостояния.

Западных академических публикаций, не попадающих в «обвинительный мейнстрим» по отношению к России, за рассматриваемый период было опубликовано очень мало, и принадлежат они нескольким авторам, среди них М. Кофман, О. Кемпф, С. Чарап, Р. МакДермотт¹⁹. Как правило, эти авторы опровергали существование в российской стратегии «доктрины Герасимова», отрицали существование угрозы прямой российской агрессии для Запада, искусственно гипертрофированной путём переноса неверно интерпретированных украинских событий на другие страны, а также возражали против трактовки действий России как неспровоцированной агрессии, поясняя реальный контекст происходящего. Также в них указывалось на абсурдность и

Rivalry Relations in an Age of Information Warfare / B. Valeriano, R. Mannes // *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* / D. S. Reveron (ed.). Georgetown University Press, 2012. P. 139-158.; Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses / S. Herzog // *Journal of Strategic Security*. 2011. Vol. 4, No. 2. P. 49-60.; Kari M. Russia: A Cyber Fortress Besieged / M. Kari, R. Kuusisto // *Proceedings of the 16th European Conference on Cyber Warfare and Security*, 2017. P. 593-602.; Connell M. Russia's Approach to Cyber Warfare / M. Connell, S. Vog // *CNA Analytic Solutions*. March 2017. URL: https://www.realcleardefense.com/articles/2017/05/09/russias_approach_to_cyber_warfare_111338.html (дата обращения: 11.11.2020); Spiegel C. Securing Cyberspace: NATO's Cyber Defence Policy as A Security Dispositive. Master thesis / C. Spiegel. Utrecht University, 2017. 78 p. URL: <http://dspace.library.uu.nl/handle/1874/355079> (дата обращения: 11.11.2020); Shakarian P. The 2008 Russian Cyber Campaign against Georgia / P. Shakaryan // *Military Review*. November-December 2011, p. 62-68; Ricks T. NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons / T. Ricks // *Foreign Policy*. 2017. 7 December. URL: <https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/> (дата обращения: 11.11.2020); Tamkin E. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? / E. Tamkin // *Foreign Policy*. 2017. 27 April. URL: <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on-estonia-is-the-world-better-prepared-for-cyber-threats/> (дата обращения: 11.11.2020)

¹⁹ Colon Piella G. La doctrina Gerasimov y el pensamiento estratégico ruso / G. Colon Piella // *Revista Ejército*. Diciembre 2018. No. 933. P. 30-37. URL: <https://www.ugr.es/~gesi/Doctrina-Gerasimov.pdf> (дата обращения: 11.11.2020); Kofman M. A Closer look at Russia's "Hybrid War" / M. Kofman, M. Rojansky // *Kennan Cable*, No. 7 April 2015; Kofman M. Russian hybrid warfare and other dark arts / M. Kofman // *War on the rocks*. 2016. 11 March. URL: <https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/> (дата обращения: 11.11.2020); Korybko A. Hybrid wars: the indirect adaptive approach to regime change/ A. Korybko. Moscow: Peoples' Friendship University of Russia, 2015. 132 p.; Kempf O. L'indirection de la guerre ou le retour de la guerre limitée / O. Kempf // *Politique étrangère*. 2015. No. 4. P. 157-169; Charap S. The Ghost of Hybrid War / S. Charap // *Survival*. Vol. 57, No. 6. P. 51-58.; McDermott R. N. Does Russia Have a Gerasimov Doctrine? / R. N. MaDermott // *Parameters*. Spring 2016. Vol. 46, No. 1, P. 97-106. URL: <http://www.worldinwar.eu/wp-content/uploads/2017/09/30894f4e5f758d946bbdde0850e9ac4e86f-GERASIMOV-UP.pdf> (дата обращения: 11.11.2020); Kofman M. Russian hybrid warfare and other dark arts / M. Kofman // *War on the rocks*. 2016. 11 March. URL: <https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/> (дата обращения: 11.11.2020); Basulto D. Russophobia: How Western Media Turns Russia Into the Enemy / D. Basulto. Lightning Source Inc. 2015. 286 p.; Matlock Jr. J. F. Amid 'Russiagate' Hysteria, What Are the Facts? We must end this Russophobic insanity / J. F. Matlock Jr. // *The Nation*. 2018. 1 June. URL: <https://www.thenation.com/article/archive/amid-russiagate-hysteria-what-are-the-facts/> (дата обращения: 11.11.2020); Cohen S. F. War with Russia? From Putin & Ukraine to Trump and Russiagate / S. F. Cohen. New York: Hot Books, 2019.

обречённость для России стратегии «гибридной войны» в понимании её западными исследователями либо на то, что инструменты «гибридной войны» в неменьшей степени используются самим Западом, признавалась неспособность РФ повлиять на выборы и воздействовать на западное информационное пространство в соответствии с приписываемыми ей целями. В частности, С. Чарап указал на то, что и в России, и на Западе принято описывать поведение и мотивацию контрагента как «гибридную войну», но данное описание очень далеко от реальности.

Но при том, что эти исследователи демонстрируют гораздо более адекватное понимание истинных мотивов российской внешней политики, они не спешат ставить под сомнение те меры, которые предпринял Запад в рамках курса на конфронтацию с Россией в последние годы, или дезавуировать тиражируемые репрезентации российского вызова либеральному порядку. Собственно, в западной академической мысли до сих пор не сформировалась полноценная проблематизация процесса создания концепции «гибридной войны» как целенаправленного конструирования со стороны заинтересованных субъектов (хотя при этом «симметричный» процесс конструирования в российском информационном пространстве «гибридной угрозы» со стороны Запада отражён весьма обширно²⁰). Наиболее близок к нашему оказался подход О. Фридмана, который указал на сознательную политизацию и искусственность притягивания «гибридной войны» к описанию поведения России²¹. Механизм намеренного представления России в роли сущностной угрозы «свободному миру» в западных СМИ, раскрывается в публицистических изданиях отдельных авторов, мало связанных с академической наукой²². При этом, если западная концепция «гибридной войны» ещё подвергается концептуальной критике на Западе со

²⁰ Один из наиболее полных на данный момент обзоров данного процесса представлен в монографии Gaufman E. *Security Threatsand and Public Perceptions. Digital Russia and the Ukraine Crisis* / E. Gaufman. Basingstoke: Palgrave Macmillan, 2017. 230 p.; см. также Pasitselska O. *Ukrainian crisis through the lens of Russian media: Construction of ideological discourse* / O. Pasitselska // *Discourse & Communication*. 2017. Vol. 11, No. 6. P. 591-609.

²¹ Fridman O. *Russian "Hybrid Warfare": Resurgence and Politicization*. Oxford: Oxford University Press, 2018. Фридман О. «Гибридная война» понятий (интервью) / О. Фридман // *Вестник МГИМО*. 2016. № (50). С. 79-85.

²² Basulto D. *Russophobia: How Western Media Turns Russia Into the Enemy* / D. Basulto. 2015. 286 p.

стороны перечисленных выше авторов, то работы, опровергающие существование «российской информационной угрозы» и целенаправленного курса Правительства Российской Федерации на раскалывание западных обществ с помощью анонимной активности в соцсетях, диссертанту не известны.

Российские исследователи довольно быстро обратили внимание на концепт «гибридной войны» и осознали важность информационного противоборства как ведущего элемента данного концепта. Уже в феврале 2015 г. на базе МГУ прошёл междуниверситетский научный семинар «Гибридные войны»²³, дискуссии в ходе которого во многом заложили основу для исследовательских разногласий и различий в подходах к оценке онтологической и аналитической сущности понятия «гибридной войны». Большинство участников семинара высказали обоснованную точку зрения, что данный термин сформулировали для того, чтобы компрометировать политику России и применить к ней массив международного права, касающийся войны и агрессора, однако некоторые исследователи указали на необходимость учитывать стратегические инновации и технологии Запада, в том числе, те, которые включаются в категорию «гибридных». По результатам семинара была издана первая отечественная коллективная монография по данной тематике²⁴.

Нынешние подходы отечественных учёных к трактовке понятия «гибридной войны» разнятся. С одной стороны, наблюдается тенденция к некоторой недооценке и даже нивелированию «гибридной войны», к её описанию сугубо как элемента политической риторики, используемого Западом в своих, преимущественно внутренних, политических целях и легко устранимого при наличии политической воли инициаторов. Научная же ценность данного концепта расценивается в рамках подобной точки зрения как минимальная или несуществующая, поскольку она не привносит новые

²³ «Гибридные войны» в мировой политике XXI века. Материалы научного семинара (февраль 2015 г., факультет политологии МГУ имени М. В. Ломоносова) // Политическая экспертиза. ПОЛИТЭКС. 2015. Том 11, № 2. С. 208-237.

²⁴ «Гибридные войны» в хаотизирующемся мире XXI века» / под ред. П.А. Цыганкова. М.: Издательство Московского университета, 2015. 384 с.

онтологические факты или методологические приёмы, а лишь описывает в иной терминологии уже давно используемые технологии межгосударственного противоборства. Такой подход представлен в публикациях Ю. Першина²⁵, В. Коньшева²⁶, С. Клименко²⁷, Ю. Б. Шипицина²⁸. С другой стороны, «гибридную войну» рассматривают как самостоятельную научную модель, описывающую инновационные для современной эпохи способы геополитического противостояния, применяемые Западом против России для подрыва её политической и социокультурной устойчивости. Этот подход стал «симметричным отражением» западных утверждений о ведо́мой *Россией против Запада* войне и подробно описывает подрывные действия самого *Запада против России* в терминах теорий гибридной войны, адаптированных с учётом замены субъекта и объекта воздействия. Среди работ подобной направленности можно отметить монографии Д. Чуракова и А. Матвеевой²⁹, статьи П. А. Цыганкова³⁰, Ю. А. Белоброва³¹, В. А. Гладышевского и Е. В. Горголы³², Г. Ю. Филимонова и Н. С. Данюка³³, Ю. В. Трапезникова и Л. М. Батурина³⁴, Л. В. Савина³⁵. При этом некоторые исследователи, например, А. В. Манойло, разделяя точку зрения о

²⁵ Першин Ю.Ю. «Гибридная война» как интеллектуальная провокация / Ю.Ю. Першин // Ученые записки Крымского федерального университета имени В.И. Вернадского. Философия. Политология. Культурология. Т. 1 (67). 2015. № 1. С. 80–88.; Першин Ю.Ю. Гибридная война: много шума из ничего / Ю.Ю. Першин // Вопросы безопасности. 2019. № 4. С. 78–109.

²⁶ Коньшев В. Гибридные войны: между мифом и реальностью / В. Коньшев, Р. Парфенов // Мировая экономика и международные отношения. 2019. Том 63, № 12. С. 56–59.

²⁷ Клименко С. Теория и практика ведения «Гибридных войн» (по взглядам НАТО) / С. Клименко // Зарубежное военное обозрение. 2015. № 5. С. 109–112.

²⁸ Шипицин Ю. Б. «Гибридная» война: Моделирование информационных полей: монография / Ю. Б. Шипицин, А. Ю. Шипицина; научный редактор А. Г. Нестеров. Екатеринбург: Издательство Уральского университета, 2018. 136 с.

²⁹ Чураков Д. Геостратегия России и гибридные угрозы на рубеже двух столетий. Исторический опыт локальных войн 1991—2008 годов / Д. Чураков, А. Матвева. М.: Прометей, 2021. 580 с.

³⁰ Цыганков П. А. «Гибридная война»: политический дискурс и международная практика / П. А. Цыганков // Вестн. Моск. ун-та. Сер. 18. Социология и политология. 2015. № 4. С. 253–258.

³¹ Белобров Ю. А. «Гибридные войны» НАТО: концепции и методы ведения / Ю. А. Белобров // Вестник Дипломатической академии МИД РФ. Россия и мир. 2022. № 4 (34). С. 6–21.

³² Гладышевский В.Л. Сетевая война Запада и обеспечение ресурсного противодействия сетевому сценарию для России / В.Л. Гладышевский, Е.В. Горгола // Национальные интересы: приоритеты и безопасность. 2017. Т. 13, вып. 2. С. 369–383.

³³ Филимонов Г. Ю. «Гибридная война»: интерпретации и реальность / Г. Ю. Филимонов, Н. С. Данюк // Свободная мысль. 2017. № 2. С. 24–36.

³⁴ Трапезникова Ю.В. Гибридная война как инструмент достижения мирового господства / Ю.В. Трапезникова, Л.М. Батурин // Политический вектор-про. Комплексные проблемы современной политики. 2017. № 1–2. С. 43–57.

³⁵ Савин Л. В. Стрелы кентавра. Кибервойна по-американски / Л. В. Савин. М.: Издательский дом «Кислород», 2020. 590 с.

реальности гибридной войны и подчёркивая порой ведущую роль информационной составляющей, полагают, что и Россия использует подобные технологии в конкуренции с Западом, при чём весьма небезуспешно³⁶. Примечательна исследовательская позиция А. А. Бартоша, начинавшего рассматривать «гибридную войну» с конструктивистских позиций, но впоследствии приблизившегося к более объективистской интерпретации данной категории³⁷.

Некоторые авторы (Т. А. Романова³⁸, П. В. Попов³⁹, Д. Ю. Базаркина⁴⁰) рассматривают западные концепции информационной угрозы в рамках «гибридной войны» как отражающие объективную реальность, игнорируя их изначальную антироссийскую направленность.

В то же время, в отечественной науке пока недостаточно представлен подход к рассмотрению дискурса о «гибридной войне» и «российской информационной угрозе» с точки зрения социального конструктивизма, в рамках которого было бы возможно провести деконструкцию этого дискурса, оценить его политическое значение для западного сообщества и последствия для внешней и внутренней политики нашей страны. Отдельные эпизоды процесса конструирования «российской угрозы» как широкомасштабной операции в социально-психологическом поле разобраны А. М. Сосновской, Т. А. Фоминой

³⁶ Манойло А. В. Технологии неклассической войны. Генезис. Эволюция. Практика / А. В. Манойло, К. С. Стригунов // М: Горячая линия – Телеком Москва, 2020. 378 стр.; Манойло А. Гибридная война – плацдарм, где великие державы меряются силами (интервью агентству News-Front 2016-05-11) / А. Манойло // URL: <https://www.youtube.com/watch?v=0NnADariaqM> (дата обращения: 11.11.2020); Низовцева Н.Ф. Гибридная война как геополитический тренд / Н.Ф. Низовцева, Н.В. Гришанин // Научные труды СЗИУ — филиала РАНХиГС. Том 7. Выпуск 3(25). С. 76-85.

³⁷ Бартош А. А. Сдерживание и принуждение в стратегии гибридной войны / А.А. Бартош // Военная мысль. 2021. № 9. С. 18-34.; Бартош А.А. Гибридная война становится новой формой межгосударственного противоборства / А.А. Бартош // Независимое военное обозрение. 7.04.2017. URL: http://nvo.ng.ru/concepts/2017-04-07/1_943_gibryd.html?print=Y (дата обращения: 11.11.2020); Бартош А. А. Гибридная война. Учебное пособие / А. А. Бартош. Москва: Кнорус, 2021. 306 с.

³⁸ Романова Т. А. Дезинформация (фейковые новости, пропаганда) как угроза стрессоустойчивости: подходы на уровне Евросоюза и Литвы как его члена / Т. А. Романова, Н. И. Соколов, Ю. Ю. Колотаев // Балтийский регион. 2020. Т. 12, № 1. С. 53-67.;

³⁹ Попов П. В. Возможности демократических государств по реагированию и противодействию гибридным угрозам / П. В. Попов // Via in tempore. История. Политология, 2020. № 47 (1). С. 187-193; Баранов Н. А. Стратегии гибридных войн стран НАТО как вызов Российской Федерации / Н. А. Баранов, П. В. Попов // Евразийская интеграция: экономика, право, политика. 2019. № 2. С. 79-86.

⁴⁰ Базаркина Д. Ю. Эволюция подхода Европейского Союза к борьбе с дезинформацией / Д. Ю. Базаркина // Власть. 2021. № 6. С.130-138.; Базаркина Д. Ю. Новые инструменты Европейского союза в борьбе с дезинформацией / Д. Ю. Базаркина // Аналитические записки Института Европы РАН. 2021. № 19 (249). 7 с.

и Е. Д. Буцик⁴¹. Из неакадемических источников многочисленные публикации российской прессы широко освещают развёрнутый в западных СМИ процесс диффамации России с помощью необоснованных обвинений, искажения и замалчивания фактов, новостные агентства информируют об очередных шагах по нормативному закреплению антироссийского курса в западных бюрократических структурах и сфере регулирования масс-медиа.

Тематика информационных и психологических войн в отечественной науке разрабатывается достаточно давно и плодотворно, но в фокусе её внимания находятся главным образом те конкретные приёмы, рычаги и средства, которые задействует Запад в информационной войне против России с целью ослабления её государственности, дискредитации политического курса, общественного устройства, ценностных основ и духовных скреп российского общества. Особенности приёмов и технологий, используемых западными государствами для дискредитации России в последние годы, описаны в разных публикациях. Наиболее близко к нашему подходу видение, представленное в статье А.М. Сосновской⁴², отметившей одновременно и конструирование «гибридной войны» на Западе, и применяемые при этом методы информационной войны. Метод криминализации любых оппонентов Запада с помощью слова «гибридный» и обвинений в ведении гибридной войны отмечены в статье В. Ю. Арчакова и О. С. Макарова⁴³. Следует отметить предложенный В. В. Собольниковым обзор⁴⁴ истории понимания гибридной войны, а затем поворота к её информационно-психологической составляющей как важнейшей. История принятия Пентагоном киберпространства как военной сферы под

⁴¹ Сосновская А. М. Идеология и массовые коммуникации: гибридная война на Украине / А. М. Сосновская // Научные труды Северо-Западного Института управления РАНХиГС. СПб 2016. Т. 7. Выпуск 3 (25). С. 134-142. URL: https://spb.ranepa.ru/images/nauka/NT/NT_7_3.pdf (дата обращения: 11.11.2020); Фомина Т.А. Манипулятивные приёмы дезинформации как средство реализации антироссийской пропаганды в заголовках англоязычных СМИ (на примере освещения «дела Скрипалей» в период с марта по октябрь 2018 года) / Т.А. Фомина, Е.Д. Буцик // Филологические науки в МГИМО. 2019. № 19 (3). С. 50-58.

⁴² Сосновская А.М. Идеология и массовые коммуникации: гибридная война на Украине / А.М. Сосновская // Научные труды Северо-Западного Института управления РАНХиГС. СПб 2016. Том 7. Выпуск 3 (25). С. 134-142. URL: https://spb.ranepa.ru/images/nauka/NT/NT_7_3.pdf (дата обращения: 11.11.2020)

⁴³ Арчаков В.Ю. Информационные технологии гибридных войн / В.Ю. Арчаков, О.С. Макаров // Геополитика и безопасность. 2017. №4 (40). С. 22-25.

⁴⁴ Собольников В.В. Место и роль психологического воздействия в стратегии ведения «гибридных» войн НАТО / В.В. Собольников // Гуманитарные проблемы военного дела: Военно-научный журнал. 2015. № 3. С. 25-31.

предлогом оборонных соображений и тесная связь Киберкомандования США с Агентством национальной безопасности изложена Е. А. Роговцевым и П.А. Шариковым⁴⁵ В другой статье П. А. Шарикова⁴⁶ изложена история срыва Соединёнными Штатами принятия международной конвенции против информационных войн. Развитие стратегических коммуникаций НАТО как элемента информационного и геополитического противостояния было рассмотрено Д. Л. Цыбаковым⁴⁷. Значимы также публикации А. Гуменского, М. Алхименкова, О. Шакирова⁴⁸.

Объект исследования: система противодействия «российской информационной угрозе» на Западе, начавшая формироваться в 2014 г. в результате так называемого «украинского кризиса» и последующих событий в Крыму и на Донбассе и построенная вокруг центрального тезиса об экзистенциальной опасности данной угрозы для всего западного либерального порядка.

Предмет исследования: концептуальный и институциональный аспекты системы противодействия «российской информационной угрозе» на Западе, процесс их дискурсивного оформления в академическом, общественном и политическом пространстве Запада, утверждения в качестве официального курса западных государств и институтов в соответствующих программных и позиционных документах и закреплении в их институциональной инфраструктуре.

⁴⁵ Роговский Е.А. Пентагон усиливает кибероборону / Е.А. Роговский, П.А. Шариков // США и Канада: экономика, политика, культура. 2011. № 1 (493), с. 51-60.

⁴⁶ Шариков П.А. Подходы РФ и США к проблеме международного обеспечения информационной безопасности / П.А. Шариков // Проблемы национальной стратегии. 2013. № 5 (20) 201. С. 131-144.

⁴⁷ Цыбаков Д. Л. Развертывание политико-информационных коммуникаций НАТО и Евросоюза в прибалтийском регионе / Д. Л. Цыбаков // Электронный научный журнал «ГосРег». 2021. № 3. URL: <http://gosreg.amchs.ru/pdf/files/37number/art/Tcibakov-37.pdf> (дата обращения: 10.02.2022); Цыбаков Д. Л. Фактор политических коммуникаций в процессе милитаризации постсоветского пространства / Д. Л. Цыбаков // Вестник Московского государственного лингвистического университета. Общественные науки. 2021. Вып. 3 (844). С. 98-111.

⁴⁸ Гуменский А. Шествие троллей. Как коммуникации разрушают дипломатию / А. Гуменский // Россия в глобальной политике. 2015. № 5. URL: <http://www.globalaffairs.ru/number/Shestvie-trollei-17745> (дата обращения: 11.11.2020); Алхименков М.А. Дипломатия США и украинский кризис / М.А. Алхименков // США и Канада: экономика, политика, культура. 2015. № 9 (549). С. 37-52; Шакиров О. «Российская пропаганда»: в соцсетях, в Восточной Европе, далее везде / О. Шакиров // РСМД. 24 июля 2018.

Цель исследования заключается в выявлении основных субъектов, инструментов и структур, задействованных в процессе конструирования, дискурсивного оформления и формально-институционального закрепления системы противодействия «российской информационной угрозе» на Западе, определении их роли в данном процессе.

Для достижения поставленной цели определены следующие исследовательские задачи:

- 1) установить, когда и под действием каких факторов происходит формирование представления о «российской информационной угрозе» в западной политической науке;
- 2) проанализировать происхождение, содержание и политические функции дискурса о «гибридной войне» как концептуальной основы западной системы противодействия «российской информационной угрозе»;
- 3) дать оценку представлению о «российской информационной угрозе» как одного из ключевых компонентов дискурса о «гибридной войне» в западной академической и экспертной среде;
- 4) выявить ключевые векторы формирования институциональных рамок информационного противодействия России на уровне западных межгосударственных объединений в период 2014-2016 гг.;
- 5) определить особенности первичной реакции на «российскую информационную угрозу» на уровне органов власти национальных государств;
- 6) раскрыть основные направления и движущие силы развития механизмов противодействия «российской информационной угрозе» в США после избрания Д. Трампа;
- 7) исследовать специфику выстраивания институциональной инфраструктуры противодействия «российской информационной угрозе» в европейских государствах в период 2017-2019 гг.;

- 8) охарактеризовать эволюцию институциональных механизмов информационного противодействия России на уровне западных международных организаций в период 2017-2019 гг.

Хронологические рамки исследования включают период с конца 2013 г., когда в ходе «евромайдана» на Украине стали звучать обвинения в предвзятом освещении его событий некоторыми российскими СМИ, а сопротивление промайданным политическим переменам в стране начали приписывать «кремлёвской пропаганде», до конца 2019 г. Выбор верхней хронологической границы обусловлен тем фактом, что именно к этому времени завершилось формирование официальной нормативной и институциональной базы системы противодействия «российской информационной угрозе» на международном и национальном уровнях, после чего начался этап практического задействования данной системы с параллельным упразднением некоторых неправительственных проектов и структур, чьи функции получили закрепление на официальных уровнях. С началом специальной военной операции РФ на Украине 24 февраля 2022 г. для данной системы открылся новый этап, когда она стала главным генератором информационного потока о происходящих событиях и фактором, в значительной степени определяющим политическую повестку дня и тем самым влияющим на ход боевых действий.

При этом в работе учитываются особенности формирования представления о «российской информационной угрозе» на предыдущем историческом этапе, когда представление о том, что Россия располагает инструментами информационного влияния и может задействовать их в своей внешней политике, только начало распространяться.

Основная гипотеза исследования. Концепции «российской информационной угрозы», «информационной агрессии», «кремлёвской пропаганды и дезинформации» являются не результатом «стихийной» попытки западных академических и политических кругов осмыслить события 2013-2014 гг., а целенаправленно сформированным, управляемым идеологическим конструктом, намеренно созданным антироссийскими силами на Западе и

последовательно возведённым в ранг политической нормы для гипертрофирования враждебного образа России на Западе, для выстраивания барьеров на пути возможного политического сближения после исчерпания конфликтного потенциала «украинского кризиса» и для снижения субъектного потенциала России как актора на международной арене. На базе данных концепций была выстроена самостоятельная система информационного противодействия России с вовлечением в неё как негосударственных «мозговых центров», представителей академической науки и экспертного сообщества, организаций гражданского общества, средств массовой информации, так и официальных государственных и межгосударственных структур, силовых и внешнеполитических ведомств, политических партий и высших чиновников. Представив Россию и инициатором конфронтации, и первопроходцем в использовании недопустимых методов «гибридной войны» и «информационной агрессии», архитекторы этих концепций смогли направить противостояние с Россией по заданному ими руслу, в том числе легитимизировать использование против неё самых жёстких инструментов политики «сдерживания». В результате конструирования системы противодействия «российской информационной угрозе» на Западе создана устойчивая плоскость политической конфронтации с Россией, поддерживаемая за счёт усилий неофициальных и полуофициальных структур и не зависящая от собственно действий или политики российского руководства.

Теоретико-методологическую основу исследования составляет теория социального конструктивизма, в соответствии с базовыми положениями которой факты политической жизни являются продуктами социального конструирования участниками политических процессов и приобретают самостоятельное значение и влияние по мере закрепления в автономных от акторов социальных структурах – дискурсивных, нормативных, институциональных и т. п. Эта теоретическая позиция сформировала исследовательскую призму диссертационной работы, в которой «российская информационная угроза» и её концептуальная основа в виде дискурса о «гибридной войне» изучаются как продукты намеренного

социального конструирования определённым кругом агентов в западном политическом пространстве.

Исходя из данной позиции, стержневым для проведения исследования стал метод отслеживания процесса (*process-tracing*), позволяющий реконструировать порядок и ход формирования системы противодействия «российской информационной угрозе» на Западе, выявить первичные источники дискурса о «российской пропаганде и дезинформации» в 2014-2015 гг., механизм распространения, логику его развития и способы институционального закрепления на государственном и международном уровнях в последующие годы. Для исследования концептуальной основы данной системы широко использовался дискурс-анализ, а также юридический и лингвистический анализ документов. Формирование и закрепление функций по сдерживанию и противодействию «российской информационной угрозе» в государственном аппарате отдельных западных стран и структуре международных организаций исследовалось с существенной опорой на структурно-функциональный и структурно-институциональный анализ. Для сопоставления и сравнения продвижения отдельных государств по пути построения механизмов отражения «российской информационной угрозы» был использован компаративный метод.

Следует отметить, что специфика предмета исследования, находящегося в стадии развития и претерпевающего изменения в период написания работы, а также включающего в себя несколько различных уровней анализа, связи между которыми нужно было установить в ходе исследования, обусловила необходимость поиска, отбора, оценки и синтеза в единой картине значительного массива разнородных фактологических данных, что повлекло за собой расширение эмпирической базы работы и приоритет методик систематизации и генерализации информации.

Источниковая база. Исследование опирается на широкий спектр источников различного типа, в том числе:

А) Нормативная база

- официальные документы НАТО, Европейского союза и других ведущих *западных* международных организаций и отдельных их органов, в том числе итоговые документы саммитов, позиционные заявления, программные и стратегические документы, инициативы в области информационной политики, обосновывающие наличие «российской информационной угрозы» и необходимость её отражения;

- официальные документы отдельных западных государств, а также их внешнеполитических и оборонных ведомств, законодательные инициативы, отчёты и доклады, прямо или косвенно затрагивающие тематику «российской информационной угрозы» и содержащие описание допустимых мер противодействия данной угрозе;

Б) Эмпирическая база

- публичные заявления западных, в том числе восточноевропейских, политических деятелей, выступления в СМИ официальных лиц, дипломатов и лидеров оппозиционных движений, экспертные выступления;

- академические публикации, материалы негосударственных аналитических центров, доклады по информационной политике, описывающие опасность «российской информационной угрозы» и призывающие к принятию мер для её нейтрализации;

- пропагандистские и агитационные сайты, материалы журналистских расследований, публикации в СМИ и соцсетях.

Научная новизна исследования заключается в том, что впервые в отечественной науке комплексно в качестве единой системы рассматривается сформированный на Западе в 2014-2019 гг. набор механизмов и инструментов по конструированию так называемой «российской информационной угрозы», её утверждению и противодействию; анализируются концептуальные основы данной системы, её институциональный механизм и функции в общем контексте конфронтации Запада с Россией. Помимо этого, другие элементы научной новизны работы включают:

- введение в отечественный научный оборот значительного массива не исследованных до этого официальных документов и академических работ, выделение ключевых «реперных» публикаций, задававших рамки западного дискурса о «гибридной войне» и «российской пропаганде»;

- осмысление дискурсов о «гибридной войне» и «российской информационной угрозе» как продуктов дискурсивного конструирования в западном академическом и публичном пространстве, использованных для объединения в единое целое конвенциональных, иррегулярных, экономических и информационных средств ведения войны и международной конкуренции и для приписывания России роли инициатора в использовании подобных средств для реализации военно-политических целей;

- формирование представления о системе противодействия «российской информационной угрозе» на Западе как о дисперсной сетевой конструкции, состоящей из ряда официальных и полуофициальных органов, аффилированных с западными международными организациями или функционирующих непосредственно в их структуре, и опирающейся на значительный негосударственный компонент в виде различных экспертно-аналитических институтов и волонтерских проектов;

- выделение основных этапов развития западной системы противодействия «российской информационной угрозе» на международном и национальном уровнях, а именно подготовительного этапа в 2006-2013 гг., когда в западном академическом дискурсе начали формироваться представления о наличии у России значительных возможностей для влияния в киберпространстве; начального этапа в 2013-2016 гг., когда были сформулированы и утверждены дискурсивные основы данной системы и заложены её институциональные рамки на уровне западных межгосударственных объединений; и основного этапа в 2017-2019 гг., когда были разработаны ключевые практические инструменты реагирования на «российскую информационную угрозу» и сформированы механизмы её нейтрализации на уровне отдельных государств;

- выявление функций, которые выполняет система информационного противодействия в рамках общего конфронтационного курса Запада в отношении России: во-первых, она закрепляет образ РФ не просто как ситуативного конкурента, а как ценностного антагониста Запада, во-вторых, акцентирует внимание на том, как этот антагонист якобы действует за гранью правил, допустимых в сообществе суверенных государств, чем открывает возможность для Запада не придерживаться этих правил в отношениях с Россией, в-третьих, она поддерживает накал и градус антироссийской напряжённости в западном обществе вне зависимости от реальных действий и заявлений официального руководства России. Тем самым искусственно ограничивается субъектность России как ответственного суверенного участника международных отношений, дискредитируется её официальная позиция и подрывается её политическая и правовая легитимность в глазах международной общественности.

Основные положения, выносимые на защиту:

1. Разворачивание между Западом и Россией идейно-политической конкуренции за влияние на общества постсоветских стран после серии «цветных революций» середины 2000-х годов использовалось антироссийскими силами на Западе для формирования контуров представления о «российской информационной угрозе». Его основой стала предвзятая интерпретация приписываемых РФ кибератак против Эстонии и Грузии в 2007-2008 гг. как свидетельства наличия у нашей страны потенциала для оказания деструктивного информационного воздействия на сопредельные страны и готовности задействовать его в кризисных ситуациях. Уже на этом этапе к элементам такого потенциала начинают относить не только технические возможности для совершения кибератак, но и другие информационные рычаги влияния, включая пропаганду, работу патриотических активистов и общественных сил, симпатии русских общин за рубежом.

2. Концепт «гибридной войны» является не результатом объективной оценки политических процессов, а продуктом дискурсивного конструирования с использованием экспертно-аналитической и академической формы подачи для имитации научности. Его предназначение заключалось в расширении оперативно-стратегического поля конфронтации Запада с Россией, включающем расширение круга реальных или потенциальных участников конфронтации, расширение сфер и театров оперативных действий и расширение диапазона допустимых к применению средств поражения противника. Дискурс о «гибридной войне» призван сформировать враждебный образ России как беспрецедентной и тотальной угрозы всему либеральному порядку, актора, преследующего нелегитимные цели недопустимыми методами, которые оправдывают аналогично тотальные меры Запада по отражению данной «угрозы». Механизм конструирования данного дискурса состоял в масштабном тиражировании нескольких ключевых «реперных» публикаций ведущих западных идеологов антироссийского курса (М. Галеотти, П. Померанцева, М. Вайса, К. Жилия, А. Илларионова, А. Поляковой, Э. Лукаса, М. Яйтнер, П. Маттсона), задававших базовые понятия «гибридной войны» и модели их аналитического применения, которые вскоре подхватывались официальными лицами западных государств и межгосударственных объединений, а также представителями академического сообщества. И хотя в научной среде эти понятия вызвали на первых порах некоторые дискуссии, массовость их использования наряду с закреплением на формальном политическом уровне создавала эффект самоочевидности – объективной данности, не требующей дополнительных доказательств.
3. Одним из центральных компонентов концепта «гибридной войны» является представление о «российской информационной угрозе» как комбинации кибернетических, сетевых, информационно-психологических, пропагандистских, дезинформационных, медийных, коммуникативных и иных методов воздействия на общественные процессы западных и других

стран, используемых российским руководством в рамках единой глобальной «гибридной» стратегии с целью подорвать либеральный миропорядок, дискредитировать его ценности и дестабилизировать западные демократические институты. Оно было сформировано путём атрибутирования в качестве сугубо российского по своему происхождению и источникам тиражирования целого класса применяемых западными структурами приёмов, манипуляций и технологий влияния на общество, а также ряда бытующих в западном политическом пространстве меседжей, нарративов и идеологем, противоречащих текущему либеральному идеологическому мейнстриму. Согласно данному представлению, Россия обладает значительным количественным и качественным преимуществом в подобных современных высокотехнологичных и инновационных инструментах непрямого противостояния, тогда как у Запада сохраняется критическое отставание в этой сфере, обуславливающее его уязвимость перед российскими «гибридными» средствами. Благодаря такому слиянию был сконструирован целостный образ деструктивной «российской пропаганды и дезинформации», поддерживаемый независимо от реальной позиции и действий РФ на международной арене. Конечной целью конструирования «российской информационной угрозы» является делегитимация внешней и внутренней политики России как полноправного субъекта международных отношений, имеющего право отстаивать собственную позицию и преследовать национальные интересы, в том числе, с помощью инструментов «мягкой силы» и публичной дипломатии.

4. На начальном этапе (2014-2016 гг.) разворачивания системы противодействия «российской информационной угрозе» формирование её институциональной инфраструктуры происходило в ориентации на ограниченный масштаб: она воспринималась как непосредственно затрагивающая только русскоязычное пространство и страны с многочисленным русским населением. Ведущую роль в этом процессе играл Североатлантический альянс. Он выступил в числе основных архитекторов

официального дискурса о российской «гибридной войне» и информационной угрозе, задал вектор их концептуального осмысления и распространял заданное видение через аналитические материалы и мероприятия своих полуофициальных структур – Центра стратегических коммуникаций в Риге и Центра по сотрудничеству в сфере киберобороны в Таллине. Оба центра были созданы по соглашению отдельных государств-членов НАТО и получили статус военных органов вне интегрированного командования уже после их создания; особые принципы их организации позволили осуществлять продвижение антироссийских инициатив отдельных государств-членов НАТО в качестве общей позиции альянса. Кроме того, Альянс включил киберпространство и «гибридные угрозы» в сферу своей оперативной ответственности с возможностью задействования гарантий статьи 5 Вашингтонского договора в ответ на «гибридные атаки» против его участников.

Включение Евросоюза в систему противодействия «российской информационной угрозе» происходило постепенно, начиная с весны 2015 г., под давлением со стороны некоторых государств-членов, НАТО и ряда негосударственных аналитических организаций и «мозговых центров». Работа по определению функций ЕС в рамках данной системы и закреплению их в институциональной структуре Евросоюза проводилась на двух направлениях – реагирования на вызов «российской пропаганды и дезинформации» для политики ЕС в восточном соседстве и создания потенциала для отражения «гибридных угроз» в целом. На первом направлении институционализация произошла довольно быстро, путём формирования летом 2015 г. Оперативной рабочей группы по стратегическим коммуникациям *East Stratcom* в рамках Европейской службы внешних действий, однако задачи данной группы формально были ограничены выявлением «российской дезинформации» в русскоязычном информационном пространстве. На втором направлении Евросоюз значительно продвинулся по пути признания актуальности информационных

и «гибридных» угроз, однако на уровне базовых позиционных документов, принятых в рассматриваемый период (в первую очередь Глобальной стратегии ЕС 2016 г.), прямая увязка этих угроз с Россией была ослаблена.

Борьба с «российской пропагандой и дезинформацией» в НАТО и Европейском союзе в этот период была организована не вокруг императивных ограничительных мер или ведения ответной контрпропаганды, а вокруг выявления фактов и источников распространения подобной «дезинформации», их своевременного «опровержения», повышения «сознательности» самих СМИ и «медиаграмотности» общественности. На практике подобный подход означал регулярную публичную стигматизацию любых фактов и оценок, не вписывающихся в западный нарратив украинского кризиса и последующих событий, в том числе официальной позиции российского руководства, как ложных, не заслуживающих внимания, основанных на недостоверной информации и «пропагандистских мифах».

5. Вовлечение западных государств в процесс выстраивания системы противодействия «российской информационной угрозы» происходило неравномерно. На начальном этапе можно было наблюдать четыре типа предпринимаемых национальными правительствами мер: а) публичное дискурсивное признание политическими лидерами отдельных стран наличия вызова «кремлёвской пропаганды», б) доктринальное закрепление в позиционных и программных документах общеполитического или, чаще, военно-стратегического характера указанного вызова, в) создание специальных постоянных органов или ситуативных рабочих групп, г) введение ограничительных мер в отношении российских СМИ, общественных организаций или отдельных граждан. Некоторые восточноевропейские государства (Польша, Чехия, Прибалтика) поспешили ввести ограничения против российских СМИ и инициировали вынесение данной темы на обсуждение европейских институтов; Великобритания, скандинавские страны и Нидерланды поддерживали их требования и активно

участвовали в создаваемых совместных структурах борьбы с «российской дезинформацией», но не форсировали создание специальных органов на национальном уровне. Государства Западной Европы ограничились дискурсивным признанием наличия угрозы «российской пропаганды» или закреплением её в своих позиционных документах. В США, при значительном присутствии дискурса о «российской информационной угрозе» в публичном пространстве, на официальном национальном уровне были предприняты лишь ограниченные действия на этом направлении в виде фиксации данной угрозы на законодательном уровне и на уровне общего военно-стратегического мышления, однако она не была выделена в качестве самостоятельного основания для введения ограничительных мер.

6. Результаты президентских выборов в США 2016 г. и резонанс вокруг предполагаемого российского вмешательства дали новый толчок процессу выстраивания инфраструктуры подавления «российской информационной угрозы», позволив представить эту угрозу как направленную против безопасности и стабильности Запада в целом, а не только русскоязычного пространства или стран Восточной Европы. В США необходимость противодействия «российской пропаганде» приобрела законодательное и институциональное закрепление, проявившееся в трёх плоскостях – политико-дипломатической, военной и разведывательной. Главную роль в этом процессе сыграли отдельные разведывательные, силовые и правоохранные структуры, присоединившиеся к уже сформированному симбиозу антироссийски настроенных представителей законодательной власти, экспертной среды и СМИ. Они провели публичное расследование «российского вмешательства» и вынесли на повестку дня вопрос о необходимости «наказания» России за него, прежде всего, через санкционные механизмы в информационной сфере и законодательное закрепление наложенных на Россию санкций без возможности их снятия решением президента. Наряду с одобрением специально созданного для противодействия иностранной пропаганде Центра глобального

взаимодействия в рамках Госдепартамента наибольший прогресс был достигнут в военной плоскости, благодаря регулярному усилению полномочий Пентагона в отношении проведения военных информационных операций, в том числе превентивных, скрытых и не достигающих порога прямых боевых действий, в ежегодных законах о военном бюджете. При этом были сняты действовавшие ранее ограничения, связанные с необходимостью межведомственной координации таких операций, а сами они были юридически приравнены к традиционным военным действиям, не требующим особых процедур согласования на уровне политического руководства страны.

7. В 2017-2019 гг. под влиянием медийного резонанса от предполагаемого «российского вмешательства» в избирательные процессы практически все европейские государства перешли к формированию собственных национальных структур для ответа на вызов «российской информационной угрозы». Однако и на этом этапе между ними сохранялись отличия: в одних, наиболее радикальных, случаях (Великобритания, Чехия, Швеция) создавались специальные подразделения в силовых ведомствах, в других речь шла о включении данной угрозы в военно-стратегические программные документы (Бельгия, Польша), в третьих (Франция, ФРГ) процесс свёлся пока что только к принятию законодательных актов по ужесточению контроля над информационной сферой и соцсетями со стороны национальных регуляторов. Ведущей тенденцией в развитии системы подавления «российской информационной угрозы» на уровне национальных европейских государств в данный период стало законодательное оформление нормативной базы контроля за информационным пространством, СМИ и социальными сетями с обязательствами последних удалять нежелательные материалы, квалифицированные как дезинформация, и возможностями государственного контроля за их удалением.

В становлении инфраструктуры борьбы с «российской информационной угрозой» в рассматриваемый период особую роль играла Великобритания.

Несмотря на то, что в британском государственном аппарате степень институционализации функций, связанных с информационным противодействием России, оставалась не самой высокой, официальный Лондон выступил в роли активного генератора дискурса об исходящих от России «гибридных угрозах» на международной арене, принял наиболее жёсткие ограничительные меры в отношении российских СМИ, а его представители участвовали и осуществляли руководство многими международными структурами, созданными для борьбы с «российской пропагандой».

8. На уровне межгосударственных объединений развитие системы информационного противодействия России проходило по пути инкорпорации информационных и «гибридных» угроз в военно-стратегический аппарат НАТО и ЕС. Для подкрепления политических обязательств о возможности задействования гарантий безопасности НАТО для отражения «гибридных атак» в структуре Альянса были образованы уже не просто аффилированные центры, а стационарные подразделения, осуществляющие мониторинг, планирование операций и подготовку потенциала для задействования в случае «гибридных сценариев» конфликтов. Также Альянс продолжил играть направляющую роль в формировании повестки дня в области «гибридных угроз» для Европейского союза, в том числе с помощью образованного для этих целей Европейского центра передового опыта в Финляндии. В структуре европейского компонента данной системы в этот период выделяются три ключевых самостоятельных направления: 1) предупреждение и нейтрализация вызовов в киберпространстве, 2) отражение «гибридных угроз» и 3) борьба с дезинформацией и «фейковыми новостями», в рамках которой отдельное значение придаётся регулированию социальных сетей. Благодаря активному подключению Еврокомиссии был достигнут значительный прогресс в виде формирования отдельного механизма регулирования «дезинформации» со специально прописанными критериями и принципами, а также

ответственностью СМИ и соцсетей за удаление нежелательного «пропагандистского» контента.

Теоретическая значимость исследования заключается в переосмыслении концепта «гибридной войны» как особого идеологического конструкта, введённого в западное публичное и академическое пространство для решения конъюнктурных политических задач в контексте конфронтации с Россией, а не описания реально существующего или вновь открытого феномена, а также в углублении представлений о дискурсивном конструировании политической реальности в западном публичном пространстве, в том числе через экспертные и академические публикации программирующего, а не описательного, характера.

Полученные результаты могут стать основой для дальнейшего изучения внешней политики западных стран и межгосударственных объединений, механизмов формирования и реализации их политического курса в отношении России и постсоветского пространства, в том числе механизма дискурсивного конструирования угроз.

Практическая значимость исследования. Положения и выводы данного исследования могут быть использованы для выработки целевых основ внешней политики России в отношении Запада в условиях комплексной политико-стратегической конфронтации, а также для разработки инструментов обеспечения международного имиджа и информационной безопасности государства. Кроме того, они могут быть использованы в ряде учебных дисциплин, связанных с внешней политикой России, современными международными отношениями, конфликтологией и информационной безопасностью.

Область диссертационного исследования. Диссертация соответствует пункту 11 «Внешнеполитическая деятельность государств, международных организаций, общественных и политических движений и других субъектов мировой политики», а также пункту 2 «Субъекты международных отношений. Деятельность государственных и негосударственных акторов. Формальные и неформальные институты в международных отношениях и в мировой политике.

Формирование и реализация внешнеполитических стратегий, концепций и доктрин» и пункту 17 «Информационные, когнитивные, био- и другие новые технологии в международных отношениях и мировой политике» паспорта специальности 5.5.4. «Международные отношения, глобальные и региональные исследования».

Апробация результатов исследования. Основные положения и выводы диссертации были представлены автором на ряде научных конференций:

- XVII Международная научно-практическая конференция "Актуальные вопросы в современной науке", г. Томск, 19 декабря 2018 г.
- XII Международная научно-практическая конференция «Актуальные вопросы в науке и практике», г. Самара, 10 декабря 2018 г.

По результатам исследований были изданы 8 научных публикаций, из них 4 статьи в профильных изданиях ВАК:

1. Царик В. С. Система противодействия «российской информационной угрозе» на Западе: структура, основные уровни и инструменты / В. С. Царик // Среднерусский вестник общественных наук. 2018. Том 13, Номер 6. С. 97-110.
2. Царик В. С. Западная интерпретация информационных конфликтов вокруг Эстонии и Грузии в 2007-2008 гг. в русле концепции «гибридной войны» / В. С. Царик // Актуальные вопросы в современной науке: сборник статей по материалам XVII международной научно-практической конференции. Уфа: Дендра, 2018. С. 173-182.
3. Царик В. С. Конструирование «гибридной войны» в западном информационном пространстве: основные стадии и субъекты / В. С. Царик // Вестник РГГУ. Серия «Политология. История. Международные отношения». 2020. № 3. С. 20-34.
4. Царик В. С. Основные подходы к исследованию «гибридной войны» в российской политологической мысли / В. С. Царик // Актуальные вопросы в науке и практике: сборник статей по материалам XIII международной научно-практической конференции. Уфа: Дендра, 2018. С. 161-171.

5. Царик В. С. Борьба с «российской дезинформацией» в публичном позиционировании западных институтов: анализ официальных сайтов НАТО и Европейского союза / В. С. Царик // Среднерусский вестник общественных наук. 2019. Том 14, Номер 6. С. 109-125.
6. Царик В. С. Деятельность западных негосударственных организаций и аналитических институтов в сфере борьбы с «российской дезинформацией» / В. С. Царик // Вестник Международного юридического института. 2019. № 4 (71). С. 152-165.
7. Царик В. С. Противодействие «российской информационной угрозе» в политике Европейского союза после украинского кризиса: дискурсивный и институциональный аспекты / В. С. Царик // Среднерусский вестник общественных наук. 2020. Том 15, Номер 5. С. 107-123.
8. Царик В. С. Принцип поэтапности в ужесточении регулирования информационного пространства в ответ на «российскую информационную угрозу» (на примере Германии и Франции) / В. С. Царик // Вестник Международного юридического института. 2020. № 3 (74). С. 14-27.

Структура диссертации. Работа выполнена в объёме, соответствующем требованиям ВАК, и состоит из введения, трёх глав, шести параграфов, списка использованных источников и литературы.

Глава 1. Конструирование «российской информационной угрозы» в западной политологической мысли

1.1. Формирование представления о «российской информационной угрозе» в западном политическом пространстве в 2007-2013 гг.

Представление о том, что Россия в её внешней политике может составлять угрозу Западу и отдельным его государствам в информационной сфере, формировалось постепенно, неравномерно и достигло нынешней степени интенсивности лишь после украинского кризиса 2014 г.

Его нельзя назвать отголоском или наследием холодной войны: хотя пропагандистская составляющая биполярной конфронтации, несомненно, имела место, она отличалась некоторой упорядоченностью и несравнимо меньше влияла на политический уровень отношений между противостоящими сверхдержавами⁴⁹. Принятие Советским Союзом демократических ценностей в ходе окончания холодной войны стало одним из зримых признаков победы Запада в этой конфронтации, в связи с чем в западном сообществе долгое время преобладало мнение о том, что на новом историческом этапе Россия не может составить ему конкуренцию в идейно-ценностной плоскости и представить миру собственную, альтернативную модель развития, привлекательную настолько, чтобы она позволила оказывать политическое влияние на иные, даже сопредельные страны. Наоборот, в центре внимания западного экспертного и политического сообщества были методы информационного управления, применяемые российским Правительством в отношении населения РФ в ходе укрепления государственной власти при Президентстве В.В. Путина⁵⁰.

⁴⁹ Фененко А. В. Новая мобилизация? / А. В. Фененко // РСМД. 26 июля 2018. URL: <http://russiancouncil.ru/analytics-and-comments/analytics/novaya-mobilizatsiya/> (дата обращения: 16.10.2018)

⁵⁰ См. например Bardach-Yalov E. Analyzing Russian propaganda: Application of Siegfried Kracauer's qualitative content analysis method / E. Bardach-Yalov // Journal of Information Warfare. 2012. Vol.11, No. 2. P. 24–36.; Hellum N. The War at Home: Putin's Information Strategy Toward the Russian Population / N. Hellum // Information Sharing in Military Operations / I. Goldenberg, J. Soeters, W. H. Dean (eds.). Switzerland: Springer International Publishing, 2017. P. 235-250.; Gaufman E. Security Threats and Public Perceptions. Digital Russia and the Ukraine Crisis. Basingstoke: Palgrave Macmillan, 2017. 230 p.

Поворот к восприятию России как авторитарной недружественной страны, несущей угрозу демократическим ценностям, начинается с середины 2000-х гг.⁵¹, однако тогда это было связано главным образом с негативным освещением внутренних перипетий в нашей стране и укреплением системы управления.

«Цветные революции» в постсоветских странах в первой половине 2000-х годов ознаменовали в глазах западной аудитории очередную идеологическую победу либеральной модели над так называемым «новым российским авторитаризмом» и таким образом создали ситуацию идейной конкуренции на постсоветском пространстве между Западом и Россией, к которой руководство нашей страны изначально не стремилось. Однако расширение западного присутствия в ближнем зарубежье заставило Москву активизировать усилия по укреплению своего авторитета и поддержки со стороны общественности сопредельных стран. И хотя официальное руководство РФ никогда не преследовало цель подрыва государственности и тотальной дестабилизации этих стран, отдельные антироссийски настроенные политические силы уже предпринимали попытки выставить «мягкую силу» России в качестве серьёзного вызова демократическим процессам и институциональной состоятельности в постсоветских странах, акцентировать деструктивный потенциал внешней политики России в информационной сфере и вынести на повестку дня необходимость целенаправленного противодействия ей. Тем самым эти силы стремились повысить собственный политический вес в западном сообществе и получить контроль над ресурсами, которые могли быть выделены на борьбу с «российской угрозой».

Так, ещё до окончательного вступления в НАТО, в 2003 г. Эстония выступила с инициативой создания особого органа Альянса в сфере кибербезопасности в свете нарастающих угроз в этой сфере, в том числе, от России⁵². Концепция подобного органа получила одобрение Верховного

⁵¹ Tsygankov A. P. Russia and America: The Asymmetric Rivalry / A. P. Tsygankov. London: Polity, 2019.

⁵² Laasme H. The Role of Estonia in Developing NATO's Cyber Strategy / H. Laasme // CICERO Foundation. Great Debate Paper. December 2012. No. 12/08. P. 11. URL: https://www.cicerofoundation.org/wp-content/uploads/Laasme_-_Estonia_NATO_Cyber_Strategy.pdf (дата обращения: 11.11.2020)

командования НАТО по трансформации в 2006 г.⁵³, однако особого публичного резонанса в тот момент она не имела. И только после инцидентов с предполагаемыми массированными кибератаками на объекты информационной системы Эстонии в 2007 г. и предполагаемым информационным воздействием на грузинскую инфраструктуру в ходе конфликта в августе 2008 г.⁵⁴ тематика «российской киберугрозы» стала продвигаться в западном академическом и политическом дискурсе⁵⁵. Это привело, в том числе, к воплощению эстонской инициативы и созданию Центра передового опыта НАТО в области кооперативной киберобороны в Таллине.

Инцидент вокруг Эстонии внёс три существенные инновации в обсуждение тематики современных информационных угроз на Западе. Во-первых, он вывел на первый план в качестве предполагаемых исполнителей кибератак ряд российских неправительственных общественных движений патриотической направленности, номинально автономных, но при этом связанных с правящей партией «Единая Россия». Во-вторых, он усилил напряжение вокруг русской общины Эстонии как возможного фактора дестабилизации этой страны и других стран со значительной долей русского населения. И, в-третьих, он актуализировал государствоцентричное измерение проблемы кибербезопасности: если до упомянутых событий киберугрозы рассматривались, как правило, в одном комплексе с так называемыми новыми угрозами безопасности, исходящими преимущественно от негосударственных субъектов,

⁵³ The NATO Cooperative Cyber Defence Centre of Excellence. URL: <https://ccdcoc.org/about-us/> (дата обращения: 11.11.2020)

⁵⁴ В 2007 г. в Эстонии, на фоне протестов против сноса таллинскими властями монумента «Бронзового солдата», а в 2008 г. в Грузии, во время августовской войны, отмечались многочисленные сбои в работе электронной инфраструктуры: не были доступны некоторые правительственные и новостные сайты, отключался электронный банкинг, наблюдались проблемы у операторов мобильной связи, проводилась подмена контента правительственных страниц на оскорбительный. Подробнее см.: Идеон А. Wikileaks: Эстония отделалась легко / А. Идеон // ИНОСМИ. 11.12.2010. URL: <https://inosmi.ru/baltic/20101211/164825182.html> (дата обращения: 11.11.2020), Pernik P. The early days of cyberattacks: the cases of Estonia, Georgia and Ukraine / P. Pernik // Hacks, leaks and disruptions – Russian cyber strategies / N. Popescu, S. Secriery (Eds.) // EU ISS Chaillot papers. 2018. No. 148. P. 55. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (дата обращения: 11.11.2020)

⁵⁵ См., например, Haukkala H. A. Close Encounter of The Worst Kind? The Logic of Situated Actors and the Statue Crisis Between Estonia and Russia / H. A. Haukkala // Journal of Baltic Studies. 2009. Vol. 40, No. 2. P. 201–213.; Crandall M. Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms / M. Crandall, C. Allan // Contemporary Security Policy. 2015. Vol. 36, No. 2. P. 346–368; Deibert R. J. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war / R. J. Deibert, R. Rohozinski, M. Crete-Nishihata // Security Dialogue. 2012. Vol. 43(1). P. 3–24.

то после 2007 г. возможность использования кибератак в ходе межгосударственной конкуренции стала гораздо более обсуждаемой темой. В официальном западном дискурсе эстонский инцидент стал рассматриваться как первый случай «политически мотивированных» кибератак против системы управления государством.

В конфликте с Грузией 2008 г. информационные средства воздействия сыграли ограниченную, если не сказать второстепенную, роль, однако сам факт их использования Россией параллельно с реальными боевыми действиями позволил заинтересованным силам делать заявления о систематическом применении нашей страной информационного оружия для нанесения прямого военного ущерба своим соседям. Увязывание в единую цепочку крайне спорных и не до конца обоснованных фактов об использовании российским руководством кибер- и информационных атак в Эстонии и Грузии стало краеугольным камнем образа «российской информационной угрозы» в западной политической риторике в 2007-2013 гг.

Это прослеживается в экспертных и академических публикациях указанного периода, в которых производится конструирование образа «российской информационной угрозы» на основе узкого разбора эстонского и грузинского инцидентов 2007-2008 гг. с приданием им явно завышенного, гипертрофированного политического и стратегического значения. Тон этим публикациям был задан работами самого таллинского центра, особенно в контексте разработки новой Стратегической концепции НАТО в 2009-2010 гг. Показательным в этом плане является опубликованный в 2010 г. легалистский разбор киберинцидентов вокруг Эстонии, Грузии, Литвы и радио «Свобода – Свободная Европа», пока ещё, впрочем, не содержащий радикальных

характеристик и предложений⁵⁶, а также ряд статей в специализированных изданиях по информационной безопасности⁵⁷.

На начальном этапе основное внимание в академических публикациях уделяется доказательству причастности российского руководства к организации кибератак против Эстонии и Грузии. Так, в развёрнутой монографии майора армии США У. Эшмора 2009 г.⁵⁸ признаётся, что прямых доказательств причастности РФ к кибератакам против Эстонии и Грузии нет, но отдельные общественные деятели РФ либо заявляли, что к атакам причастны какие-то их знакомые (заявление депутата Госдумы РФ Сергея Маркова), либо предлагали что-то похожее (идеи профессора МГИМО Игоря Панарина о кибервойне).

В отсутствие неопровержимых фактов доказательство нередко проводилось методом поиска главного бенефициара, которым, ожидаемо, выступали именно российские власти. Например, в работе капитана армии США П. Шакаряна 2011 г.⁵⁹ разбираются три версии кибератак, якобы проведённых против Грузии: самоорганизация патриотической Интернет-общественности России, действия русской организованной преступности и задание российского правительства. Версия самоорганизации российских патриотов отвергается автором на том основании, что инициаторы атаки заранее знали, какие грузинские ресурсы подлежат приоритетной атаке; версия об организации атак русской оргпреступностью отвергается автором на том основании, что не просматривается мотива, наконец, версия об организации атак Правительством РФ подтверждается косвенными аргументами о том, что *«кибератаки в целом способствовали успеху российской операции»*.

⁵⁶ Tikk E. International Cyber Incidents: Legal Considerations / E. Tikk, K. Kaska, L. Vihul // Cyber Defence Centre of Excellence (CCD COE). 12 Filtri Rd. 10132 Tallinn, Estonia. 2010. 132 p.

⁵⁷ См. например Efthymiopoulos M. P. NATO's Security Operations in Electronic Warfare: the Policy of CyberDefence and the Alliance's new Strategic Concept / M. P. Efthymiopoulos // Journal of Information Warfare. 2009. Vol. 8, No. 3. P. 61-70.

⁵⁸ Ashmore W. C. Impact of Alleged Russian Cyber Attacks / W. C. Ashmore // Baltic Security & Defence Review. 2009. Vol. 11. P. 4-40. URL:

https://www.baltdefcol.org/files/files/documents/Research/BSDR2009/1_Ashmore - Impact of Alleged Russian Cyber Attacks.pdf (дата обращения: 11.11.2020)

⁵⁹ Shakarian P. The 2008 Russian Cyber Campaign against Georgia. / P. Shakarian // Military Review. November-December 2011, p. 62-68.

Шаблонность приведённой схемы можно обнаружить, сравнив её с ходом рассуждений из статьи Р. Дейберта, Р. Рогожинского и М. Крит-Нишихаты 2012 г.⁶⁰ В разделе об атрибуции кибератак против Грузии авторы разбирают, действительно ли можно приписать их авторство Правительству РФ. Они пишут, что DDoS-атаки исходили из разных стран (больше всего из США), по распределению их в течение суток тоже нельзя выявить закономерность. Нет и прямых доказательств того, что Правительство России вдохновляло эти атаки от частных лиц. Далее разбирается гипотеза о самоорганизации российских криминальных групп для кибербунта против Грузии из патриотических соображений, вероятность которой косвенно подтверждена прецедентами самоорганизации российских патриотических групп и тем, что информация о путях нанесения ущерба Грузии размещалась на российских хакерских форумах. Авторы пишут, что этот сценарий вероятен, поскольку в Интернет-пространстве легче договориться о коллективных действиях, как и координировать их. *«Если бы этот сценарий имел место во время войны между Россией и Грузией, он бы сигнализировал о появлении нового фактора в операциях в киберпространстве – способности группы, отличной от воюющих сторон, создавать значительные эффекты в киберпространстве и через него»*⁶¹. В то же время, в заключении установление авторства кибератак вновь сводится к мотивационному рассуждению «кому выгодно?».

В рамках той же линии на увязывание отдельных киберинцидентов и приписывание их организации Кремлю написана статья А. Козловского начала 2014 г.⁶², но в ней к числу объектов российских кибератак отнесена даже Киргизия. Среди наиболее резких материалов, предвосхитивших радикальный тон последующих лет, следует отметить материал С. Герцога⁶³, в котором

⁶⁰ Deibert R. J. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war / R. J. Deibert, R. Rohozinski, M. Crete-Nishihata // Security Dialogue. 2012. Vol. 43(1). P. 3–24.

⁶¹ Ibid., P. 17.

⁶² Kozlowski A. Comparative Analysis of Cyberattacks on Estonia, Georgia and Kyrgyzstan / A. Kozlowski // European Scientific Journal. February 2014. Special edition. Vol. 3. P. 237–245.

⁶³ Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses / S. Herzog // Journal of Strategic Security. 2011. Vol. 4, No. 2. P. 49–60. URL: <http://scholarcommons.usf.edu/jss/vol4/iss2/4> (дата обращения: 11.11.2020)

предполагаемые атаки на Эстонию названы терроризмом, угрожающим «суверенитету в киберпространстве», им приписана высокая степень опасности. Тем не менее, вопрос об установлении подлинного инициатора в очередной раз излагается через призму потенциальных интересов, а не реальных фактов: *«Учитывая передовые возможности России в области кибервойн и серьёзность атак на Эстонию, закономерно задать вопрос, были ли эти атаки действительно совершены автономными сетями русскоязычных хакеров или они были совершены или спонсированы Кремлём. Несмотря на то, что технические эксперты ЕС и НАТО не смогли найти доказательств причастности России к инциденту с кибертеррористической ситуацией в Эстонии, организовать DDoS-удары было бы в интересах Москвы»*⁶⁴.

Ещё одним важным материалом, раздувающим информационную угрозу со стороны РФ, якобы нависающую над Западом, можно назвать написанную Н. Гвоздевым главу «Медведь становится цифровым: Россия и её кибервозможности» из сборника 2012 г. «Киберпространство и национальная безопасность»⁶⁵. Эта работа служит примером искусственного объединения разнородных сторон информационного соперничества в единый пучок и его привязывания к общей проблематике геополитического противостояния, которая спустя некоторое время получит освещение в рамках концепции «гибридной войны». По утверждению автора, современная Россия ушла от стратегии баланса сил и намерена захватывать Европу *«если не танками, то банками»*, поэтому в итоге пришла к необходимости ведения информационной войны. Для этого Правительство РФ, по утверждению авторов, привлекает к участию в своих операциях хакеров, участвовавших в нелегальной деятельности против американских финансовых структур. Автор также приводит примеры и бесплатного участия добровольцев в кибератаках против Грузии, и оплаченного

⁶⁴ Ibid., P. 53.

⁶⁵ Gvosdev N. K. The Bear Goes Digital: Russia and Its Cyber Capabilities / N. K. Gvozdev // Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World Book / D.S. Revelon (ed.). Georgetown: Georgetown University Press, 2012. P. 173–190.

участия кибергруппировки «Серые гуси» против Эстонии⁶⁶. В итоге, по мнению автора, Россия значительно усилила свой потенциал в информационной сфере и при желании может пустить его в ход.

Более объективным направлением публикаций указанного периода было исследование состояния информационной сферы и её возможной роли в межгосударственном противостоянии. Так, в другой главе вышеуказанного сборника⁶⁷ Дж. Шелдон анализирует роль киберопераций среди прочих военно-стратегических инструментов. В частности, он довольно чётко указывает на то, что сами по себе кибероперации – лишь один из инструментов достижения реального стратегического результата, бессмысленный без операций соответствующего масштаба вне виртуальной сферы. В то же время приписываемые РФ кибератаки не сопровождались никакими неvirtуальными действиями, призванными закрепить успех. Дополняет выводы Дж. Шелдона материал Б. Валерьяно и Р. Манесса в другой главе того же сборника⁶⁸, в котором разбираются теоретические вопросы киберстратегии в отношении стойких противников – стран, отношения с которыми очень враждебны в течение длительного времени (США и Израиль против Ирана, Россия против Грузии). На основе изучения показательных случаев авторы приходят к выводу, что стойкие противники используют кибернетическое противостояние, однако оно не слишком распространено и до сих пор не повышало напряжённость. Тот факт, что государства отрицают свою причастность к кибератакам, приписывая их патриотическим негосударственным акторам, как в случае с Россией и Грузией в 2008 г., говорит о наличии весомых сдерживающих факторов, препятствующих эскалации противостояния в киберсфере⁶⁹.

⁶⁶ Ibid., P. 182-183.

⁶⁷ Sheldon J. B. Toward a Theory of Cyber Power: Strategic Purpose in Peace and War / J. B. Sheldon // *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* Book / D.S. Reveron (ed.). Georgetown: Georgetown University Press, 2012. P. 207-224.

⁶⁸ Valeriano B. Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare. / B. Valeriano, R. Mannes // *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* / D. S. Reveron (ed.). Georgetown: Georgetown University Press, 2012. P. 139-158.

⁶⁹ Ibid., P. 153-154.

Важным свидетельством этого периода может служить работа Кера Жилия 2011 г.⁷⁰, привлечённого тогда к сотрудничеству с натовским центром в Таллине и сыгравшего после 2014 г. видную роль в конструировании «российской информационной угрозы». Тогдашний анализ Жилия полностью опровергает его же трактовку «российской информационной угрозы» после 2014 г. Автор отмечает, что после провала информационной составляющей войны против Грузии в российских политических кругах началось обсуждение возможности создания информационных войск, но официально они не появились. Мало того, в РФ раскрылось много киберуязвимостей, вплоть до контроля западными фирмами кибербезопасности важных отраслей, включая даже таможню и «Газпром». Однако никаких следов объединённого киберкомандования в РФ Жиль не находит и отмечает, что отношение к идее создания подобного рода войск в российских военной среде весьма скептическое, но, несмотря на это, их формирование является неизбежным вследствие общих тенденций милитаризации киберпространства⁷¹.

При очевидной тенденции на формирование преувеличенного образа «российской информационной угрозы» в экспертной среде Запада на официальном уровне этой угрозе придавалось весьма ограниченное, локальное, оперативное значение, поэтому она не была вынесена на политико-стратегическую повестку дня отношений Запада с Россией и не стала препятствием для «перезагрузки» отношений России с США в 2009-2011 гг. Более того, по мере того, как первичная «перезагрузка» начал заходить в тупик, в западной печати стали появляться публикации, постулирующие целесообразность сотрудничества с РФ в информационной сфере для поддержания наметившегося кооперативного импульса.

⁷⁰ Giles K. "Information Troops" – a Russian Cyber Command? / K. Giles // 2011 3rd International Conference on Cyber Conflict / C. Czosseck, E. Tyugu, T. Wingfield (Eds.). Tallinn, 2011, P. 45-60. URL: http://www.conflictstudies.co.uk/files/Russian_Cyber_Command.pdf (дата обращения: 11.11.2020)

⁷¹ Ibid., P. 56.

Так, в работе Джоффа ван Эппса⁷², опубликованной осенью 2013 г., указывалось, что, несмотря на всю проблемность РФ для Запада (РФ может доставить Западу неприятности, но заведомо не представляет экзистенциальной угрозы), необходимо продолжить с ней сотрудничество ради общих интересов в определённых областях кибернетической безопасности, в частности, достичь консенсуса по международному киберзаконодательству. Статья группы российских и американских авторов, написанная в 2011 г.⁷³, содержит полезный сравнительный обзор развития сюжета и понимания кибербезопасности в США и РФ. Наконец, в работе Ш. Гросса⁷⁴ содержится вполне объективное и уважительное описание российского подхода к информационной безопасности, указывается, что именно Россия была объектом террористических атак с использованием экстремистами Интернета, и подробно разбирается суть разногласий по конвенции о кибербезопасности с Западом.

Само по себе наличие подобных работ показывает, что даже после эстонского и грузинского инцидентов «российская информационная угроза» в западном политическом пространстве воспринималась неоднозначно и не имела настолько подавляющего веса, чтобы делать недопустимой идею о налаживании сотрудничества с руководством РФ в данной сфере.

Следует отметить, что в начале 2010-х гг. Россия приступила к развитию собственных информационных ресурсов для зарубежной аудитории, прежде всего, канала *Russia Today*, радио «Голос России» и агентства *Sputnik*. Российские медиа продемонстрировали способность создавать качественный информационный продукт, представляющий интерес для общественности многих западных государств и в то же время предлагающий альтернативные интерпретации текущих событий, отличные от предвзятой, идеологизированной

⁷² Van Epps G. Common Ground U.S. and NATO Engagement with Russia in the Cyber Domain / G. Van Epps // Connections. Fall 2013. Vol. 12, No. 4. P. 15-50.

⁷³ Barmin Yu. International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and Information Security / Yu. Barmin, G. Jones, S. Moiseeva Z. Winkelman // The Quarterly Journal. Fall 2011. P. 73-94.

⁷⁴ Cross Sh. N. Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the "Reset" / Sh. N. Cross // Journal of Strategic Security. 2013. Vol. 6, No. 4, P. 1-24. URL: <http://scholarcommons.usf.edu/jss/vol6/iss4/1> (дата обращения: 11.11.2020)

направленности большинства западных «мейнстримных» СМИ. Появление подобных ресурсов вынесло на поверхность наличие у России своих инструментов «мягкой силы»⁷⁵, что стало неожиданностью для западных наблюдателей, убеждённых, что в этой сфере Москва не обладает сколь-нибудь значимыми возможностями. Одновременно, начиная с 2012 г., наблюдается усиление градуса идеологически мотивированной критики в отношении России и Запада, когда западные лидеры и СМИ подвергли острой критике принятые российским руководством меры, расцененные как ограничительные для свободы прессы и Интернета, в т. ч. принятие закона об иностранных агентах, расширение полномочий Роскомнадзора, ограничения для телеканала «Дождь» и т. п.⁷⁶

Таким образом, в период 2007-2013 гг. на Западе с опорой на предвзятую интерпретацию инцидентов вокруг Эстонии и Грузии были сформированы основные контуры представления о «российской информационной угрозе» как целенаправленном использовании кибератак и других информационных средств влияния для достижения политических и военно-стратегических целей в ущерб интересам и безопасности западных государств. Тем не менее, российские оперативные возможности в информационной сфере и киберпространстве и результаты их задействования оценивались западным академическим сообществом весьма скептически. С одной стороны, инциденты с кибератаками против Эстонии и Грузии, руководство которыми приписывали российским спецслужбам с возможным привлечением некоторого числа «патриотических хакеров» вне государственных структур, рассматривались только как свидетельство наличия у России достаточного потенциала для организации подобных локальных атак против более слабых противников⁷⁷, и лишь отдельные эксперты полагали, что данные инциденты играли роль «пробного

⁷⁵ Довольно полный систематизированный обзор этих инструментов представлен в статье Е. Осиповой: Osipova Ye. Indigenizing soft power in Russia / Ye. Osipova // The Routledge Handbook of Soft Power / N. Chitty, L. Ji, G. D. Rawnsley, C. Hayden (eds.). Abingdon: Routledge, 2017. P. 346–357.

⁷⁶ См. подробнее Tsygankov A. P. The Dark Double US Media, Russia, and the Politics of Values / A. P. Tsygankov. Oxford: Oxford University Press, 2019. 192 p.

⁷⁷ Giles K. “Information Troops” – a Russian Cyber Command? / K. Giles // 2011 3rd International Conference on Cyber Conflict. C. Czosseck, E. Tyugu, T. Wingfield (Eds.). Tallinn, Estonia, 2011, P. 45-60.

шара» для отработки более масштабных методов воздействия, которые могут быть применены в случае конфликта с США и НАТО⁷⁸. Но, с другой стороны, оба эти инцидента принесли российскому руководству довольно сомнительные результаты в информационном плане, что, с учётом общей ограниченности ресурсов и дефицита «мягкой силы», делало потенциальную «российскую информационную угрозу» весьма относительной. К тому же, российское стратегическое мышление в информационной сфере, по мнению западных аналитиков, носило явно оборонительный, а не наступательный характер⁷⁹.

На основании этого можно заключить, что на этапе до 2014 г. большинство академических и экспертных работ, посвящённых возможному информационному и кибернетическому противостоянию с Россией, достаточно объективно оценивали положение дел и описывали существующие разногласия, однако ряд авторов, связанных с американской армией, натовским центром в Таллине и др. уже приступили к обвинению России в организации кибератак и ведении информационной борьбы на основе косвенных данных по нескольким инцидентам (Эстония, Грузия, Киргизия). Однако и они не объявляли эти приписываемые России действия актом прямой войны, наиболее радикальной характеристикой являлось приравнивание этих действий к терроризму.

1.2. Дискурс о «гибридной войне» как концептуальная основа противодействия «российской информационной угрозе»

Вне сомнений, украинский кризис 2013-2014 гг. дал основной толчок процессу конструирования и утверждения «российской информационной угрозы» в западном политическом дискурсе, причём не только как самостоятельного вызова или проблемы, а как составной части более широкого комплекса враждебных действий, направляемых единой стратегической линией.

⁷⁸ Clarke R. A. Cyber War: The Next Threat to National Security and What to Do About It / R. A. Clarke, R. K. Knake. – New York: HarperCollins Publishers, 2010. 304 p. (p. 21)

⁷⁹ Richards J. Cyber-War: The Anatomy of the Global Security Threat / J. Richards. Basingstoke: Palgrave Macmillan, 2014. 91 p. (p. 47)

Концептуальным обоснованием данного комплекса послужила теория «гибридной войны».

Ещё на раннем этапе украинского кризиса, в конце 2013 г., стало очевидно, что одним из его аспектов является столкновение различных интерпретаций происходящего в понимании внутренних и внешних игроков. Их несовместимость выступала ключевым препятствием на пути конструктивного взаимодействия в целях урегулирования кризиса, что показал, в частности, безрезультатный саммит Россия-ЕС 28 января 2014 г. По мере развития событий дистанция между позициями Москвы и западных столиц только увеличивалась, а после вооружённого переворота в Киеве 22 февраля 2014 г. вопрос интерпретации развернувшихся событий приобрёл не только сугубо пропагандистское, но политическое и правовое значение, так как был напрямую связан с оценкой их законности и легитимности. Дальнейшие процессы – присоединение Крыма к России и русское восстание на Донбассе – только усугубили данную проблему и поставили перед их участниками задачу обоснования как собственных действий, так и ответных действий своих контрагентов в выгодном для себя свете, а также конструирования желаемого информационного фона для продвижения своих политических целей.

Задача нового руководства Украины и наиболее антироссийской части западного истеблишмента в этот период заключалась в формировании такого нарратива, в котором любое сопротивление их курсу, как в практической плоскости, так и в информационном пространстве, можно было представить как целенаправленную, спланированную и осознанную войну России против Украины. Также для получения поддержки западных институтов и предотвращения выработки компромисса между Западом и Россией, необходимо было максимально гипертрофировать угрозу подобной войны для других государств, в том числе, и членов НАТО.

Решению этой задачи и служил дискурс о развязывании Россией «гибридной войны» против Запада, введение которого в публичное пространство происходило в апреле-мае 2014 г. С одной стороны, он формировал

научнообразное теоретическое обоснование продвигаемого упомянутыми силами нарратива о «российской агрессии», который противопоставлялся российскому нарративу о «гражданской войне» и «внутриукраинскому конфликту», а с другой, предоставлял аргументы для преодоления тех правовых противоречий, которые возникали вследствие вооружённого переворота в Киеве и дальнейших действий нового украинского руководства.

Термин «гибридная война» возник в недрах американской военно-стратегической мысли во второй половине 2000-х годов в контексте изучения нетрадиционных асимметричных конфликтов и изменения характера войн в современную эпоху⁸⁰. Он разрабатывался применительно к двум проблемам оперативно-тактического характера – комбинированному характеру угроз, исходящих от потенциальных противников в асимметричных конфликтах, и выработке адекватной тактики и потенциала для нейтрализации подобных угроз. Собственно, категория гибридности в этих разработках относилась к различным элементам стратегического ландшафта: а) сочетанию регулярных и иррегулярных методов ведения войны более слабыми противниками США, которые, тем не менее, могли наносить ощутимый ущерб американской армии, используя её оперативные и психологические уязвимости; б) задействованию оперативных инструментов одновременно в различных военно-стратегических измерениях (политическом, инфраструктурном, экономическом, информационном, социально-психологическом, энергетическом, и в киберпространстве); в) комбинированию военных и гражданских ресурсов для урегулирования кризисов и постконфликтной стабилизации, требующей не только обеспечения физической безопасности территории, но и идеологической обработки местного населения⁸¹. Первоначальный концепт «гибридной войны»

⁸⁰ Цыганков П. А. «Гибридные войны» в XXI веке: социальные и политические аспекты / П. А. Цыганков // Вестн. Моск. ун-та. Сер. 18. Социология и политология. – 2015. – № 4. – С. 253-258; Белозеров В. К. Гибридная война в отечественном политическом и научном дискурсе / В. К. Белозеров, А. В. Соловьев // Власть. – 2015. – № 9. – С. 5-11. URL: http://www.isras.ru/files/File/Vlast/2015/2015_9/Belozerov.pdf (дата обращения: 11.11.2020)

⁸¹ Подробнее о генеалогии понятия «гибридная война» см. нашу статью Царик В. С. Конструирование «гибридной войны» в западном информационном пространстве: основные стадии и субъекты // Вестник РГГУ. Серия «Политология. История. Международные отношения». 2020. № 3. С. 20-34., а также Конышев В. Гибридные войны: между мифом и реальностью / В. Конышев, Р. Парфенов // Мировая экономика и международные отношения. 2019. Том 63, № 12. С. 56-59.

разрабатывался для описания оперативно-тактической специфики реальных боевых действий, усиливающим дополнением которых могло стать информационное противостояние, но информационный компонент никогда не рассматривался в нём в качестве самостоятельного, действующего в отрыве от реальных боевых действий в рамках «обычного» политического противоборства⁸².

По мере разработки данной тематики исследователи указывали на возможность использования «гибридных» методов в конкуренции между великими державами, особенно в контексте перехода к многополярному миру⁸³, но способность России или какого-либо иного государства выступать в качестве «гибридного» противника серьёзно не анализировалась. Наоборот, некоторые учёные указывали на то, что Россия сама стала объектом применения «гибридных» методов в ходе обеих Чеченских войн⁸⁴.

Приписывание России инновационных военно-стратегических подходов обозначилось в ходе осмысления западными аналитиками опыта операции по присоединению Крыма весной 2014 г.

Первое обстоятельное упоминание «войн нового поколения» в контексте украинских событий встречается, по нашим данным, в работе латышского аналитика Я. Берзиньша, опубликованной 25 апреля 2014 г.⁸⁵. Ссылаясь на выступление начальника Генерального штаба РФ В. Герасимова в феврале 2013 г.⁸⁶, в котором было сказано о применяемых Западом невоенных методах дестабилизации других стран, Я. Берзиньш говорит, что современное российское понимание стратегии основано на большой роли информационной и психологической войны, которая позволяет усилить превосходство через

⁸² Fridman O. Russian "Hybrid Warfare": Resurgence and Politicization. Oxford: Oxford University Press, 2018.

⁸³ De Wijk R. Hybrid Conflict and the Changing Nature of Actors // The Oxford Handbook of War / Y. Boyer, J. Lindley-French (eds.) // Oxford: Oxford University Press, 2012. P. 359-373.

⁸⁴ Nemeth W. J. Future war and Chechnya : a case for hybrid warfare / W. J. Nemeth // Naval Postgraduate School, Monterey, CA. June 2002. 88 p. URL: <https://calhoun.nps.edu/handle/10945/5865> (дата обращения: 11.11.2020)

⁸⁵ Bērziņš J. Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy/ Bērziņš J.// Policy Paper, 2014, No 02. April, p. 1-13.

⁸⁶ Герасимов В. Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий / В. Герасимов // Военно-промышленный курьер. 26 февраля 2013. URL: <http://www.vpk-news.ru/articles/14632> (дата обращения: 11.11.2020)

морально-психологическое подавление вооружённых сил и гражданского населения противника. Это позволит минимизировать использование собственных вооружённых сил, прибегая к поддержке военных и гражданских лиц атакуемой страны, которые должны выступить против своей собственной страны и правительства. Война становится перманентной, без чётко выделенного начала и конца, со стороны России она направлена, по мысли Я. Берзиньша, против западной цивилизации, западных ценностей, культуры, политической системы и идеологии⁸⁷. Далее, ссылаясь на статью российских экспертов С. Чекинова и С. Богданова 2013 г.⁸⁸, автор приводит восемь стадий военного конфликта, согласно российскому их пониманию, где вслед за расшатыванием политической и экономической системы неизбежно следуют установление бесполётной зоны, широкомасштабные подрывные мероприятия во всех возможных сферах, целенаправленные авиационные операции с использованием высокоточного оружия и, наконец, выведение из строя оставшихся узлов сопротивления противника, десантные операции и т. д. В конце работы Берзиньш говорит, что те же методы Россия может использовать и в Латвии.

На следующий день, 26 апреля 2014 г., Радио Свобода разместило интервью отставного генерала Франка Ван Каппена⁸⁹, члена верхней палаты парламента Нидерландов. В нём прямо используется термин «гибридная война», но акцент сделан на применении Россией незаконных вооружённых групп на территории Украины вместо открытого применения армии, а также высказывается опасение, что аналогичные методы В. Путин может использовать для завоевания членов НАТО без открытого введения войск, например, сформировав «Нарвскую народную республику».

Это интервью только на русском языке было перепечатано более сотни раз в различных СМИ и блогах, и термин тут же вошёл в широкий оборот. Так, 30

⁸⁷ Там же, С. 5.

⁸⁸ Чекинов С. Г. О характере и содержании войны нового поколения / С. Г. Чекинов, С. А. Богданов // Военная мысль. 2013. № 10. С. 13-24.

⁸⁹ Корниенко С. Пиджак рвётся по шву / С. Корниенко // Радио Свобода. 26.04.2014. URL: <https://www.svoboda.org/a/25362031.html> (дата обращения: 11.11.2020)

апреля 2014 г. тезис о ведомой против Украины гибридной войне подхватывает отставной генерал СБУ А. Скипальский⁹⁰. И уже 13 мая 2014 г. польский публицист Л. Вуйчик⁹¹, соединив подходы Я. Берзиньша и Ф. Ван Каппена, изложил в качестве российской методики «гибридной войны» не только использование «прокси-сил» (местных агентов влияния, не принадлежащих формально к Вооружённым силам или спецслужбам РФ, но действующих в направлении, продиктованном руководством РФ), но и широкий спектр операций из статьи Я. Берзиньша. Вслед за этим, 22 мая 2014 г. выходит весьма ангажированная статья польской исследовательницы И. Даржевской об информационной войне, которую РФ вела против Украины в ходе крымской операции, об используемых нашей страной идеологемах и культивируемых программах⁹².

По мере распространения дискурса о «гибридной войне» в академической среде он подхватывается политическими деятелями и официальными лицами Украины. 20 мая 2014 г. заявление о ведении Россией гибридной войны в интервью изданию *Financial Times* сделал и. о. секретаря СНБО Украины А. Парубий⁹³. А 14 июня 2014 г. об этом заявил глава СБУ В. Наливайченко (в т. ч. упомянув, что именно православие используется Россией в «гибридной войне» против Украины)⁹⁴.

⁹⁰ Экс-генерал СБУ рассказал о «гибридной войне» и украинских олигархах // РИА. 30.04.2014. URL: <https://ria.ru/world/20140430/1006101683.html#ixzz30QtUV51P> (дата обращения: 11.11.2020); В Украине происходит полноценная война XXI века, "гибридная" война – Скипальский // 24 канал. 30.04.2014 URL: https://24tv.ua/ru/v_ukraine_proishodit_polnotsennaya_voyna_xxi_veka_gibridnaya_voyna_skipalskiy_n437989 (дата обращения: 11.11.2020)

⁹¹ Вуйчик Л. (Łukasz Wójcik). Украинская гибридная война / Л. Вуйчик // Иносми. 15.05.2014. URL: <https://inosmi.ru/sngbaltia/20140515/220303215.html> (дата обращения: 11.11.2020) [Оригинал: Wójcik L. Ukraińska wojna hybrydowa / L. Wójcik // Polityka. 13.05.2014. <https://www.polityka.pl/tygodnikpolityka/swiat/1579805,1,ukrainska-wojna-hybrydowa.read> (дата обращения: 11.11.2020)]

⁹² Darczewska J. The Anatomy of Russian Information Warfare. The Crimean Operation, a Case Study / J. Darczewska // OSW Point of View Number 42. May 2014. URL: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf (дата обращения: 11.11.2020)

⁹³ Parubiy says Russia's 'hybrid war' against Ukraine shows need to reform defense sector, NATO ready to help // Kyiv Post. 20.05.2014. URL: <https://www.kyivpost.com/article/content/war-against-ukraine/parubiy-says-russias-hybrid-war-against-ukraine-shows-need-to-reform-defense-sector-nato-ready-to-help-348538.html?cn-reloaded=1> (дата обращения: 1.07.2020)

⁹⁴ Nalyvaichenko: Russia making 'hybrid war' against Ukraine // Kyiv Post. 14.07.2014. URL: <https://www.kyivpost.com/article/content/war-against-ukraine/nalyvaichenko-russia-making-hybrid-war-against-ukraine-351866.html> (дата обращения: 1.07.2020); Православие объявлено главной угрозой для Украины // Е-

Из данного обзора становится понятно, что применение теоретической концепции «гибридной войны» к действиям России было формой интерпретации роли вооружённых формирований без опознавательных знаков пророссийской направленности в Крыму и на Донбассе, с одной стороны, и значения информационных методов воздействия, с другой. Слияние трёх компонентов – конвенционального конфликта, иррегулярных методов сопротивления и информационно-пропагандистского воздействия – в едином понятии с ключевым семантическим и смысловым маркером «война» и заложило основу данного дискурса, обусловив ряд его концептуальных инноваций⁹⁵.

Во-первых, формулирующие его авторы во многом абстрагируются от существующих теоретических наработок по этой теме и основывают свои заключения на примере одних только событий в Крыму и на Донбассе, представляют их чуть ли не первым историческим примером «гибридной войны» и искусственно гиперболизируют их беспрецедентность и уникальность для современного мира. Между действиями России весной 2014 г. и термином «гибридная война» был поставлен смысловой знак равенства, а вопрос, насколько эти действия соответствуют ранее сформулированной теории, вообще не поднимался.

Во-вторых, дискурс о «гибридной войне» позволял произвести «огосударствление», «этатизацию» нетрадиционных угроз, ассоциируемых до этого преимущественно с негосударственными акторами, и спроецировать на них те же способы противодействия, которые применяются в случае противостояния между государствами. Соответственно, и сама «гибридная война» из формы асимметричного конфликта превратилась в форму межгосударственного противостояния, ведущегося без формального оглашения неявными, опосредствованными методами. То, что в работах американских военных стратегов рассматривалось как гипотетическая возможность, в статьях

News. 17.06.2014. URL: <https://e-news.su/info/14562-pravoslavie-obyavleno-glavnoy-ugrozoy-dlya-ukrainy.html> (дата обращения: 11.11.2020)

⁹⁵ Tsygankov A. P. Putin's "Global Hybrid War": U.S. Experts, Russia, and the Atlantic Council / A. P. Tsygankov, P. A. Tsygankov, H. Gonzales // Russia in Global Affairs. 2021. Vol. 19, No. 1. P. 153.

польских и прибалтийских аналитиков представлялось как политический факт. Тем самым априори нивелировалась не только субъектность тех структур, которые озвучивали позицию условно «антимайданной» части населения Украины, но и тех, которые могли поддерживать или сочувствовать этой позиции. Их политические цели отбрасывались как не имеющие значения, поскольку их действия якобы подчинены исключительно целям «гибридной войны» РФ против Запада⁹⁶.

В-третьих, благодаря подобному терминологическому слиянию происходила своего рода «милитаризация» «мягкой силы», превращение её из инструмента межгосударственной конкуренции в инструмент подрыва устойчивости противника, попросту говоря, в оружие⁹⁷, а, следовательно, – в прямую угрозу государственной безопасности, требующую соразмерных мер упреждения и противодействия. Разумеется, понятия информационной угрозы и информационной безопасности давно вошли в политический лексикон, о чём свидетельствует наличие собственной доктрины или стратегии информационной безопасности у многих государств, но введение в публичное пространство понятия «гибридной войны» значительно понижало «порог чувствительности» к подобным угрозам и, фактически, означало секьюритизацию информационного пространства.

В-четвёртых, в новом политическом контексте термин «гибридная война» обозначал уже не «кинетические действия» (этим термином западные авторы называют «обычные» передвижения войск и боевые столкновения), а попытки разрушить правительственные структуры и институты, ослабить национальное единство, в том числе, через применение фейковых новостных сообщений, кибератак и т. д. В новой трактовке «гибридная война» приобретала практически тотальный характер, охватывала все сферы общественной жизни и исходила из

⁹⁶ Котляр В. К вопросу о «гибридной войне» и о том, кто же ее ведет на Украине / В. Котляр // Международная жизнь. 2018. № 8. С. 57-72.

⁹⁷ Dayspring S. M. Countering Russian Hybrid Warfare: Acknowledging the Character of Modern Conflict / S. M. Dayspring // Countering Hybrid Warfare: the Best Uses of SOF in a Pre-Article V Scenario. Ed. Michael Freeman et al. CTX | Vol. 6, No. 4. Special Issue. P. 20.

задействования в ходе подрывных операций широкого круга средств и акторов, не имеющих прямой правовой связи с государством-противником.

При этом термину «гибридная война» намеренно придавалась эмоционально негативная коннотация как феномену, носящему безнравственный, противозаконный, вероломный характер, присущему исключительно «недемократичным режимам» и не соотносимому с действиями «нормальных» стран⁹⁸. Как указывает В.Н. Порывкин, *«по своей сути «гибридная война», как явление международной жизни, в отличие от войны «классической», стало восприниматься, прежде всего, как война «бесчестная», безнравственная, «подлая», «из-за угла», вне исторически и юридически установленных ранее норм и правил ведения войны»*⁹⁹.

Как верно подметил С. Клименко¹⁰⁰, *«термин "гибридная война" (операция) никогда не будет применен Североатлантическим союзом по отношению к действиям Запада, даже если бы по их содержанию и направленности они полностью совпадали с российскими мероприятиями в Крыму. Свои операции и миссии альянс всегда рассматривает как законные и соответствующие морально-этическим нормам. И наоборот, теперь любые активные действия России на постсоветском пространстве будут подпадать под раскручиваемое Западом понятие "гибридная операция"»*.

Подобная негативная коннотация не только формировала соответствующее психоэмоциональное восприятие феномена у целевой аудитории, но и делала допустимым применение в отношении противника по «гибридной войне» инструментов, выходящих за рамки общепринятого военно-политического инструментария.

В концептуальном отношении итогом подобной интерпретации категории «гибридной войны» стали множественное расширение оперативно-

⁹⁸ Арчаков В. Ю. Информационный фактор в гибридных войнах / В. Ю. Арчаков, В. Н. Пунченко, В. Е. Ременчик // Геополитика и безопасность, 2017, № 2 (38), С. 16-27.

⁹⁹ Порывкин В. Н. Классическая, «гибридная» и «холодная» война как понятия в мировой политике / В.Н. Порывкин // Современные тенденции развития науки и технологий. 2017. № 2-7. С. 85-89.

¹⁰⁰ Клименко С. Теория и практика ведения «Гибридных войн» (по взглядам НАТО) / С. Клименко // Зарубежное военное обозрение. 2015. № 5. С. 109-112.

стратегического поля конфликтных действий, включающее расширение круга реальных или потенциальных участников конфликта (вплоть до ликвидации разделения между комбатантами и некомбатантами), расширение сфер и театров оперативных действий и расширение диапазона допустимых к применению средств поражения противника. В значительной степени западное стратегическое мышление уже прошло подобную расширительную эволюцию в отношении конфликтных зон Ближнего Востока, где грань между воюющими сторонами и мирным населением подчас действительно размывается. Однако открытый перевод в подобное русло конкуренции с другой великой державой стал подлинной инновацией для современной мировой политики.

Также уже на ранней стадии в дискурс о «гибридной войне» закладывается ряд манипулятивных приёмов, соответствующих решаемым его авторами политическим задачам, на которых будет строиться его дальнейшее развитие и политическое использование.

Это касается, прежде всего, конструирования «недостающих» элементов политической мотивации и стратегического потенциала России, доказывающих наличие у российского руководства готовности и способности вести «гибридную войну» против Запада и либерального миропорядка. Для этого используются академические или публицистические работы российских авторов, обладающих официальным статусом или выступающих сугубо в личном качестве, отдельные тезисы которых или специфическая их интерпретация приводятся как обоснование политической воли Москвы к оказанию разрушительного влияния на западное сообщество с помощью «гибридных» методов.

Ключевым подобным элементом стала так называемая «доктрина Герасимова», олицетворяющая наличие у России не только агрессивных планов в отношении Запада, но и готовой стратегии их реализации. Уже в статье Я. Берзиньша и выступление В. Герасимова, и статья С. Чекинова и С. Богданова, в которых излагается западный подход к современным войнам, опробованный против Югославии, Ирака, Ливии и Сирии, преподносятся как изложение планов России против сопредельных стран. И если Я. Берзиньш не

утверждает этого прямо, исподволь подводя читателя к такому выводу рассуждениями о российском подходе к современным войнам, то в последовавших публикациях стратегия «гибридной войны» в описанном формате прямо называется «доктриной Герасимова» на основе единственного публичного выступления В. Герасимова за год до украинских событий, трактуемого как неоспоримое доказательство того, что Россия вынашивала агрессивные замыслы до начала кризиса. При таком подходе даже прямое указание в упомянутых первоисточниках, что в них рассматриваются стратегии, применённые странами НАТО против третьих стран, не принимаются во внимание. Как написал в своём блоге в июле 2014 г. один из ведущих протагонистов идеи «гибридной войны» и специалист по российским силовым структурам Марк Галеотти, *«ложно представляя Арабскую весну как результат скрытых западных операций, Герасимов получил возможность свободно высказаться о том, о чём он хотел поговорить: как Россия может подорвать и уничтожить другие государства без прямого, открытого и масштабного военного вмешательства»*¹⁰¹. Соответственно, последователь М. Галеотти из финского Института международных отношений изложил своё понимание сюжета: *«Галеотти утверждает, что, хотя Герасимов придерживался оборонительной риторики, ссылаясь на внешние угрозы и часто упоминая о необходимости защиты России от нового типа войны, которую Запад ведёт в арабском мире, на самом деле генерал, вероятно, имел в виду обратное, а именно что это тот тип войны, который должна вести Россия. Галеотти назвал этот подход «эзоповым», где оборона означает нападение, а отражение атаки на самом деле означает атаку»*¹⁰².

Примечательно, что весной 2018 г. М. Галеотти признал, что термин «доктрина Герасимова» появился с его подачи, но на самом деле наличие

¹⁰¹ Galeotti M. 'The 'Gerasimov doctrine' and Russian Non-Linear War'. / M. Galeotti. // In Moscow's shadows. 2014. 6 July. URL: <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/> (дата обращения: 11.11.2020)

¹⁰² Там же.

подобной «доктрины» не соответствует действительности¹⁰³. Тем не менее, отсутствие доктрины не отменяет, по его мнению, факта наличия у России описанных агрессивных намерений и планов.

Помимо выступления В. Герасимова, в качестве подобного доказательства приводится (правда, не так активно) рассказ ассоциируемого с помощником Президента Российской Федерации по вопросам социально-экономического сотрудничества с государствами СНГ, Абхазией и Южной Осетией В.Ю. Сурковым автора под псевдонимом Натан Дубовицкий «Без неба», опубликованный 12 марта 2014 г. Ссылаясь на то, что в нём используется термин «нелинейная война» с описанием характера ведения современных войн, лондонский журналист П. Померанцев в своей статье в начале мая утверждает, что рассказ Н. Дубовицкого излагает кремлёвский подход к нелинейной войне¹⁰⁴. В последующие годы целый ряд западных экспертов, повторяя установку П. Померанцева, ссылались на рассказ Н. Дубовицкого как провозвестник «гибридной войны», в то время как интересующие их обычно информационные аспекты этой войны в рассказе как раз не затрагивались.

Подобно мифу о «доктрине Герасимова», И. Даржевская использует публикации И. Панарина о методах проводимой Западом информационной кампании против России для утверждения читателя во мнении о планах России использовать эти методы против Запада, заодно вводя понятие «школа Панарина». После этого автор описывает «школу Дугина», в которой достаточно маргинальные для официальной России воззрения евразийцев и рассматриваемые ими сценарии сетецентрической войны, раздела Украины, «четвёртая политическая теория» интерпретируются как планы действующей власти, «доктрина Путина».

Летом 2014 г. продвижение дискурса о «гибридной войне» вышло на международный уровень. Избрание П.А. Порошенко Президентом Украины и

¹⁰³ Galeotti M. I'm Sorry for Creating the 'Gerasimov Doctrine' / M Galeotti // Foreign Policy. 2018. 5 March. URL: <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/> (дата обращения: 11.11.2020)

¹⁰⁴ Pomerantev P. How Putin Is Reinventing Warfare / P. Pomerantev // Foreign Policy. 2014, May 5. URL: <https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/> (дата обращения: 11.11.2020)

формирование нового, формально законного правительства усилило антироссийскую линию Киева и позволило вынести вопрос о «российской агрессии» на повестку дня ряда международных институтов. К тому же подготовка саммита НАТО в Уэльсе создала удобный контекст для возможной формализации данного дискурса и закрепления его в качестве элемента публичного позиционирования Альянса.

Однако основную роль в его продвижении продолжали играть негосударственные институты и представители экспертного сообщества. Так, 31 мая на заседании Парламентской ассамблеи НАТО с докладом о сути ведущейся Россией «гибридной войны» выступил сотрудник вашингтонского института Катона, экс-советник Президента РФ А. Илларионов¹⁰⁵.

Именно в его докладе был задан базовый, эталонный набор тезисов, которые в дальнейшем будут ассоциироваться с понятием «гибридная война»:

- 1) события на Украине – это не проблема одной только Украины, а задел для войны России против всего остального мира;
- 2) происходящее страшнее холодной войны, потому что включает аннексию территорий;
- 3) это не новое и не уникальное явление: такая же агрессия уже проводилась Россией против Грузии в 2008 г.;
- 4) эта политика продолжает методы, использованные Россией в Абхазии, Южной Осетии и Приднестровье в 90-е годы, а также СССР против Прибалтики в 1940 г., а затем использованные в Северной Корее и на Кубе;
- 5) В.В. Путин запустил войну против Украины, потому что к лету 2013 г. прозападные силы в ней политически победили «проевразийские», «просоветские»;
- 6) война готовилась Россией, её властями, идеологами и спецслужбами многие годы;

¹⁰⁵ Illarionov A. Speech by Mr. Andrei Illarionov at NATO Parliamentary Assembly. Committee on Economics and Security. 31 May 2014 / A. Illarionov // Livejournal.com. 11 июня 2014. URL: <https://aillarionov.livejournal.com/696630.html> (дата обращения: 11.11.2020).

7) кампания России на Украине преследует цели на нескольких уровнях. Это переход Украины под контроль Путина или её разрушение. Это становление «Русского мира», в который могут быть включены любые соотечественники не только русского происхождения, но и потомки жителей СССР и Российской империи. Это подрыв западного альянса – разрушение англосаксонского мира и его верных антироссийских союзников (Прибалтики и Польши) и нейтрализация либо превращение в союзников остального Запада;

8) война имеет неконвенциональный характер и включает использование разведки, контрразведки, информации/дезинформации и пропаганды, кибератак, спецназа, негосударственных исполнителей (включая криминал, религиозные организации), подрывных акций, террористических атак с использованием женщин и детей как живых щитов, энергетических ограничений, экономического давления, коррупции, «пятой колонны» и, наконец, «Путининтерна» – политиков и политических партий по всему миру, поддерживаемых Путиным и поддерживающих Путина. В этой войне не будет линии фронта – она будет вестись против каждой страны;

9) необходимо принять стратегию противодействия России, в первую очередь, понять, что идёт настоящая война, затеянная агрессивнейшим режимом, и для запуска стратегии нужно принять решения по образцу «14 пунктов» Вудро Вильсона, Атлантической хартии, Фултонской речи Черчилля и т. д.;

10) надо принять меры военного, пропагандистского, международно-юридического, политического характера.

Ключевыми новациями дискурса о «гибридной войне» на этой стадии стали, во-первых, его ретроспективная проекция на политику Москвы в постбиполярный и биполярный период, призванная доказать имманентность мышления в духе «гибридной войны» для российского руководства, а, во-вторых, построение образа России как извечного стратегического врага (а не ситуативного конкурента и партнёра) Запада, чьи намерения неизменно были и

остаются враждебными вне зависимости от тех или иных кооперативных инициатив или шагов. Причинами такой имманентной враждебности России назывались особенности её геополитического положения, характер политического режима или качества русской идентичности и социокультурных черт русского народа.

Тот факт, что подобные тезисы были озвучены человеком, имевшим в прошлом прямое отношение к российским властным структурам, несомненно, добавляло им правдоподобности в глазах западной аудитории. Трибуна Парламентской ассамблеи НАТО позволяла делать заявления лицам, не имеющим официального статуса, но была достаточно представительной для того, чтобы сделанные на ней заявления получили медийную огласку.

В этот же период упоминание «гибридных методов войны» начинает появляться в лексиконе официальных лиц стран Западной Европы. Так, этот термин был употреблён Федеральным министром иностранных дел Германии Ф.-В. Штайнмайером в правительственном отчёте о состоянии дел в сфере контроля над вооружениями в контексте необходимости адаптации действующей системы ограничения обычных вооружений в Европе с учётом «гибридных методов войны»¹⁰⁶, а вскоре был подхвачен немецкими СМИ¹⁰⁷.

Поворотным моментом в продвижении дискурса о «гибридной войне» на международном уровне стало размещение на сайте «Вестника НАТО» 1 июля 2014 г. двух видеоматериалов по данной тематике, представленных как собрание высказываний независимых экспертов, однако в идейном плане их тезисы повторяют выступления А. Илларионова и И. Даржевской в более политкорректном формате. В одном из них¹⁰⁸ утверждалось, что уже кризисы в Эстонии 2007 г. и Грузии 2008 г. указывали на агрессивные планы России в

¹⁰⁶ Steinmeier F.-W. « Grußwort des Bundesministers des Auswärtigen », dans Auswärtiges Amt (Hrsg.) / F.-W. Steinmeier. – Jahresabrüstungsbericht 2014, Berlin, 2014, p. I. URL: <http://docplayer.org/77468928-Jahresabruestungsbericht-2014.html> (дата обращения: 11.11.2020)

¹⁰⁷ Barbin J. La guerre hybride : un concept stratégique flou aux conséquences politiques réelles / J. Barbin // Les Champs de Mars 2018/1 (N° 30 + Supplément), p. 109-116. URL : <https://www.cairn.info/revue-les-champs-de-mars-2018-1-page-109.htm> (дата обращения: 11.11.2020)

¹⁰⁸ Россия, Украина и Крым: предсказуемый кризис? // Вестник НАТО. 1.07.2014. URL: <https://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-Crimea-crisis/RU/index.htm> (дата обращения: 11.11.2020)

отношении Крыма, в другом¹⁰⁹ – что Россия вторгается по всему миру, навязывает свою волю, аннексирует территории, переигрывает НАТО, ведёт информационную войну с помощью канала *Russia Today*, комбинирует медленное и быстрое продвижение, информационные атаки, использует русские традиции ведения войны и не собирается ограничиваться Украиной. Особенно важно признать, говорилось в роликах, что Россия ведёт войну в империалистических целях, и организовать противодействие НАТО. Ключевая идея противодействия, сформулированная бывшим послом США при НАТО и будущим спецпредставителем США по Украине Куртом Волкером, состоит в максимально «сильном ответе» для того, чтобы Россия не попыталась идти дальше, стабилизировать ситуацию в «подвешенном» состоянии, а затем – добиться «деэскалации» (под которой, по всей видимости, имеется в виду отказ России от заявленных переговорных позиций).

Проанализировав содержание видеоматериалов с помощью методов символического конструктивизма и дискурсивного анализа, российский исследователь А.М. Сосновская показала¹¹⁰, что они носили тенденциозный и пропагандистский характер и были направлены на то, чтобы внушить аудитории страх перед «гибридной угрозой» со стороны РФ.

Неделю спустя, 8 июля 2014 г., выступая перед журналистами после встречи с Президентом США Бараком Обамой, Генеральный секретарь НАТО Андрес Фог Расмуссен заявил¹¹¹, что Россия ведёт против Украины «гибридную войну», сочетая прямые военные действия, скрытые операции и агрессивную программу дезинформации в расчёте на то, чтобы ослабить новое украинское Правительство и сохранить под своим контролем восточную часть страны.

¹⁰⁹ Гибридная война – гибридная ответная реакция // Вестник НАТО. 1.07.2014. URL: <https://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/RU/index.htm> (дата обращения: 11.11.2020)

¹¹⁰ Сосновская А.М. Идеология и массовые коммуникации: гибридная война на Украине / А.М. Сосновская // Научные труды Северо-Западного Института управления РАНХиГС. СПб 2016. Том 7. Выпуск 3 (25). С. 134-142. URL: https://spb.ranepa.ru/images/nauka/NT/NT_7_3.pdf (дата обращения: 11.11.2020)

¹¹¹ Landler M. NATO Chief Warns of Duplicity by Putin on Ukraine / M. Landler, M. Gordon // The New York Times. 2014. 8 July. URL: https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html?_r=0 (дата обращения: 11.11.2020)

Оставшиеся до саммита НАТО в Уэльсе 3-4 сентября 2014 г. два месяца были использованы органами Альянса для подготовки почвы к принятию официальных резолюций антироссийской направленности. Заметную публичную роль в курировании их «теоретического обоснования» сыграл бывший командующий силами НАТО в Европе генерал Ф. Бридлав. Так, в интервью изданию *die Welt* в середине августа¹¹² генерал заявил о широком использовании «гибридных войн», в которых используются все возможные дипломатические, информационные, военные и экономические средства. По его словам, если на дипломатическом уровне Россия осуждает действия киевских властей, то в СМИ одновременно ведется кампания по дезинформации и сокрытию российских преступлений, на военном фронте используется весь доступный арсенал, идут перемещения войск, ведутся артиллерийские обстрелы через границу, наконец, оказывается экономическое давление путем ограничения поставок энергоресурсов. Ф. Бридлав указал, что нужно подготовить полицию и армию стран Восточной Европы для противодействия возможному появлению там «зелёных человечков» – вооружённых солдат без опознавательных знаков, которые занимают правительственные здания, обучают «сепаратистов», подстрекают местное население к бунту и таким образом способствует дестабилизации в регионе. В случае же проникновения на территорию НАТО [опознанных] иностранных военных, что будет являться актом агрессии, вступит в действие 5-я статья устава НАТО, в соответствии с которой нападение на одну или несколько стран Европы или Северной Америки рассматривается как нападение на них в целом, и тогда НАТО даст военный ответ на агрессию.

В тот же день, 17 августа 2014 г., в издании *The Wall Street Journal* вышла совместная статья генерала Ф. Бридлава и генсека Альянса Андерса Фог

¹¹² Bolzen S. “Die Nato muss auf grüne Männchen vorbereitet sein”. Interview mit Nato-Oberbefehlshaber Philip Breedlove / Bolzen S. // Die Welt. 2014. 17 August. URL: <https://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.html> (дата обращения: 11.11.2020)

Расмуссена «НАТО для опасного мира»¹¹³, в которой говорилось: *«Мы продолжаем призывать Россию незамедлительно сделать ответственный выбор: вывести войска, прекратить использование тактики гибридной войны, искать политическое решение кризиса вместе с международным сообществом и украинским правительством».*

Благодаря проведённой подготовке, на сентябрьском саммите в Уэльсе тематика гибридных угроз была не только официально вынесена на повестку дня, но и получила формальное закрепление как предмет ведения Альянса: было принято решение о наделении его инструментами для сдерживания и купирования гибридных угроз. Так, в п. 13 принятой на этом саммите декларации говорилось: *«Мы сделаем так, чтобы НАТО была способна эффективно преодолевать конкретные вызовы, возникающие в связи с угрозами гибридной войны, при ведении которой применяется широкий ряд тесно взаимосвязанных открытых и скрытых военных, военизированных и гражданских мер. Принципиально важно, чтобы у Североатлантического союза были инструменты и процедуры, необходимые для эффективного сдерживания угроз гибридной войны и реагирования на них, а также потенциалы для усиления войск (сил) государств. Сюда также входит усиление стратегических коммуникаций, разработка сценариев учений в свете гибридных угроз и укрепление координации между НАТО и другими организациями в соответствии с принятыми решениями, с тем, чтобы улучшить обмен информацией, политические консультации и координацию на уровне секретариатов (штабов). Мы приветствуем создание в Латвии аккредитованного НАТО Центра передового опыта по стратегическим коммуникациям, который является значительным вкладом в усилия НАТО в*

¹¹³ Rasmussen A. F., Breedlove Ph. A NATO for a Dangerous World. Russian aggression has made it clear. We need an alliance that is fitter, faster and more flexible / A. F. Rasmussen, Ph. Breedlove // Wall Street Journal. 2014. 17 August. URL: <https://www.atlanticcouncil.org/blogs/natosource/a-nato-for-a-dangerous-world> (дата обращения: 11.11.2020)

данной области. Мы поручили вести обзор работы по гибридной войне, наряду с осуществлением Плана действий по обеспечению готовности»¹¹⁴.

Как можно увидеть, в декларации НАТО уже не только констатировался факт наличия «гибридных угроз», но также фиксировались политические обязательства Альянса по борьбе с ними, и устанавливался первичный институциональный механизм, призванный выполнять базовые функции в этой сфере. Также на прошедшем вскоре после саммита совещании начальников штабов стран-членов НАТО в Вильнюсе Ф. Бридлав упомянул сугубо военные меры в ответ на российскую тактику гибридной войны¹¹⁵.

Таким образом, Североатлантический альянс выступил в роли главной движущей силы в процессе формализации и институционализации дискурса о «гибридной войне» летом 2014 г. Инициировав обсуждение этой темы сначала на Парламентской ассамблее НАТО, затем выпустив серию агитационных материалов и, наконец, включив соответствующий пункт в итоговую декларацию саммита в Уэльсе, Альянс не только ввёл данный термин в международно-политический оборот, но и наложил на своих членов базовые политические обязательства по совместному противодействию «гибридным угрозам». В дальнейшем именно под эгидой НАТО проводились наиболее масштабные исследования и презентационные мероприятия по теме «гибридной войны», задававшие магистральный вектор развития данного дискурса.

Легитимизировав «гибридную войну» как элемент якобы объективной политической реальности, саммит НАТО в Уэльсе дал толчок дальнейшему развитию данного концепта в двух плоскостях – официального государственного и международного дискурса, с одной стороны, и академической мысли и аналитической экспертизы, с другой. Вектор процесса при этом оставался единым: внедрение «гибридной войны» и «гибридных угроз» в политическое

¹¹⁴ Заявление по итогам встречи на высшем уровне в Уэльсе, обнародовано главами государств и правительств, участвующими в заседании Североатлантического союза в Уэльсе. – 4-5 сентября 2014 г. // НАТО. URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=ru (дата обращения: 11.11.2020)

¹¹⁵ Генерал Бридлав: План НАТО в Восточной Европе // Радио «Голос Америки». 2014. 15 сентября. URL: <https://www.golos-ameriki.ru/a/2450747.html> (дата обращения: 11.11.2020)

мышление государственных элит и общественное сознание западных стран в качестве ординарного, нормативно признанного феномена, имеющего как свои теоретические особенности и модели, так и неоспоримые практические проявления в современной мировой политике, которые требуют конкретных стратегических и оперативных мер противодействия. Кроме того, термин «гибридная война» превращался в общую, рамочную характеристику нынешнего этапа отношений Запада и Россией в целом, как в своё время термин «холодная война» стал рамочным для биполярного периода.

Экспертно-академический и политический уровни работали на усиление друг друга: увеличение количества научных и экспертных публикаций, исследующих феномен «гибридной войны» позволяло политическим деятелям использовать его как академически обоснованный и научно признанный концепт, а не пропагандистский конструкт, тогда как всё более широкое распространение этого термина в политическом лексиконе государств и международных организаций создавало потребность в его академическом осмыслении и изучении. Тем более, что подобное осмысление происходило на разных аналитических уровнях: на уровне политической науки в более абстрактном теоретическом ключе, на уровне военной науки в более прикладном, оперативном аспекте, на уровне аналитических разработок различных экспертных структур, на уровне тематических исследований различных государственных и межгосударственных органов. Нередко эти уровни переплетаются между собой, когда официальные органы заказывают соответствующие исследования аналитическим организациям и подкрепляют их выводы своим политическим авторитетом.

Массив изданных с 2014 г. публикаций по «гибридной войне» насчитывает несколько сотен работ. Подавляющее большинство из них, включая статьи в рецензируемых академических изданиях, излагают один и тот же круг идей с вариацией в деталях. Ведение Россией «гибридной войны», согласно этим текстам, опирается как на советскую военную практику, так и на традицию русского стратегического мышления, берущую своё начало чуть ли не во

временах Ивана Грозного¹¹⁶. К традиционной российской практике «гибридной войны» относят события вокруг «Бронзовой ночи» в 2007 г. в Эстонии, а в советский период – вторжение в Афганистан и даже мирные протесты движения «Единство» в Литве против выхода из СССР в 1990 г.¹¹⁷ и др.

Некоторая часть работ критикует использование термина «гибридная война», но только ради того, чтобы подменить его сходным термином, например, «составной войной», «диффузной войной» при сохранении общепринятого содержания данной концепции¹¹⁸. Другие статьи, напротив, привязывают действия РФ к ранее разработанной общей теории «гибридной войны» и воспроизводят с незначительными вариациями список основных её признаков¹¹⁹.

В наиболее ёмкой форме эти представления изложены в сборнике «Ответ НАТО на гибридные угрозы» с предисловием генерала Ф. Бридлава: *«Российские военные действия в украинском кризисе отражают сложный, комплексный, многовариантный подход к применению силы для достижения решающих политических целей. Российские военные стратеги и планировщики*

¹¹⁶ Thiele R. D. Hybrid Threats – And how to counter them / R. D. Thiele // ISPSW Strategy Series: Focus on Defense and International Security. Issue No. 448. Sep. 2016. URL: https://www.ispsw.com/wp-content/uploads/2016/09/448_Thiele_Oslo.pdf (дата обращения: 11.11.2020); Sherr J. The Challenge of “Hybrid War” / J. Sherr // National Security and Defense. No. 9-10 (167-168). – Kiev: Razumkov Centre, 2016. P. 85-86. URL: http://razumkov.org.ua/uploads/journal/eng/NSD167-168_2016_eng.pdf (дата обращения: 11.11.2020); Hybrid Threats and Asymmetric Warfare: What to do? Stockholm 14-15 November, 2017 at the Swedish Defence University, Stockholm, Sweden. Conference proceeding, February 2018. Ed. Karl Hickman et al. URL: https://www.researchgate.net/publication/332224423_Hybrid_Threats_and_Asymmetric_Warfare_What_to_do_Conference_proceeding (дата обращения: 11.11.2020); Johnson R. Hybrid War and Its Countermeasures: A Critique of the Literature / R. Johnson // Small Wars & Insurgencies. 2018. Vol. 29, No. 1. P. 141-163; Kilinskas K. Hybrid Warfare: an Orientating or Misleading Concept in Analysing Russia’s Military Actions in Ukraine? / K. Kilinskas // Lithuanian annual strategic review. 2015-2016. Vol. 14. P. 139-159; Rácz A. Russia’s Hybrid War in Ukraine. Breaking the Enemy’s Ability to Resist / A. Rácz // The Finnish Institute of International Affairs. 2017. – 208 p.

¹¹⁷ Countering Hybrid Warfare: the Best Uses of SOF in a Pre-Article V Scenario // M. Freeman et al. (Eds.) // CTX. Vol. 6, No. 4. Special Issue. P. 9

¹¹⁸ Minasyan S. “Hybrid” vs. “Compound” War. Lessons from the Ukraine conflict // PONAS Eurasia policy memo. November 2015. No. 401. URL: https://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/Pepm401_Minasyan_Nov2015.pdf (дата обращения: 11.11.2020); Renz B. Russia and ‘hybrid warfare’ / B. Renz // Contemporary Politics. 2016. Vol. 22, Issue 3: Russia, the West, and the Ukraine Crisis. P. 283-300.; Lanoszka A. Russian hybrid warfare and extended deterrence in eastern Europe / A. Lanoszka // International Affairs. 2016. Vol. 92, No. 1. P. 175-195.

¹¹⁹ Erol M. S. Hybrid Warfare Studies and Russia’s Example in Crimea / M. S. Erol, Ş. Oğuz // Akademik Bakış. Kış 2015. Cilt 9 Sayı 17. P. 261-277; Munteanu R., hybrid warfare – the new form of conflict at the beginning of the century / R. Munteanu // Strategic Impact. 2015. No. 3, P. 19-25; Wither J. K. Making Sense of Hybrid Warfare / J. K. Wither // Connections. Spring 2016. Vol. 15, No. 2. P. 73-87; Schnauffer T. A. II. Redefining Hybrid Warfare: Russia’s Non-linear War against the West / T. A. II. Schnauffer // Journal of Strategic Security. 2017. V. 10, No. 1. P. 17-31. URL: <http://scholarcommons.usf.edu/jss/vol10/iss1/3> (дата обращения: 11.11.2020); Rusnáková S. Russian New Art of Hybrid Warfare in Ukraine / S. Rusnáková // Slovak Journal of Political Sciences. 2017. Vol. 17, No. 3-4, p. 343-380; Veljovski G. The danger of “hybrid warfare” from a sophisticated adversary: the Russian “hybridity” in the Ukrainian conflict / G. Veljovski, N. Taneski, M. Dojchinovski // Defense & Security Analysis. 2017. Vol. 33, Issue 4. P. 292-307.

*взяли классические элементы советского и российского военного мышления, объединили их с инструментами, тактикой и возможностями XXI века и создали новые модели военных действий, адаптированные к стратегической ситуации в России»*¹²⁰.

Обилие публикаций позволило прочно инкорпорировать концепт «гибридной войны» в академический оборот, однако не способствовало кристаллизации его унифицированного аналитического наполнения и выработке чёткого самостоятельного оценочного инструмента на основе конкретных вводных данных. В значительной степени это объясняется политическим контекстом, в котором произошла популяризация термина «гибридная война» в западном общественном сознании и академической мысли: поскольку данный термин был позаимствован из военной науки для оценки и стигматизации политики России, его содержательное наполнение формировалось, отталкиваясь от одного конкретного эпизода современной международной политики, причём формировалось не с целью выработки нового качественного аналитического инструмента, применимого в других случаях и контекстах, а с целью конструирования псевдонаучного обоснования курса на конфронтацию с Россией. В результате вокруг данного концепта возник целый ряд дискуссионных вопросов и противоречий как сугубо теоретического характера, так и прикладного, а том числе, касательно трактовки конкретных действий РФ, которые далеко не всегда укладывались в сформированный конструкт.

Прежде всего, это касается вопроса о научной новизне самого понятия «гибридная война» и его соотношении с конвенциональными определениями войны и военных действий. Как военная, так и политическая наука уже давно выработали целый диапазон понятий, отражающих различные формы ведения международных конфликтов за рамками прямого применения военной силы, в том числе так называемые «войны серой зоны». Понятие «гибридной войны» в той интерпретации, в какой оно получило распространение в западном публично

¹²⁰ NATO's Response to Hybrid Treats. / G. Lasconjarias, J. A. Larsen (eds.). Rome: NATO Defense collodge, 2015. URL: https://www.files.ethz.ch/isn/195405/fp_24.pdf (дата обращения: 11.11.2020).

пространстве после 2014 г., мало что привносит в дополнение к уже существующим терминам и моделям¹²¹, поэтому у некоторых исследователей возникают сомнения относительно того, не является ли понятие «гибридной войны» избыточным, дублирующим уже оформившиеся и устоявшиеся в науке термины.

Кроме того, остаётся неясным, является ли «гибридная война» самостоятельным типом международного конфликта, заменяет ли она конвенциональное прямое военное столкновение, или же только предваряет его, готовя нужную почву для ввода войск на ту или иную территорию. Киевский исследователь Г. Почепцов считает, что *«реально это диффузная война по множеству направлений одновременно, в рамках которой мягкая сила принимает более серьёзный характер»*¹²². Строится она на создании замедленного реагирования противника, чтобы выиграть время и достичь поставленных целей без явного применения силы.

С другой стороны, в статье американских экспертов М. Кофмана и М. Рожански¹²³ отмечается, что ярлык «гибридной войны» просто навешан на разворачивавшиеся стадии украинского кризиса, а говорить о проработанной общей стратегической концепции гибридной войны не приходится хотя бы потому, что похожие методы не смогли бы сработать в других странах из-за принципиально других условий. На самом деле, имело место применение дипломатических, экономических, военных и информационных инструментов в соседней стране в связи с ощущением угрозы жизненно важным национальным интересам.

Парадоксально, но даже в некоторых работах, авторы которых критиковали теоретическое наполнение концепции «гибридной войны», чаще всего всё равно

¹²¹ Jordan J. Hybrid Warfare: A Catch-all Concept / J. Jordan // GESI Mosaic Blog. 2017. 17 October. URL: <https://global-strategy.org/hybrid-warfare-a-catch-all-concept/> (дата обращения: 11.11.2020)

¹²² Почепцов Г. Гибридная война в головах и на экране / Г. Почепцов // «Хвиля», 17.05.2018, URL: <http://hvylya.net/analytics/politics/gibridnaya-golova-v-golovah-i-na-ekrane.html> (дата обращения: 11.11.2020)

¹²³ Kofman M. A Closer look at Russia's "Hybrid War" / M. Kofman, M. Rojansky // Kennan Cable. April 2015. No. 7. URL: https://www.files.ethz.ch/isn/190090/5-KENNAN_CABLE-ROJANSKY_KOFMAN.pdf (дата обращения: 11.11.2020)

содержались те же самые практические выводы о необходимости жёсткого противостояния России. Так, в статье К. Пола¹²⁴ приводится следующая критика концепции гибридной войны: *«Во-первых, существует целый спектр различных состояний конфликта и конкуренции, не связанных с войной, и даже при их переходе в «войну» по-прежнему существует спектр вариаций в интенсивности, используемых способностях и видимости противника. Конкуренция и конфликт в этих диапазонах могут включать как обычные, так и нетрадиционные вооружённые силы, а также возможности всех элементов силы, включая (но не ограничиваясь) дипломатические, информационные, военные, экономические и правовые.*

Во-вторых, противники могут противоборствовать поэтапно или постепенно, ползучим образом или пробивая себе путь к успеху, в отложенном порядке или скрывая принадлежность, не доходя до пороговых уровней эскалации, создавая проблемы и дилеммы для другого конкурента».

Однако конечный вывод выглядит не менее радикально, чем у авторов концепции «гибридной войны» и призывает считать происходящее противостояние состоянием войны, выходящим за рамки «честного и дружественного соревнования мирного времени между странами» и, со своей стороны, отвечать России соответственно этому пониманию.

Основная идея изложенной К. Полом теории конфликтов серой зоны, состоящая в возможности применения соперничающими государствами всего спектра военных и невоенных мер, перекочевала в теорию «гибридных войн», но, несмотря на свою кажущуюся очевидность, это и наиболее слабый элемент западной концепции «гибридной войны»: фактически стандартные действия государства по отстаиванию своих интересов или даже без явно выраженного отстаивания своих интересов, чаще всего ненасильственные, произвольным образом объединяются по признаку якобы проводимой им «гибридной войны», но никакого объединяющего признака этих действий и даже стоящего за ними

¹²⁴ Paul C. Confessions of a Hybrid Warfare Skeptic / C. Paul // Small Wars Journal. 16 mar 2016. URL : <https://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic> (дата обращения: 11.11.2020)

мотива такое описание не содержит. Не приведено ни критериев отнесения любого действия к «гибридно-военному», ни критериев заведомого неподпадания этого действия под категорию «гибридно-военных». Не приведено ни уверенных признаков, позволяющих зафиксировать ведение кем-то гибридной войны против Запада, ни надёжного теста, который бы позволил констатировать состояние мира без «гибридной войны».

Неопределённость сущностного наполнения понятий, лежащих в основе концепции «гибридной войны», влечёт за собой и неопределённость целевых и результативных параметров. Многие протагонисты этого концепта так и не могут чётко сформулировать, какие именно конкретные оперативно-тактические цели преследует Россия, прибегая якобы к «гибридным» методам воздействия. Даже в «стратегических» статьях разбор действий России в рамках «гибридной войны» постоянно ограничивался используемыми ею методами, но не описывал конечных стратегических целей, если не считать таковыми самых общих выражений типа «навязать свою волю», «подорвать демократию» и т. д.

Пожалуй, наиболее подробная критика западной концепции ведомой РФ «гибридной войны» содержится в статье С. Чарапа¹²⁵. Так, анализируя действия РФ на востоке Украины, он замечает (с. 53-54), что своими спецоперациями Москва достигла только более скромной цели – сорвать установление контроля киевских путчистов над двумя регионами, где у неё была поддержка населения, общая граница, один язык, проникновение бизнеса и спецслужб. Но даже в этих условиях к июлю-августу восстание на Донбассе оказалось на грани полного разгрома, что заставило РФ отказаться от гибридных методов и скрытно послать в поддержку восставших регулярные войска. Повторение же крымского сценария в странах Прибалтики с установлением контроля над каким-либо регионом исключительно силами добровольцев и нерегулярных вооружённых формирований нереалистично ввиду наличия путей для быстрой переброски туда сил НАТО. И единственный шанс для РФ предотвратить такое развитие

¹²⁵ Charap S. The Ghost of Hybrid War / S. Charap // Survival. 2015. Vol. 57, No. 6. P. 51-58.

событий – открытое вторжение сухопутных сил с полномасштабным применением всей огневой мощи и быстрая оккупация Прибалтики, не оставляющая шансов для прибытия подкреплений НАТО. Наконец, разбирая утверждения, что РФ уже ведёт против Запада гибридную войну с помощью дипломатических, пропагандистских и других мер, автор отмечает, что поклонники этой идеи просто уравнивают тактику приобретения влияния с подрывными действиями, угрожающими национальной безопасности.

Другая аргументация в защиту российской позиции предложена О. Кемпфом¹²⁶, работа которого отстаивает тезис, что к стратегии «гибридных войн» перешли и США, и РФ, причём первым был Барак Обама, который вывел (полностью или частично) войска из Ирака и Афганистана, но продолжил влиять на происходящее там другими методами. При этом, если РФ пытается вести «гибридную войну» только в непосредственном приграничье, то США – по всему миру. С похожими посылами обращаются к западной аудитории представители академической мысли России. Так, в работе Э. Корыбко¹²⁷ обосновывается тезис, что, на самом деле, это Запад ведёт с Россией гибридную войну, а в монографии Д. Тренина¹²⁸ утверждается, что реальные притязания РФ на влияние и установление своих порядков ограничены ближним зарубежьем, и, тем самым, они никак не угрожают Западу.

Таким образом, ряд западных учёных ставит под сомнение правомерность описания действий России, якобы проводимых ею в рамках стратегии «гибридной войны», как военных (и поэтому преступных, подрывающих основы миропорядка), а также расходятся с представлением о возможности широкого применения этих методов в других регионах, отличных от СНГ (М. Кофман, О. Кемпф). Но отдельные голоса не влияют на оценку стратегической угрозы от РФ как таковой.

¹²⁶ Kempf O. L'indirection de la guerre ou le retour de la guerre limitée / O. Kempf // Politique étrangère. 2015. No. 4. P. 157-169.

¹²⁷ Korybko A. hybrid wars: the indirect adaptive approach to regime change / A. Korybko. Moscow: Peoples' Friendship University of Russia. 2015. 132 p.

¹²⁸ Trenin D. Should we fear Russia? / D. Trenin. Polity. 2016. 144 p.

К полемическим можно отнести статьи уже упомянутого М. Галеотти, который выдвинул немало аргументов для спора вокруг характера военно-политической стратегии России. Так, он признаёт, что и в самом деле, *«настоящая гибридная фаза конфликта длилась всего несколько месяцев и закончилась именно потому, что методы, эффективные в том, чтобы посеять хаос, не помогли с ним совладать»*¹²⁹ (и, следовательно, расхождение реальных действий России с «доктриной Герасимова» и сценарием С. Чекинова и С. Богданова не опровергает того, что она хотела поступить именно так). В другой своей работе¹³⁰ он описывает ограниченность военных возможностей России, подводя читателя к мысли, что именно это ограничение и страх перед военной мощью НАТО помешали РФ захватить Украину методом «жёсткой силы», а не отсутствие подобных намерений как таковых, однако имперские амбиции РФ всё равно очень велики.

Инициативные предложения по борьбе с «гибридной угрозой» находятся в ранге от сочетания военных и гражданских методов¹³¹ до запугивания РФ жёсткой реакцией НАТО¹³² и принятия возможными жертвами российской агрессии, например, республиками Балтии, новой доктрины о том, что констатировать гибридную войну и запускать соответствующее состояние можно будет на основе накопления фактов, которые по отдельности никак не означают состояния войны, поскольку относятся к гражданской и политической области¹³³.

Описанные противоречия делают весьма относительной аналитическую ценность концепта «гибридной войны», но не мешают использовать его в публичном пространстве для пропагандистских целей расширения и

¹²⁹ Galeotti M. Hybrid war or gibrindnaya voina? Getting Russia's non-linear military challenge right / M. Galeotti. Mayak Intelligence, 2016. P. 63.

¹³⁰ Galeotti M. Heavy metal diplomacy: Russia's political use of its military in Europe since 2014 / M. Galeotti // ECFR Policy Brief. 2016. No. 200. 12 p. URL: http://www.ecfr.eu/page/-/Heavy_Metal_Diplomacy_Final_2.pdf (дата обращения: 11.11.2020)

¹³¹ A Civil-Military Response to Hybrid Threats / E. Cusumano, M. Corbe (eds.). Palgrave Macmillan, 2018. 320 p.

¹³² Takacs D. Ukraine's deterrence failure: Lessons for the Baltic States / D. Takacs // Journal on Baltic Security. 2017. No. 3 (1). P. 1–10.

¹³³ Bou Nader Ph. The Baltic states should adopt the self-defence pinpricks doctrine: the “accumulation of events” threshold as a deterrent to Russian hybrid warfare / Ph. Bou Nader // Journal on Baltic Security. 2017. No. 3(1). P. 11–24

гиперболизации российской угрозы, предлагая и внедряя запредельные меры «сдерживания» России. Таким образом, концепт «гибридной войны» сам по себе превращается в мощное оружие пропаганды и опасный инструмент дестабилизации и повышения неопределённости в международной системе.

Отсутствие теоретической чёткости концепта «гибридной войны» позволяет его пропагандистам адаптировать концепт под кажущиеся наиболее насущными нужды. В результате постоянно меняется баланс между различными компонентами «гибридной агрессии»: если изначально основной упор делался на иррегулярные вооружённые формирования, а информационное влияние и пропаганда рассматривались как фактор одобрения этих действий, то с течением времени и ввиду отсутствия боевых действий на первый план выходит именно информационная составляющая в связке с другими политическими и функциональными факторами.

Необходимо отметить, что российский академический и публичный дискурс в отношении понятия «гибридной войны» также внёс определённый вклад в его практическое наполнение. Так, отдельные заявления либо действия некоторых официальных лиц, публичных фигур или представителей академической среды вполне укладывались в концепцию «русской гибридной агрессии», якобы ведущейся против всего Запада, укрепляя тем самым её мнимое соответствие действительности. Однако эти заявления и действия не отвечали когда-либо принятой государственными органами РФ стратегической линии на ведение геополитической конкуренции с Западом подобными средствами. Самое главное, русская внешняя политика до недавних пор не носила тотально ревизионистского характера, и тем более не руководствовалась целью подорвать либеральный миропорядок извне или изнутри. Британский исследователь Р. Саква не раз указывал на то, что ревизионизм присущ внешнеполитическому курсу нашей страны лишь в ограниченной мере и направлен на изменение принципов применения действующих универсальных международных норм, а не изменение или отказ от

этих норм как таковых¹³⁴. А российские учёные подчёркивали преобладающую в российском стратегическом мышлении тенденцию к сохранению статус-кво и «институциональному консерватизму»¹³⁵.

В российских политических и военных кругах термин «гибридная война» довольно быстро получил распространение в качестве полноценной научной категории, отражающей текущее состояние российско-западных отношений¹³⁶ или тенденции в развитии военного дела¹³⁷. Наиболее авторитетным было употребление данного термина начальником Генерального штаба Вооружённых сил РФ, генералом армии В. Герасимовым в своих статьях в 2016-2017 гг.¹³⁸, где «гибридная война» представлялась передовой формой межгосударственных противостояний современности, хотя, по мнению автора, «использовать этот термин как устоявшийся пока преждевременно». Учитывая, какую роль в становлении дискурса о российской «гибридной войне» сыграла пресловутая «доктрина Герасимова», использование данного термина начальником российского Генштаба в нейтральном аналитическом ключе в период, когда обвинения России в ведении «гибридной войны» против Запада, стали повсеместными, выглядит как минимум опрометчивым шагом. То обстоятельство, что в российской академической среде дискурс о «гибридной войне» и «гибридных угрозах» был воспринят некритично, без должного понимания его идеологической природы, и взят в разработку как подлинно

¹³⁴ Саква Р. Россия против остальных. Кризис мирового порядка после окончания холодной войны / пер. с англ. / Р. Саква. М.: Весь мир, 2020. С. 148-155.; Sakwa R. Russian Neo-Revisionism / R. Sakwa // Russian Politics. 2019. Vol. 4, No. 1. P. 1-21.

¹³⁵ Истомин И. Россия как держава статус-кво / И. Истомин // Россия в глобальной политике. 2020. № 1. URL: <https://globalaffairs.ru/articles/rossiya-kak-derzhava-status-kvo/> (дата обращения: 11.11.2020)

¹³⁶ См. например Тренин Д. Смягчение конфликта в условиях гибридной войны / Д. Тренин // Московский центр Карнеги. 2018. 25 января. URL: <https://carnegie.ru/2018/01/25/ru-pub-75296> (дата обращения: 11.11.2020) ; Россия и США находятся в состоянии гибридной войны. Это всерьёз и надолго. Интервью Дмитрия Тренина // Новая газета. 2018. 1 октября. № 108. URL: <https://novayagazeta.ru/articles/2018/09/27/77969-rossiya-i-ssha-nahodyatsya-v-sostoyanii-gibridnoy-voyny-eto-vserez-i-nadolgo> (дата обращения: 11.11.2020)

¹³⁷ Бартош А. А. Гибридная война. Учебное пособие / А. А. Бартош. Москва: Кнорус, 2021. 306 с. ; Иншаков С. М. Гибридная война в системе военных угроз национальной безопасности / С. М. Иншаков. М.: Русайнс, 2018. 306 с.

¹³⁸ Герасимов В. В. Организация обороны Российской Федерации в условиях применения противником «традиционных» и «гибридных» методов ведения войны / В. В. Герасимов // Вестник Академии военных наук. 2016. № 2 (55). С. 19-23.; Герасимов В. По опыту Сирии / В. Герасимов // Военно-промышленный курьер. 2016. 7 марта. URL: https://vpk.name/news/150974_po_opytu_sirii.html (дата обращения: 11.11.2020) ; Герасимов В. Мир на гранях войны / В. Герасимов // Военно-промышленный курьер. 2017. 15 марта. URL: https://vpk.name/news/177000_mir_na_granyah_voiny.html (дата обращения: 11.11.2020)

новый элемент военно-стратегической обстановки только укрепило западных обозревателей в обоснованности данного дискурса.

Кроме того, в отечественной политической публицистике и, в меньшей степени, в научной литературе присутствует аргументационная линия¹³⁹, доказывающая необходимость ведения Россией «гибридной войны» против Запада или констатирующая факт её будто бы успешного ведения. При всей спорности подобных тезисов они также способствуют усилению западного нарратива, выступая наглядным подтверждением его истинности.

Таким образом, дискурс о «гибридной войне» РФ против Запада был сформулирован весной 2014 г. для подкрепления и теоретического обоснования украинского нарратива о «российской агрессии на Украине», а также консолидации западного сообщества вокруг идеи помощи новому украинскому руководству в отражении этой «агрессии» и предотвращения выработки какого-либо компромиссного варианта урегулирования кризиса между Западом и Россией. На начальной стадии основную роль в утверждении этого дискурса сыграли представители аналитических структур стран Балтии, Польши, Великобритании, Украины, «запустившие» термин «гибридная война» в публичное пространство, где его довольно быстро переняли политические деятели и официальные лица этих стран. В концептуальном отношении дискурс о «гибридной войне», объединяя в единое целое конвенциональные, иррегулярные и информационные средства ведения войны, способствовал «этатизации» нетрадиционных угроз безопасности и «милитаризации» «мягкой силы» как инструмента, способного вызвать коллапс государственности. Итогом подобной интерпретации категории «гибридной войны» стало множественное расширение оперативно-стратегического поля конфликтных действий, включающее расширение круга реальных или потенциальных участников конфликта (вплоть до ликвидации разделения между комбатантами и

¹³⁹ См., например: Марков С. «Гибридная война» против России / С. Марков. М.: Алгоритм, 2015. 208 с.; Панарин И. Н. Гибридная война: теория и практика / И. Н. Панарин. М.: Горячая линия – Телеком, 2017. 404 с.; Низовцева Н. Ф. Гибридная война как геополитический тренд / Н. Ф. Низовцева, Н. В. Гришанин // Научные труды СЗИУ — филиала РАНХиГС. 2016. Том 7. Выпуск 3 (25). С. 76–85.

некомбатантами), расширение сфер и театров оперативных действий и расширение диапазона допустимых к применению средств поражения противника. При этом данный дискурс основывался на ряде искусственно сконструированных (или откровенно сфабрикованных) представлений о внешней политике России, доказывающих наличие у её лидеров агрессивных замыслов в отношении Запада задолго до украинского кризиса, прежде всего, на пресловутой «доктрине Герасимова».

1.3. Развитие представления о «российской информационной угрозе» в рамках теории «гибридной войны»

С внедрением концепта «гибридной войны» представление о «российской информационной угрозе» получило дополнительный вес и содержательное наполнение в западном политическом пространстве. Это связано с тем, что информационный компонент играет центральную роль в создании пропагандистского конструкта «гибридной войны» и его использовании в качестве концептуального фундамента курса на конфронтацию с Россией. Он является цементирующим элементом, позволяющим сочетать в едином концепте разнородные формы военного противостояния и невоенной конкуренции государств и придать ему тотальный устрашающий характер. Кроме того, информационная сфера представляет собой потенциально наиболее обширный источник фактов о якобы деструктивных действиях России, иллюстрирующих тезис о ведении ею «гибридной войны» против Запада, в том числе, в силу присутствия в информационном пространстве большого числа индивидуальных и коллективных акторов, действия и дискурс которых можно увязать с Россией или российским обществом.

С другой стороны, помещение информационной сферы в центр единого комплекса оперативных театров военных действий приводит к её милитаризации и даёт основания для применения формальных и неформальных мер

регулирования и ограничения, которые не являются необходимыми, если речь идёт об отдельном измерении традиционной межгосударственной конкуренции.

Самым заметным в публичном пространстве последствием развития западного дискурса о «гибридной агрессии России» стала милитаризация «мягкой силы» России, провозглашение вполне конструктивных, законных и невраждебных действий, применяемых российской дипломатией на международной арене, инструментами «гибридной стратегии», к которым можно и нужно применять самые жёсткие меры противодействия. В наибольшей степени это проявилось в делегитимации любых попыток информационного влияния РФ за рубежом как заведомо злонамеренных и разрушительных.

Важной концептуальной инновацией стало совмещение в едином понятии «российской информационной угрозы», как минимум, трёх направлений информационного воздействия, воспринимаемых до этого как разнородные явления: (1) собственно кибератак, призванных подорвать функционирование технической инфраструктуры, (2) пропаганды, призванной воздействовать на политические симпатии и активность населения своей или чужой страны, и (3) дезинформации, приводящей к принятию ошибочных решений политическими лидерами или введению в заблуждение общественного мнения. Соединение настолько разнородных явлений информационного противоборства в единый комплекс следовало общей методологии конструирования «гибридной войны», в рамках которой любые, даже самые мирные действия соперника в информационной, политической и экономической сферах начинают рассматриваться как часть его якобы агрессивной стратегии и имеющие поэтому непосредственное военно-стратегическое значение.

Подобно тому, как в вопросе о «гибридной войне» западные публикации, в основном, отталкивались от «основополагающей» статьи Я. Берзиньша, тон подавляющего большинства академических и экспертных публикаций этого периода о «российской информационной угрозе» был задан несколькими «реперными» текстами, главным из которых стал материал Питера Померанцева и Майкла Вайса «Угроза ирреальности: как Кремль использует в качестве

оружия информацию, культуру и деньги»¹⁴⁰, опубликованный в ноябре 2014 г. и удостоившийся огромного количества ссылок в последовавших публикациях на эту тему. Объявив РФ реваншистской страной с захватническими намерениями, авторы утверждают, что в рамках «нелинейной войны», якобы ведущейся Кремлём, происходит массированное использование информационного оружия против соседей РФ и стран Запада, что само по себе представляет огромную угрозу. В число таких угроз внесено и распространение вполне рациональных и подкреплённых наблюдениями трактовок украинского кризиса, распространённых в России, поэтому они отвергаются на корню как заведомый абсурд, не стоящий внимания, а само распространение этих трактовок криминализуется.

Другой «реперной» публикацией (хоть и с меньшим количеством ссылок на неё) стал материал Маргариты Яйтнер и Петера Маттсона¹⁴¹, опубликованный в 2015 г. всё тем же натовским Центром в Таллине. В нём тезис о неразрывной связи киберактивности, дезинформации, использования пропаганды через СМИ и соцсети, попыток построения собственного нарратива, был утверждён как объективный факт и стал шаблоном для смешения этих тем в последующих публикациях других авторов.

Ещё одним автором, часто привлекаемым для задания «правильного понимания» происходящего, стал Кер Жиль. В публикации 2015 г., выпущенной натовским Центром в Риге¹⁴², он объяснил, что, в отличие от Запада, для которого информационная война сводится к опровержению ложной информации, для России инфовойна – это нечто тотальное, включающее целостные нарративы на тему истории, языка, культуры, национализма, усугублённое использованием

¹⁴⁰ Pomerantsev P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money / P. Pomerantsev, M. Weiss // A Special Report presented by The Interpreter, a project of the Institute of Modern Russia. URL:

https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev_The_Menace_of_Unreality.pdf

(дата обращения: 11.11.2020)

¹⁴¹ Jaitner M. Russian Information Warfare of 2014 / M. Jaitner, P. A. Mattsson // 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace. M. Maybaum, A.-M. Osula, L. Lindström (Eds.) Tallinn: NATO CCD COE Publications, 2015. P. 39-52

¹⁴² Giles K. The Next Phase of Russian Information Warfare / K. Giles // The NATO Strategic Communications Centre Of Excellence. 2015. URL: <https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles> (дата обращения: 11.11.2020)

компьютерных вирусов и троллей. Очевидно, в данном случае задавался стандарт, в соответствии с которым любое действие Запада в информационном пространстве должно было рассматриваться изолированно от его геополитических целей, как простое выражение мнения, а любое действие России (или приписываемое ей действие) – как часть тотальной информационной войны, ведущейся с самыми злонамеренными целями.

Заданная таким образом очевидная ненаучность, с которой противоположные шаблоны произвольно применялись для описания однородных явлений с претензией на объективность, воспроизводилась в десятках публикаций разных авторов, последовавших в 2016 г. Так, в статье Бена Ниммо¹⁴³, претендующей на изучение деятельности «таблoидного» сайта «Спутник» в Восточной Европе, созданного структурами РФ, криминализируются совершенно стандартные приёмы пропаганды, повсеместно используемые, в том числе, и западными информационными структурами: *«Ясно, что Спутник предоставляет непропорциональное освещение протестным, антиистеблишментским и пророссийским депутатам Европарламента от ЦВЕ; что это происходит систематически; и что даже когда он цитирует основных политиков, он выбирает комментарии, которые соответствуют более широкому нарративу о коррумпированном, декадентском и русофобском Западе»*¹⁴⁴.

Аналогичным образом, в статье К. Пола и М. Мэтьюс¹⁴⁵ стандартные и банальные приёмы манипуляции, изначально взятые на вооружение именно Западом, преподносятся как российское изобретение. Борьбу же с «российской пропагандой» предлагается вести всеми доступными способами, вплоть до договоров с провайдерами и соцсетями на тему блокирования «шланга лжи» для ослабления масштабов российской пропаганды.

¹⁴³ Nimmo B. Sputnik: Propaganda in a New Orbit / B. Nimmo // Information Warfare Initiative. January 2016. Center for European Policy Analysis (CEPA). Paper No. 2. URL: <https://silo.tips/download/propaganda-in-a-new-orbit> (дата обращения: 11.11.2020)

¹⁴⁴ Там же.

¹⁴⁵ Paul C. The Russian “Firehose of Falsehood” Propaganda Model. Why It Might Work and Options to Counter It / C. Paul and M. Matthews // Perspective – RAND Corporation. 2016

В статье Стива Абрамса¹⁴⁶ «путинская пропаганда» возводится к советским образцам, причём стандартные меры пропаганды, применяемые всеми, преподносятся как нечто инфернальное и присущее только русским. Автор вспоминает, что сразу после прихода к власти Р. Рейгана был создан комитет по исследованию советских «активных мер», который продолжал свою деятельность до демонтажа СССР и всё время существования разоблачал злостные меры КГБ, направленные на уничтожение США. Автор приходит к выводу, что новые времена подтвердили полную правоту рейгановской комиссии, а старые советские методы применяются с новыми технологиями и в новых условиях (деятельность телеканала *Russia Today* и проч.).

Похожий стиль изложения темы с нагнетанием истерии выдержан в американском милитаристском сборнике, выпущенном фондом Маршалла¹⁴⁷ и в статье Д. Витера¹⁴⁸, причём последний автор приравнивает Россию к Исламскому государству (ИГ)¹⁴⁹ на основе того, что и РФ, и ИГ проводили информационные операции.

Надо сказать, что упомянутые выше «реперные» материалы 2014–2015 гг. задавали шаблон для последующих публикаций, претендующих на академичность, и служили для них точкой референции с обязательным оформлением ссылки на первоисточник. Вброс ключевых, знаковых, сформулированных в наиболее радикальных и шокирующих выражениях антироссийских идеологов, раздувающих якобы нависающую над Западом экзистенциальную угрозу со стороны России, провоцировал общественное обсуждение, в «воронку» которого втягивались уже настоящие академические авторы, а их подключение легитимизировало и придавало солидность исходным тезисам. И уже в ходе этого обсуждения, благодаря массовости однотипных

¹⁴⁶ Abrams S. Beyond Propaganda Soviet Active Measures in Putin's Russia / S. Abrams // Connections. Winter 2016. Vol. 15, No. 1. P. 5-31. URL: <https://www.jstor.org/stable/26326426> (дата обращения: 07.08.2018)

¹⁴⁷ Countering Russian Propaganda. Concordiam (Journal of George Marshall European Center for Security Studies). Special Edition. Vol. 7, 2016. 40 p.

¹⁴⁸ Wither J.K. Making Sense of Hybrid Warfare / J.K. Wither // Connections. Spring 2016. Vol. 15, No. 2. P. 73-87. URL: <https://www.jstor.org/stable/26326441> (дата обращения: 07.08.2018)

¹⁴⁹ Террористическая организация, запрещённая в РФ.

публикаций о «российской информационной угрозе», обеспеченной ресурсами НАТО и антироссийски настроенными НГО, самые радикальные тезисы из «реперных» публикаций укоренялись как самоочевидные и не требующие дальнейшего обоснования.

В этот же период, пока общее представление о серьёзности «российской информационной угрозы» только устанавливалось на Западе и опиралось на далёкие для западного обывателя примеры Украины, Грузии, Киргизии и, может быть, Прибалтики и Центрально-Восточной Европы, заблаговременно издавались и новые «реперные» публикации, готовивших почву для усиленной стигматизации России в последующем. В этом ряду стоит выделить два крайне радикальных материала. Во-первых, 45-страничный сборник с предложениями о «полномасштабной» американской стратегии в отношении России, выпущенный фондом *Heritage* в 2015 г.¹⁵⁰. В нём изложена фактически стратегия всеобъемлющей конфронтации без сохранения каких-либо кооперативных или переговорных путей взаимодействия, а лишение Москвы возможностей для внешнего информационного влияния выступает одной из ключевых задач. Показательным в этой связи является, к примеру, предложение *«делегимитизировать притязания России на защиту меньшинств. Стратегия России в большинстве этих конфликтов заключалась в том, чтобы заявить, что она защищает угнетённые меньшинства. Эта претензия призвана обратиться к нежной совести Запада. Запад должен придерживаться стандарта, согласно которому бунт против репрессивных режимов является правом, но нет права на революцию без справедливой причины и, конечно, на внешнюю поддержку революции. Без такого стандарта не удастся отвергнуть попытки России разжечь пламя новых конфликтов»*¹⁵¹.

В 2016 г. вышла новая работа с участием П. Померанцева – совместное с Эдвардом Лукасом 70-страничное руководство по ведению информационной

¹⁵⁰ U.S. Comprehensive Strategy Toward Russia/ James Jay Carafano (ed.). – Davis Institute For National Security and Foreign Policy. Special Report No. 173 | December 9, 2015. The Heritage Foundation. URL: <https://www.heritage.org/europe/report/us-comprehensive-strategy-toward-russia> (дата обращения: 11.11.2020)

¹⁵¹ Ibid., P. 28.

войны¹⁵². В основном обобщая и собирая в одном месте наработанные за два года риторику и обвинения с привычными примерами «дезинформации» от России (авторы утверждают, что риторика российских СМИ о русофобском сносе монумента героям войны – такая же дезинформация, как и утверждения, что события Евромайдана – это переворот), они формулируют рекомендации: анализ контента российской пропаганды и её эффекта на разные страны и социальные медиа, усиление качества контрпропаганды и участия в них НГО, создание новых агентств и объединения западных политических сил против России по типу межпартийных комитетов в США, более широкое привлечение к информационному противостоянию России организаций типа *Global Witness* и *Transparency International*, работа с историческими травмами, использование соцсетями новых технологий против пророссийски настроенных групп, усиление «независимого» вещания прозападной ориентации, взаимодействие блогеров, создание «фабрики» русскоязычного прозападного контента на базе Украины, Прибалтики и Кавказа, распространение прозападных новостей на русском языке, повышение «медиаграмотности» населения, пресечение финансирования через рекламу каналов антизападной ориентации.

На этом фоне выделяются работы с меньшим радикализмом либо ставящие антироссийский «мэйнстрим» под сомнение. Некоторые можно отнести, хоть и к ангажированным, но исследовательским проектам западных «мозговых центров», призванных дать объективное знание о ведении информационных войн и способности России к её ведению, а потому содержащих более объективные формулировки, чем чисто пропагандистские материалы¹⁵³, однако более интересны единичные случаи прямого оппонирования общепринятому подходу. Так, в статье С. Симбалы и Р. МакДермотта 2015 г.¹⁵⁴ снова содержится

¹⁵² E. Lucas. Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe / E. Lucas and P. Pomeranzen // A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute. August 2016. 70 p.

¹⁵³ См. например *Cyber War in Perspective: Russian Aggression against Ukraine* / K. Geers (Ed.) // NATO CCD COE Publications, Tallinn 2015, 175 p.; Andersson J.J. Hybrid operations: lessons from the past / J.J. Andersson // European Union Institute for Security Studies Brief. October 2015. 4 p. URL: [https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief 33 Hybrid operations.pdf](https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2033%20Hybrid%20operations.pdf) (дата обращения: 11.11.2020)

¹⁵⁴ Cimbala S. J. A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War / S. J. Cimbala, R. N. McDermott // *Comparative Strategy*. 2015. Vol. 34, No. 1. P. 95-111.

призыв не преувеличивать степень угрозы, которая в принципе может быть вызвана информационными войнами и кибероперациями. Они пишут, что нет оснований отходить отвлекаться от строгих стратегических представлений о войне, изложенных Клаузевицем. Сами по себе кибервойны затрагивают только информационную сферу и не могут нанести такого мгновенного разрушительного ущерба, как ядерное оружие, поэтому опасаться надо только их соединения с оружием массового поражения, а страхи провоцируются по другим, недостаточным поводам. Показательны заключительные предложения, осторожно отмечающие методологическую несостоятельность возобладавшего в тот момент подхода, преувеличивающего «информационную угрозу»:

«Киберподдержка ядерного сдерживания и обычных вооружённых сил жизненно важна, но шумиха, связанная с информационным веком, отвлекает от строгости стратегии, изложенной Клаузевицем. Прежде всего, необходимо понять тип войны или принудительной операции, в которой мы участвуем, а затем чётко осознавать, чего мы хотим при этом достичь. Информационные технологии могут изменить характер войны, но не её фундаментальную природу – с ядерным оружием или без него»¹⁵⁵.

Другим важным материалом, полностью оппонирующим мейнстриму, стала статья О. Бойд-Барретта¹⁵⁶, в которой чётко указывается на необъективность западных правительств и СМИ, прямой обман ими своих народов. Вспомнив недавние агрессии, развёрнутые западными странами под ложными предлогами, которые потом были опровергнуты, автор задаётся вопросом: а в этот раз сможет ли западный обыватель не попасться на обман своих правительств? Ответ он предлагает пессимистичный и исследует борьбу нарративов вокруг конфликта на Украине. В частности, он указывает, что в отношении Крыма западные СМИ не раскрывали всего контекста событий и утаивали действительное стремление жителей полуострова воссоединиться с Россией, умалчивали о враждебных

¹⁵⁵ Ibid., P. 106.

¹⁵⁶ Boyd-Barrett O: Ukraine, Mainstream Media and Conflict Propaganda / O. Boyd-Barrett // Journalism Studies. 2017. Volume 18. P. 1016-1034.

действиях Правительства Украины по перекрытию электроэнергии и воды на полуостров, подавали исключительно негативное описание жизни крымчан после воссоединения.

Таким образом, конструкт «российской информационной угрозы» как комплексного сочетания различных методов и технологий информационного воздействия был вброшен на волне украинского кризиса несколькими медийно растиражированными провокационными публикациями экспертов, известных своей ангажированной антироссийской идеологической ориентацией. И хотя в отдельных работах содержательность этого конструкта и целесообразность его использования ставилась под сомнение, западная академическая среда в целом не только не отвергла его как ложный и не соответствующий критериям научной верификации, но и присоединилась к его дальнейшему закреплению и тиражированию уже в качестве научно обоснованного факта.

Наибольшая гиперболизация «российской информационной угрозы» и придание ей практически тотального характера происходит после президентских выборов в США в 2016 г. и неожиданной победы на них Дональда Трампа. Активно муссируемые в прессе факты предполагаемых связей команды Д. Трампа с политическим руководством РФ и предполагаемого российского вмешательства в избирательный процесс стали основой для политических обвинений избранного Президента и открытых разбирательств со стороны правоохранительных органов США. Публике навязывалось представление, что отныне Россия угрожает не далёким Украине, Прибалтике и Польше, а осуществляет прямую агрессию против самих США и крупнейших западноевропейских стран, на их национальной территории. Переосмысливались и расширялись прежние обвинения: так, кибератаки теперь становились инструментом решающего вмешательства в выборы, способным привести к власти угодные Кремлю режимы, а не ударами по отдельным элементам инфраструктуры. К новым, ранее не описанным инструментам России

теперь начинали относить задействие «Путининтерна»¹⁵⁷ – симпатизирующих России либо настроенных против конфронтации с ней политических и общественных деятелей. К особо опасным инструментам Кремля стали относить организованную преступность¹⁵⁸, якобы действующую по всему миру, включая западные страны. Следствием этого стало резкое повышение значимости «российской информационной угрозы» во внутривнутриполитическом процессе США и европейских государств и активизация мер по противодействию ей. Кроме того, прямое обвинение симпатизирующих России политических сил в работе на Кремль исключало их из общественного обсуждения и позволяло нейтрализовать их попытки воспрепятствовать дальнейшему укреплению антироссийского курса.

Так же, как и на предыдущем этапе, отдельный сегмент публикаций был направлен на академическое исследование предмета (информационных войн) и возможностей противника (России), и поэтому содержал более объективные данные¹⁵⁹, ещё какая-то часть публикаций готовилась под влиянием инерции предыдущего периода и отличалась менее радикальными формулировками¹⁶⁰. В статье К. Бойта¹⁶¹, несмотря на ряд общепринятых фактических ошибок (например, о «доктрине Герасимова») и общую необъективность выводов, следующих принятой парадигме вопреки известным фактам, содержится много ценной информации, раскрывающей понимание западными аналитиками хода информационной войны, в частности, указание на то, что в англоязычном медиaprостранстве удалось успешно погасить российскую пропаганду, представив её риторикой «холодной войны».

¹⁵⁷ Эйджман И. Кремль уже создал в Европе «Путин-Интерн» / И. Эйджман // Ліга.нет. 01.09.2017. URL: <https://www.liga.net/politics/opinion/kreml-uzhe-sozdal-v-evrope-putin-intern> (дата обращения: 11.11.2020)

¹⁵⁸ Galeotti M. Crimintern: How the Kremlin uses Russia's criminal networks in Europe // ECFR. 18.04.2017. URL: https://ecfr.eu/publication/crimintern_how_the_kremlin_uses_russias_criminal_networks_in_europe/ (дата обращения: 11.11.2020)

¹⁵⁹ См., например, Connell M. Russia's Approach to Cyber Warfare / M. Connell, S. Vog // CNA Analytic Solutions. March 2017. URL: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf (дата обращения: 11.11.2020)

¹⁶⁰ См., например, подготовленную «Атлантическим советом» Стратегию сдерживания в информационном пространстве: Strategy of "Constrainment". Countering Russia's Challenge to the Democratic Order / F.O. Hampson et al. // Atlantic Council. March 16, 2017. URL: <https://www.cigionline.org/publications/strategy-constraintment-countering-russias-challenge-democratic-order> (дата обращения: 11.11.2020)

¹⁶¹ Boyte K. J. An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine / K. J. Boyte // Journal of Information Warfare. 2017. Vol. 16, No. 1. P. 88-111.

К достаточно объективным по заявленным фактам, но не по их интерпретации, можно отнести статью М. Люпайон¹⁶², которая сравнила сложность и многогранность статей в электронных изданиях РФ времён августовской войны 2008 г. и Русской весны 2014 г., автор заметила, что во второй раз статьи были более умеренно прокремлёвские, рассматривали проблему с разных углов и т. д. По мнению автора, это говорит о том, что за 6 лет, отделявших эти события, Кремль научился пропаганде: стал готовить более сложные и тем самым потенциально более убедительные статьи с широким спектром подкрепляющих его позицию аргументов. В то же время, более простую гипотезу – о том, что тема Украины и Новороссии была для российской публики намного важнее, чем Закавказье, а авторы могли и хотели сказать о ней намного больше, – автор не рассмотрела.

Отдельного упоминания заслуживает статья М. Ристолайнена¹⁶³, написанная с позиции предубеждения, что демократичный Запад воспринимает Интернет как открытое пространство со свободным обменом мнениями, а Россия выработала «цифровую Вестфальщину» («цифровой суверенитет») и хочет построить автономный Рунет к 2020 г. Далее рассказывается, что делается в России для повышения цифрового суверенитета, включая, например, появление кириллических доменов, для сохранения русскоязычного Рунета как отдельного пространства со своим способом мысли. Автор считает, что эти действия провоцируют укрепление менталитета осаждённой крепости, использование информации в качестве оружия и т. п. Таким образом, из изложенных автором фактов становится понятно, что РФ стремится огородиться от чужих атак и опасностей, связанных с тем, что в глобальном Интернете хозяйничают США. Но затем автор приходит к выводу, что такая реализация программы РФ по автономизации Рунета будет большой угрозой, потому что она сможет сколько угодно пропагандировать, проводить психологические операции и

¹⁶² Lupion M. The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News / M. Lupion // The Journal of Slavic Military Studies. 2018. Vol. 31, No. 3. P. 329-353.

¹⁶³ Ristolainen M. Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West / M. Ristolainen // Journal of Information Warfare. 2017. Vol. 16, No. 4. P. 113-131.

манипулировать информацией. Иными словами, выводы в подобных исследованиях были заданы уже господствующей на Западе парадигмой и слабо зависели от фактов.

Однако подавляющее большинство материалов носит уже радикально антироссийский характер с тяжелейшими обвинениями в адрес России и выводимыми из них предложениями по нанесению ущерба России. Так, в статье М. Бергмана и К. Кенни 2017 г.¹⁶⁴ уже пункты содержания раскрывают сущность и тяжесть обвинений: *«Россия агрессивно атакует и шпионит за США в киберпространстве; Продолжающиеся шпионские усилия России против США; Россия прорабатывает способы нападения на Америку; Россия продолжает вмешиваться в американскую политику; Россия подрывает международное право и договоры; российские военные действуют опасно и вызывающе; Россия действует против интересов США и международной стабильности во всем мире»*. Косвенным соучастником российских преступлений объявлена администрация Трампа, никак не препятствующая этим действиям. Качество обоснования обвинений хорошо иллюстрируется одним из примеров – отсылкой к тому, что где-то в Иллинойсе были отмечены следы кибервмешательства с целью удалить или повредить списки избирателей. Не приведено никакого доказательства, что автор акции – РФ, а не кто-то, желающий инсценировать вмешательство для обвинения РФ; нет никакого обоснования того, как такое вмешательство может навредить интересам США и послужить интересам РФ. Ещё один пример – обвинение в похищении хакерами данных 40 олимпийских атлетов, полностью лишённое пояснения о мотивации Кремля. В числе рекомендаций авторов можно отметить предложения остановить «умиротворение» Москвы, защитить избирательную систему от кибератак, агрессивно накладывать новые санкции, усилить контроль над социальными сетями, пресекать отмывание денег, поддерживать восточноевропейские страны

¹⁶⁴ Bergmann M. Acts of an Adversary. Russia's Ongoing Hostilities Toward the United States and Its Allies / M. Bergmann, C. K. December // Center for American Progress. 2017. 48 p. URL: <https://www.americanprogress.org/issues/security/reports/2017/12/05/443574/acts-of-an-adversary/> (дата обращения: 11.11.2020)

в их сопротивлении российскому влиянию, сохранять сотрудничество с Россией в тех областях, где это полезно для США, во избежание чрезмерной эскалации.

Похожим по содержанию, но намного более детализированным является знаковый доклад Р. Блэквилла и Ф. Гордона для авторитетного Совета по внешним отношениям¹⁶⁵, на основании которого ими была опубликована статья в журнале *Foreign Affairs*¹⁶⁶. С первого же абзаца предисловия идёт запугивание читателя рассуждением, что факт вмешательства РФ в выборы имел место, и вопрос о том, произвёл ли он какой-то эффект, – это увод в сторону: главное, что вмешательство было. И преследовало оно цель подрыва американской демократии, чтобы «ослабить Соединённые Штаты, разделить их с европейскими союзниками и распространить российское влияние в Европе, на Ближнем Востоке, в Азии и далее»¹⁶⁷.

Список обвинений России и якобы потворствующей ей администрации Белого дома примерно повторяет идеи предыдущего доклада (разве что, существенно детализировано обвинение о якобы организации бесплодных споров между американскими политизированными группами), но рекомендации расширены: помимо мер по ведению информационной войны, предлагается наращивание чисто военного давления. Отдельно предлагается список мер по поддержанию контроля над обычными вооружениями в Европе либо выход из соглашений, если РФ поведёт себя «плохо», предлагается публично объявить, что РФ нарушает ДРСМД и предъявить РФ ультиматум о немедленном возвращении к выполнению договора под угрозой выхода из него США, не инвестировать слишком много в ракеты наземного базирования, поскольку европейские союзники будут недовольны, и инвестировать в морское и авиационное вооружение, строить могучую ПРО, усиливать американские

¹⁶⁵ Blackwill R. Containing Russia. How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge / R. D. Blackwill, Ph. H. Gordon // Council on Foreign Relations (CFR). Council Special Report No. 80 January 2018, 43 p.

¹⁶⁶ Blackwill R. Containing Russia, Again. An Adversary Attacked the United States—It's Time to Respond / R. D. Blackwill, Ph. H. Gordon // Foreign Affairs. January 18, 2018. URL: <https://www.foreignaffairs.com/articles/russian-federation/2018-01-18/containing-russia-again> (дата обращения: 11.11.2020)

¹⁶⁷ Ibid., P. p. Vii.

ядерные вооружения и т. д. Часть этих предложений была реализована с момента публикации. В целом, данная статья является хорошим примером того, как западные эксперты, в отличие от российских, в ответ на «гибридные» угрозы не предлагают ограничиться «гибридными» мерами, но и требуют активировать средства из классического арсенала жёсткой силы.

По тому же шаблону были построены многие другие публикации. Уже упомянутые выше М. Бергман и К. Кенни опубликовали ещё одну статью¹⁶⁸ с детализацией якобы используемых Россией технологий информационной войны, которые привязывались к якобы существующей давней советской традиции таких мероприятий.

Эксперты по европейской тематике следовали за американским примером. В 2018 г. фонд Карнеги опубликовал крайне алармистский (доходящий до истеричного тона) доклад Э. Браттберга и Т. Маурера¹⁶⁹ о том, как враждебные действия РФ против выборов США показали, что избирательная система входит в число критически уязвимой инфраструктуры, а теперь и Европа пережила пять попыток российского вмешательства: в Нидерландах в марте 2017 г., во Франции в мае-июне 2017 г., в Великобритании в июне 2017 г., в Германии в сентябре 2017 г., в Швеции в сентябре 2018 г. Эту же линию продолжила серия брошюр Атлантического совета о попытках влияния РФ в Европе и «тройанских конях» РФ, под которыми понимались немэйнстримные политические силы этих стран, когда-либо поддержанные российской пропагандой¹⁷⁰. В сборнике под редакцией Н. Попеску и С. Секрьери¹⁷¹ говорится, что у РФ нет никакого другого

¹⁶⁸ Bergmann M. War by Other Means. Russian Active Measures and the Weaponization of Information. War by Other Means. M. Bergmann, C. Kenney. – Center for American Progress. Posted on June 6, 2017. 45 p. URL: <https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/> (дата обращения: 11.11.2020)

¹⁶⁹ Brattberg E. Russian Election Interference. Europe's Counter to Fake News and Cyber Attacks / E. Brattberg, T. Maurer // Carnegie Endowment for International Peace. May 2018. 54 p. URL: https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf (дата обращения: 11.11.2020)

¹⁷⁰ См. например The Kremlin Trojan Horses. Russian Influence in Greece, Italy, and Spain / A. Polyakova et al. Atlantic Council – Eurasia Center. November 2016. 36 p. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/> (дата обращения: 11.11.2020)

¹⁷¹ Hacks, leaks and disruptions – Russian cyber strategies / N. Popescu, S. Secriery (Eds.) // EU ISS Chaillot papers. 2018. No. 148. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (дата обращения: 11.11.2020)

выхода, кроме кибератак, если она хочет оставаться в лидерах киберпространства, т. к. у неё нет других возможностей добиться этого, при этом также используют рассуждение «кому выгодно» как доказательное при атрибуции кибератак.

Ряд публикаций на других языках представлял собой компиляцию и изложение высказанных ранее тезисов англоязычных публикаций другими словами, без попытки расширения идейного наполнения. В публикации К. Лимонье и К. Жерара¹⁷² излагается такая же версия взлома сервера Демократической партии и утечек информации, использованных РФ, что показало высочайшую уязвимость западных демократий. Авторы задаются целью исследовать, как Москва превращает киберпространство в поле противостояния. По их словам, обладая меньшими киберресурсами, чем США, Китай и Израиль, именно РФ провела одну из успешнейших в истории наступательных операций в цифровых сетях. В общей сложности РФ обвиняют в не менее чем 32 атаках после 2007 г., включая не менее 30 после 2014 г. (приводится рисунок на апрель 2017 г.). Окончательных доказательств того, что их виновником была РФ, не представлено, потому что это следовало из разведданных у западных правительств, которые скрывают доказательства, чтобы избежать эскалации взаимных доказанных обвинений. Далее авторы обсуждают поддержку Россией Марин Лё Пен, деятельность каналов *Russia Today* и *Sputnik*, а также приводят важную схему, показывающую природу распространения информации при пропаганде: поскольку непосредственно у этих каналов аудитория небольшая, то их интерпретации пробиваются к широкой публике через блоги крайне-правых репостеров, через некритичных последователей и через автоматизированную систему раскрутки (ботов). Та же линия изложения используется в другой публикации с участием К. Лимонье¹⁷³.

¹⁷² Limonier K. Guerre hybride russe dans le cyberspace/ K. Limonier, C. Gérard/ / Hérodote 2017/3, N°166-167, p. 145-163. URL: <https://www.cairn.info/revue-herodote-2017-3-page-145.htm> (дата обращения: 11.11.2020)

¹⁷³ Limonier K. La stratégie d'influence informationnelle et numérique de la Russie en Europe / K. Limonier, M. Audinet // Hérodote 2017/1 (N°164), P. 123-144. URL: <https://www.cairn.info/revue-herodote-2017-1-page-123.htm> (дата обращения: 11.11.2020)

Другой французский автор – Ж. Носетти¹⁷⁴ тоже перечисляет все «преступления» РФ в информационной сфере, начиная с якобы «парализованной» в 2007 г. Эстонии и кончая якобы попыткой РФ запутать мировой общественное мнение по поводу якобы предпринятой сторонниками Асада химической атаки в Думе в 2018 г. (автор не ставит под сомнение, что атака была и её предприняли лоялисты; факт фальсификации данных ОЗХО об этой атаке был вскрыт намного позже).

Параллельно выходили публикации, в большей степени ориентированные на мультиплицирование наработанных технологий информационной войны против России. Так, в работе Е. Крюк¹⁷⁵ разбирается опыт «информационного сопротивления» Украины. Например, польза перекрытия трансляции российских каналов на Украине иллюстрируется тем, что их в результате стали меньше смотреть, хотя потом всё-таки приводятся данные падения доверия к российским каналам, последовавшего за сокращением их аудитории. Автор также рекомендует широкое использование в информационной войне НГО, специальных сайтов и проч. Ещё одна украинская исследовательница¹⁷⁶, разбирая работу российских СМИ накануне свержения Януковича, криминализирует даже те репортажи последних, в которых поведение участников беспорядков критикуется по совершенно справедливым поводам, а также вскрывают роль Запада в беспорядках.

Общие рекомендации по борьбе с «российской дезинформацией», издаваемые в этот период, собирали всевозможные меры, разработанные «на местах»: от откровенно репрессивных и связанных с запретом на «неправильную» точку зрения, до идей по контрпропаганде и навязыванию собственного нарратива. В отдельных случаях выпускались мини-учебники

¹⁷⁴ Nocetti J. Géopolitique de la cyber-conflictualité / J. Nocetti // Politique étrangère. 2018. No. 2. P. 15-28.

¹⁷⁵ Kruk K. Analyzing the Ground Zero. What Western Countries Can Learn from Ukrainian Experience of Combating Russian Disinformation / K. Kruk // European Values Kremlin Watch Report. 11.12.2017. 24 p. URL: <https://www.europeanvalues.net/wp-content/uploads/2017/12/Analyzing-the-Ground-Zero..pdf> (дата обращения: 11.11.2020)

¹⁷⁶ Pasitselska O. Ukrainian crisis through the lens of Russian media: Construction of ideological discourse/ O. Pasitselska // Discourse & Communication. 2017. Vol. 11, No. 6. P. 591-609.

(«методички») для журналистов¹⁷⁷, предложения бороться с российским нарративом как целым, привлекая к сотрудничеству фирмы, владеющие соцсетями¹⁷⁸. Обстоятельный сборник по противодействию российской пропаганде в соцсетях выпустила корпорация RAND¹⁷⁹. Но наиболее радикальным выглядит изданный Атлантическим советом в феврале 2018 г. перечень рекомендаций по «защите от российской дезинформации» под редакцией Д. Фрида и А. Поляковой¹⁸⁰. В частности, они пишут: *«Мы рекомендуем создать «Коалицию по борьбе с дезинформацией», неофициальную группу правительств-единомышленников и неправительственных заинтересованных сторон, для разработки передовых методов защиты от дезинформации, включая стандарты для социальных сетей, такие как добровольный кодекс поведения, и даём рекомендации по будущим вызовам, возникающие в недемократических странах»*¹⁸¹.

Особое внимание уделяется противодействию распространению российской пропаганды через соцсети, щедрому финансированию «независимых журналистов» и гражданского общества пронатовской направленности, необходимости создать орган по взаимодействию с частными лицами в информационном пространстве с участием представителей ФБР, ЦРУ, Пентагона и вышеупомянутых структур. Относительно Европы предлагается законодательно преследовать СМИ, распространяющие дезинформацию, как это делает Великобритания и Литва с *Russia Today*, делать собственные «правдивые» русскоязычные СМИ типа «Медузы», вещающей из Латвии, потребовать от

¹⁷⁷ KEY STEPS FOR COUNTERING RUSSIAN PROPAGANDA. A toolkit for journalists // Political Capital Institute. Budapest, March 2017. URL: https://www.stopfake.org/content/uploads/2017/05/Toolkit_RussianPropaganda_Journalists_170509.pdf (дата обращения: 11.11.2020)

¹⁷⁸ Hanlon B. It's Not Just Facebook: Countering Russia's Social Media Offensive / B. Hanlon // The Alliance for Securing Democracy (at the German Marshall Fund of the United States Brief. April 2018, No. 19, 9 p. URL: <https://securingdemocracy.gmfus.org/its-not-just-facebook-countering-russias-social-media-offensive/> (дата обращения: 11.11.2020)

¹⁷⁹ Russian Social Media Influence. Understanding Russian Propaganda in Eastern Europe / T. C. Helmus et al. 2018 RAND Corporation. URL: https://www.rand.org/pubs/research_reports/RR2237.html (дата обращения: 11.11.2020)

¹⁸⁰ Fried D. DEMOCRATIC DEFENSE AGAINST DISINFORMATION. / D. Fried, A. Polyakova // Atlantic Council – Eurasia Center. February 2018. 24 p. <https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/> (дата обращения: 11.11.2020);

¹⁸¹ Ibidem.

соцсетей удалять хейт-спичи, координировать работу ЕС и НАТО с национальными правительствами по противодействию органам российской пропаганды, проводить операции по официальной контрпропаганде и контрвлианию, разоблачать дезинформацию онлайн. Гражданское общество («Стопфейки», Лаборатория Атлантического Совета и проч.) должны развивать способность выявлять русских ботов и троллей и стать «охотниками на ботов» в реальном времени. Традиционные СМИ должны определять контент, происходящий от российских пропагандистских органов и очищать от него свой продукт как от подозрительного. Фейсбук, Гугл, Твитер и прочие должны помечать российские пропагандистские источники и их материал как русскую пропаганду, перенастроить алгоритмы так, чтобы различать «правдоподобный» и «неправдоподобный» контент, Гугл должен более объективно выстраивать поиск и удалять из верхних строчек пропагандистский контент, в частности, в результатах поиска деранжировать материалы от *Russia Today* и *Sputnik*.

В период после 2016 г. попытки оппонировать общепринятому подходу о «русской информационной угрозе» в западном академическом мире стали ещё более редкими и маргинальными, чем в 2014-2016 гг. В наиболее радикальных случаях лишь ставятся под сомнение базовые представления о возможности воздействовать на геополитические реалии через кибератаки и дезинформацию. Так, в работе украинских авторов Н. Костюк и Ю. Жукова¹⁸² анализируется соотношение динамики кибератак и обострений на фронтах Донбасса и в Сирии. Авторы приходят к выводу, что ожидаемой корреляции, в которой кибератаки должны были содействовать результату «на земле», не было: после правительственных атак росли кибератаки повстанцев, и наоборот. Связь между кибератаками правительства и реальными атаками ребелов – слабее, и ещё меньше было случаев, когда бы за кибератаками следовали кинетические действия. Авторы приходят к выводу, что кибератаки неэффективны как

¹⁸² Kostyuk N. Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? / N. Kostyuk, Y. M. Zhukov // Journal of Conflict Resolution. 2017. P. 1-31. URL: <https://journals.sagepub.com/doi/abs/10.1177/0022002717737138> (дата обращения: 11.11.2020)

инструмент кинетической войны. Но из этого следует, что кибератаки едва ли могут привести к геополитическому результату, в том числе и в рамках «гибридных войн», а значит, значимость этого вида информационных войн для геополитических подвижек - ничтожна.

В статье А. Ланозки¹⁸³ рассматривается возможность изменения Россией по своему вкусу международного мнения и, соответственно, государственной политики западных государств. Анализируя эту возможность с точки зрения теории международных отношений и проверяя полученные выводы на практическом примере – попытках Кремля воздействовать на политику прибалтийских республик, – автор приходит к выводу о стратегической неэффективности дезинформации, как минимум, в случае существования в стране-объекте дезинформации независимых внешнеполитических элит и нерегулируемого извне плюрализма общественного мнения.

Резюмируя проведённый анализ ключевых западных публикаций, можно заключить, что конструирование «российской информационной угрозы» в описанном потоке западных публикаций имело проработанный характер и, на первый взгляд, отвечало всем признакам системного и добросовестного научного подхода. Оно включало следующие составляющие:

- описание непосредственно наблюдаемых фактов;
- атрибуция авторства обсуждаемых действий одному главному организатору – предполагаемому противнику;
- достраивание непосредственно не наблюдаемой структуры, якобы стоящей за всеми этими фактами;
- приведение новых фактов, укладывающихся в построенную схему;
- приписывание мотивов предполагаемому организатору;
- раздувание угрозы, следующей из приписанных мотивов;
- осуждающая трактовка самых безобидных действий предполагаемого противника, следующая из их предназначения для реализации угрозы;

¹⁸³ Lanoszka A. Disinformation in international politics / A. Lanoszka // European Journal of International Security 2019. Vol. 4, No. 2. P. 227-248.

- практические предложения, направленные на нейтрализацию любых действий, приписанных «враждебной» структуре, включая самые мирные.

Именно по этой причине постоянное смешение разнородных сюжетов в потоке западных публикаций не вызывало нареканий, а только придавало солидности и отдельным публикациям, и общему конструкту. Недостаток конкретных доказательств по одному вопросу «компенсировался» аналогией с другим случаем (в котором либо тоже отсутствовали доказательства, либо не было ничего преступного). Предположительно проведённая кем-то кибератака и выступление официального российского публициста с выражением собственной позиции объединялись в единую схему под тем предлогом, что имеют общего организатора и единую цель подорвать жизненные интересы Запада, представляют для него экзистенциальную угрозу; из этого тут же выводилась необходимость ограничения свободы слова в соцсетях и стигматизация любого выражения позиции, идущей вразрез с западным мейнстримом. Все эти элементы информационного противостояния сочетались в одной публикации и дополнялись упоминанием в качестве имеющих сходную природу других, более деструктивных реальных или предполагаемых действий Москвы, как то использование вооружённых формирований без опознавательных знаков или деятельность «русской мафии», якобы подчиняющейся Кремлю, а также утверждениями о необходимости принятия чисто военных мер для сдерживания России, включая выход из Договора о ликвидации ракет средней и меньшей дальности (ДРСМД).

Слабые места этой конструкции коренятся не столько в общей схеме аргументации, в принципе, отвечающей конвенциональным принципам исследования, сколько в частностях реализации: недопустимых логических переходах, отсутствии тестирования более простых гипотез, произвольном увязывании явлений разной природы при возможности их более простого объяснения. Кроме того, данная конструкция приводит к глобальным обвинениям в адрес целой страны и её политически активной части населения

(или даже ряда стран, якобы ведущих «гибридную войну» с Западом). Сам по себе конструкт «российской информационной войны» априорно относит к дезинформации не только оправдания официальной Москвы, но причисляет к агентам Кремля, якобы пытающимся дезинформировать Запад, любые общественные силы, включая русские организации за пределами РФ, и на этом основании любые их альтернативные объяснения представлены заведомо ложными и укрепляющими конструкт.

Вне сомнений, конечным итогом конструирования «российской информационной угрозы» является делегитимация внешней и внутренней политики России как полноправного субъекта международных отношений, имеющего право отстаивать собственную позицию и преследовать национальные интересы, в том числе, с помощью возможностей «мягкой силы» и публичной дипломатии. Следует признать, что выбор Запада в пользу подобного курса имел под собой и некоторые объективные основания, связанные в первую очередь с реакцией российского руководства на распространение и укрепление западного влияния в Центрально-Восточной Европе, Прибалтике и на пространстве СНГ в предыдущие десятилетия. Отсутствие серьёзного противодействия, пренебрежение интересами русского населения и готовность соблюдать нормы международного права даже в отношении стран, открыто проводящих русофобскую политику, породили на Западе ожидания продолжения этого процесса вплоть до полной геополитической деградации России и отказа от каких-либо претензий на влияние в своём ближайшем окружении. Возможность даже частичного восстановления позиций Москвы благодаря созданию Евразийского экономического союза и, тем более, перспектива воплощения объединительных проектов на русских территориях выходила за пределы допустимого поведения России с точки зрения Запада, чего российское руководство, по всей видимости, полностью не осознавало, продолжая рассчитывать на достижение компромисса даже в условиях развернувшейся диффамационной кампании. Тогда как с момента её запуска стало очевидно, что беспрецедентность и тотальный характер якобы ведущейся

Россией «гибридной войны» против Запада и всего либерального порядка оправдывают аналогично тотальные меры по отражению данной «угрозы».

Сама постановка вопроса о наличии данной угрозы не имеет под собой реальных оснований: российская дипломатия в своих попытках оказать влияние на зарубежную общественность использовала тот же инструментарий «мягкой силы», который до этого активно применялся Западом, включая открытие своих СМИ, телеканалов и неправительственных организаций за рубежом. На пространстве СНГ диапазон применяемых средств был крайне узок. Ввиду ограниченного масштаба эти инструменты никак не могли привести к подрыву либеральной модели политического устройства и прочим приписываемым им эффектам. Более того, конкретные репутационные и политические выигрыши, которых добилась Москва в результате применения данных средств, выглядят крайне сомнительно.

Выводы по главе 1

1. Дискурс о «гибридной войне» России против Запада был сформулирован весной 2014 г. рядом военных экспертов и представителей аналитических структур стран Балтии, Польши, Великобритании, Украины для акцентирования беспрецедентности событий кризиса на Украине 2013-2014 гг., теоретического обоснования украинского нарратива о «российской агрессии», а также консолидации западного сообщества вокруг идеи помощи новому украинскому руководству в отражении этой «агрессии» как проявления специфической, крайне опасной и до того момента неосознаваемой на Западе «гибридной угрозы» со стороны России. Главной движущей силой в процессе формализации и институционализации дискурса о «гибридной войне» летом 2014 г. выступил Североатлантический альянс, запустив одновременно ряд академических исследований о сущности и природе «гибридной войны» и серию наглядных агитационных материалов, раскрывающих желаемое значение этого термина для широкой публики, а

также включив его в политический оборот благодаря упоминанию отдельным пунктом в итоговой декларации саммита НАТО в Уэльсе.

2. Сформулированный в американской военно-стратегической науке как аналитический инструмент оперативно-тактического уровня для обозначения способов сочетания регулярных и нерегулярных методов ведения военных действий в рамках локального конфликта, концепт «гибридной войны» в новом политическом контексте был использован для объединения в единое целое конвенциональных, иррегулярных, экономических и информационных средств ведения войны и международной конкуренции и для приписывания России роли инициатора в использовании подобных средств для реализации военно-политических целей. Данный дискурс основывался на ряде искусственно сконструированных (или откровенно сфабрикованных) представлений о внешней политике России, доказывающих наличие у её руководства агрессивных замыслов в отношении Запада и планов по его дестабилизации задолго до украинского кризиса, прежде всего, в частности, на пресловутой «доктрине Герасимова». В нынешнем виде концепт произвольно приравнивает к военным действиям любые методы международной конкуренции и продвижения интересов страны во внешней политике, обосновывает право на максимально жёсткую реакцию в ответ на любые действия, трактуемые как проявления «гибридной войны».
3. Несмотря на серьёзную критику в академической и экспертной среде в адрес теории «гибридной войны» с точки зрения её терминологической и онтологической новизны, практической содержательности и политической эффективности, данный концепт прочно вошёл в западный академический и политический лексикон и выполняет в нём ряд важных функций по конструированию и поддержанию политической конфронтации с Россией, криминализации реальных или предполагаемых действий РФ на международной арене и торпедированию возможностей нормализации отношений с ней. Якобы ведущаяся Россией против Запада и других стран

«гибридная война», позволила представить Россию экзистенциальным противником либерального миропорядка и стимулировать мобилизацию Запада против «российской гибридной угрозы», несмотря на отсутствие осязаемых признаков конфронтационного поведения и готовности выступать в подобной роли со стороны российского руководства. Кроме того, концепт «гибридной войны» позволяет придать текущей конфронтации характер, не ограниченный традиционным межгосударственным военно-политическим противостоянием, охватывающий практически все сферы общественной жизни и предполагающий задействование широкого круга средств и акторов, не имеющих прямой формальной связи с российским государством.

4. Одним из центральных компонентов концепта «гибридной войны» является представление о «российской информационной угрозе» как комбинации технологических, сетевых, информационно-психологических, пропагандистских, дезинформационных, медийных, коммуникативных и иных методов воздействия на общественные процессы западных и других стран, способствующее поддержанию гипертрофированного образа России как врага западного сообщества, обладающего превосходством в современных высокотехнологичных и инновационных инструментах противостояния, в которых у Запада якобы сохраняется критическое отставание или уязвимость. В ходе конструирования «российской информационной угрозы» в западной академической и политической среде был сформирован целостный самостоятельный феномен «российской пропаганды», к которому отнесён и атрибутирован как сугубо российский по своему происхождению и источникам тиражирования целый класс применяемых западными структурами приёмов, манипуляций и методов деструктивного воздействия на общество, а также ряд возникших и бытующих в западном политическом пространстве меседжей, нарративов и идеологем, противоречащих общему либеральному идеологическому курсу.

5. Конструирование «российской информационной угрозы» как важнейшей составляющей «гибридной войны» в западной академической и экспертной мысли проходило три этапа:

- 1) *Подготовительный* (до 2013 г.). При общей скептической оценке российского потенциала «мягкой силы» в научной литературе периодически возникает интерес к силовым возможностям России в кибер- и информационном пространстве в условиях международных кризисов и конфликтов. На примере инцидента вокруг Эстонии в 2007 г. и конфликта в Грузии в 2008 г. формировалось представление о скрытых, неафишируемых попытках российского руководства добиться дезорганизации вероятного или реального противника с помощью кибератак и дезинформационных вбросов. При этом в отдельных, хотя и малозаметных публикациях разнородные явления (кибератаки, пропаганда, полемические выступления и официальная позиция органов публичной власти РФ) начали увязываться в единый инструментарий, якобы подчинённый общей деструктивной стратегии, а правомерность соответствующих реальных или приписываемых действий России предлагалось оценивать по якобы преследуемому результату, а не по их природе.
- 2) *Начальный* (2014-2016 гг.). Характеризуется ускоренным формированием и вынесением в публичное пространство конструкта «российской пропаганды», якобы оказавшей значительное влияние на ход событий украинского кризиса и охватывающей всё русскоязычное пространство и пространство присутствия российских СМИ. Тиражирование данного конструкта происходило, с одной стороны, благодаря усилиям представителей украинского и восточноевропейского медиасообщества, усиленно педалирующих эту тему в СМИ, а, с другой стороны, благодаря публикации и широко освещаемой презентации «реперных» аналитических материалов от имени некоторых западных

«мозговых центров», задавших общий терминологический и оценочный шаблон, репродуцируемый далее в академических и экспертных работах. Таким образом, тематика «российской информационной угрозы» с самого начала развивалась в двух плоскостях – как сфера академического изучения и осмысления и как область практической политики, требующей немедленного контроля и регулирования со стороны государств, межгосударственных структур и гражданского общества. Также на этом этапе произошла резкая переоценка информационного влияния России в сторону изображения его серьёзным оружием и существенной угрозой европейской стабильности.

- 3) *Основной* (2016-2019 гг.), в ходе которого наблюдается значительное расширение «российской информационной угрозы» и её проекция не только на русскоязычное, но и на всё западное публичное пространство в целом. Резкий всплеск академических публикаций с разбором различных аспектов якобы российского подрывного воздействия на западные общества сопровождается включением широкого круга различных негосударственных аналитических структур в процесс регулярного отслеживания, фиксации и опровержения «российских фейков и дезинформации» и выработки рекомендаций по нейтрализации данной угрозы с опорой на опыт Украины и других восточноевропейских стран. В научной литературе происходит закрепление «российской информационной угрозы» в качестве объективного и неоспоримого факта, а единичные попытки оппонировать антироссийскому дискурсу воспринимаются как маргинальные либо стигматизируются как исходящие от агентов «российской пропаганды».
6. Конечным итогом конструирования «российской информационной угрозы» является делегитимация внешней и внутренней политики России как полноправного субъекта международных отношений, имеющего право

отстаивать собственную позицию и преследовать национальные интересы, в том числе, с помощью возможностей «мягкой силы» и публичной дипломатии. Беспрецедентность и тотальный характер якобы ведущейся Россией «гибридной войны» против Запада и всего либерального порядка оправдывают аналогично тотальные меры по отражению данной «угрозы».

Глава 2. Становление институциональной инфраструктуры западной системы противодействия «российской информационной угрозе» после украинского кризиса (2014-2016 гг.)

Во второй и третьей главах работы мы рассмотрим становление и эволюцию институционального измерения системы противодействия «российской информационной угрозе» в том виде, в каком она сформировалась на Западе в 2014-2019 гг. Официальные государственные механизмы в рамках данной системы оперируют на трёх уровнях: 1) национальном, 2) двустороннем либо ситуативном многостороннем и 3) на уровне формальных многосторонних международных организаций. Формирование и развитие институциональной инфраструктуры борьбы с «российской информационной угрозой» на указанных уровнях происходило неравномерно, под действием различных сил и факторов. Причём в процессе её становления отчётливо выделяются два отдельных этапа: период 2014-2016 гг., когда оформление тех или иных структур происходило главным образом под влиянием событий украинского кризиса 2014 г. и его осмысления в западном публичном пространстве, и период 2017-2019 гг., на протяжении которого осуществлялась эволюция и преобразование сформированного институционального каркаса в ответ на перипетии и неожиданный исход президентских выборов в США конца 2016 г.

Мы изучим особенности институционального измерения западной системы противодействия «российской информационной угрозе» на каждом из этих этапов, проследив развитие событий на международном и национальном уровнях, и определим ключевые характерные черты и факторы, под действием которых происходило изменение политики ведущих западных государств и международных институтов.

2.1. Формирование политико-институциональных рамок информационного противодействия России западными межгосударственными объединениями

При всей остроте украинского кризиса и последовавших за ним событий одного только резонанса от них было явно недостаточно для перевода всего комплекса российско-западных отношений из плоскости взаимного отчуждения с элементами сотрудничества в плоскость открытой конфронтации. По этой причине сторонникам жёсткого курса во взаимодействии с Россией требовалось как можно быстрее добиться вынесения и закрепления необходимости повсеместного противодействия нашей стране в политике ведущих западных институтов, даже если это достигалось путём неправдоподобной гиперболизации исходящих от неё угроз.

Предпосылкой для подобной милитаризации послужила, прежде всего, масштабная общественная мобилизация вокруг идеи защиты русского населения как в самой РФ, так и среди соотечественников за рубежом, получившая название Русская весна. Она наглядно показала, что, даже при минимальных ресурсах, выделяемых российским руководством на поддержание русских за рубежом, у Москвы был на тот момент немалый потенциал влияния в виде лояльности этой категории населения и её готовности выступить в поддержку российских объединительных проектов. Причём легитимность этого потенциала была неоспоримой, учитывая провозглашение Западом в предыдущие годы идей гуманитарной интервенции и «ответственности по защите». Для того, чтобы лишить РФ этого, крайне важного, рычага политического влияния, а также сохранить за западным сообществом идеологическую монополию на гуманитарные мотивы во внешней политике, был запущен процесс делегитимации русского нарратива путём приравнивания его к дезинформации и объявления поддержки объединительных проектов со стороны зарубежных русских продуктом «дезинформации и пропаганды». При этом тезис о том, что общественная поддержка политики Кремля является исключительно результатом агрессивной пропаганды и может резко снизиться при условии

предоставления российским гражданам подлинно демократического выбора, уже был утверждён в сознании западной аудитории применительно к внутренней политике Президента РФ В.В. Путина в предыдущие годы¹⁸⁴ и был легко спроецирован во внешнеполитическую плоскость.

Ещё одна задача, решаемая с помощью этих средств, заключалась в блокировании возможных попыток достижения той или иной формы политического компромисса с Россией и признания законности её интересов, как на уровне локальных Минских соглашений, так и в отношении более широких, всеобъемлющих форматов, касающихся вопросов европейской или глобальной безопасности. По мере развития этого процесса продвигающие его силы получили возможность добиться более масштабной цели – перестроить весь механизм политики западных государств и институтов в отношении России, исключив из него любые кооперативные импульсы, исходящие даже из собственных экономических и стратегических интересов.

Угроза, якобы исходящая от российской пропаганды и дезинформации и усиленная концептом «гибридной войны», выступила эффективным катализатором конфронтационных тенденций в западном сообществе на уровне массового сознания и экспертно-академического мейнстрима. Но её реификация на официальном государственном и межгосударственном уровне потребовала определённых усилий, чтобы представить «кремлёвскую пропаганду» не только как вызов в рамках конкуренции за влияние на население стран «общего соседства», но и как полноценную угрозу безопасности западного сообщества, способную подорвать существующий международный порядок в Европе и в мире.

Совет Европы

¹⁸⁴ Tsygankov A. P. The dark double: the American media perception of Russia as a neo-Soviet autocracy, 2008–2014 / A. P. Tsygankov // Politics. 2017. Vol. 37, No. 1. P. 31.

На начальном этапе разворачивания «постмайданного» периода украинского кризиса и перерастания его в подавление русского восстания в юго-восточных областях немалую роль в милитаризации информационной сферы сыграла позиция ведущих международных организаций, призванных следить за соблюдением демократических ценностей и прав человека. Квалификация ими прорусского нарратива о событиях февраля-марта 2014 г. как допустимой, оправданной и заслуживающей уважения точки зрения могла бы предотвратить или, по крайней мере, затормозить нагнетание истерии вокруг якобы «российской пропаганды» как движущей силы антимайданного сопротивления в Крыму и других регионах. Однако вместо этого данные организации либо заняли деструктивную позицию, подыгрывая заинтересованным в развязывании конфронтации силам, либо устранились от однозначной оценки, позволив данным силам беспрепятственно тиражировать свою интерпретацию происходящего как единственно верную.

В конце марта 2014 г. Консультативный комитет Рамочной конвенции о защите прав национальных меньшинств направил на Украину специальную миссию, которая в своих выводах указала, что положение национальных меньшинств в результате февральского переворота никак не изменилось и угроза негативных изменений отсутствует¹⁸⁵. Опираясь на эти выводы, докладчицы Мониторингового комитета Совета Европы М. Репс (Эстония) и М. де Пурбэ-Ланден (Швеция) 8 апреля 2014 г. представили в Парламентской ассамблее доклад о функционировании демократических институтов на Украине, на основании которого 9 апреля 2014 г. ассамблея приняла резолюцию 1988¹⁸⁶, содержащую, в том числе, такие положения:

¹⁸⁵ Reps M. Recent developments in Ukraine: threats to the functioning of democratic institutions / M. Reps, M. de Pourbaix-Lundin // Report of the Committee on the Honouring of Obligations and Commitments by Member States of the Council of Europe (Monitoring Committee). Parliamentary Assembly of the Council of Europe. 8 April 2014. Doc. 13482. P. 23-27. URL: <http://semanticpace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbmQvbnNveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0yMDcxMiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRClBVC1YUwyUERGLnhzbA==&xslparams=ZmlsZWlkPTIwNzEy> (дата обращения: 11.11.2020)

¹⁸⁶ Недавние события на Украине: угрозы функционированию демократических институтов (неофициальный перевод) // Резолюция Парламентской ассамблеи Совета Европы. 9 апреля 2014 г. № 1988. URL: [https://www.coe.int/T/r/Parliamentary_Assembly/\[Russian_documents\]/\[2014\]/April2014/Res1988_rus.asp](https://www.coe.int/T/r/Parliamentary_Assembly/[Russian_documents]/[2014]/April2014/Res1988_rus.asp) (дата обращения: 11.11.2020)

«13. Частые и необоснованные сообщения о нарушениях прав меньшинств на Украине, а также создание некоторыми национальными и зарубежными СМИ негативного образа новой власти в Киеве негативно повлияли на межэтнические отношения на Украине и, в конечном счете, – на единство и стабильность страны. Мы призываем все СМИ воздерживаться от таких необоснованных сообщений и освещать события в стране и в её регионах беспристрастно и опираясь на факты. Мы призываем власти воздерживаться от любой цензуры СМИ. Мы призываем власти Украины пересмотреть решение прекратить вещание некоторых телевизионных каналов в стране и воздерживаться от любой цензуры СМИ.

15. По мнению Ассамблеи, никакие аргументы, приводимые Российской Федерацией для обоснования своих действий, не подтверждаются фактами и свидетельствами. Не было никакого ультраправого переворота с целью захвата центральной власти в Киеве, не было какой-либо непосредственной угрозы правам этнического российского меньшинства в стране, в том числе, или особенно, в Крыму. Учитывая, что ни сепаратизм, ни присоединение к Российской Федерации не преобладали в политической повестке крымского населения и не имели широкой поддержки до российской военной интервенции, Ассамблея полагает, что кампания за отделение и присоединение к Российской Федерации была спровоцирована и инспирирована российскими властями под прикрытием военной интервенции.

На следующий день, 10 апреля 2014 г., ПАСЕ принимает резолюцию 1990¹⁸⁷ об ограничениях полномочий российской делегации, где озвучивает аналогичную позицию:

«8. Ассамблея выражает сожаление в связи с тем, что неподтверждённые сообщения о якобы имевших место нарушениях прав русскоязычного меньшинства и обвинения в адрес киевских властей в приверженности крайне

¹⁸⁷ Пересмотр по существенным основаниям ранее утвержденных полномочий российской делегации (неофициальный перевод) // Резолюция Парламентской ассамблеи Совета Европы. 10 апреля 2014 г. № 1990. URL: [https://www.coe.int/T/r/Parliamentary_Assembly/\[Russian_documents\]/\[2014\]/April2014/Res1990_rus.asp](https://www.coe.int/T/r/Parliamentary_Assembly/[Russian_documents]/[2014]/April2014/Res1990_rus.asp) (дата обращения: 11.11.2020)

правым взглядам использовались в политических целях многими высокопоставленными официальными лицами и членами парламента Российской Федерации в публичных выступлениях.

9. Ассамблея крайне обеспокоена ситуацией со свободой СМИ и свободой выражения мнений в России, в особенности предвзятым освещением событий на Украине и даже манипуляциями, которые в значительной степени способствовали межэтнической нестабильности в стране, а также подавлением публичной дискуссии и критики. Особую обеспокоенность вызывает преследование независимых СМИ, в том числе онлайн-новых, и журналистов».

Указанные положения резолюций ПАСЕ не просто оспаривали прорусский нарратив, но прямо называли его инспирированным и неподтверждённым, хотя и не содержали пока что риторики в категориях пропаганды и дезинформации. После этого Совет Европы к данному вопросу долгое время не возвращался, хотя регулярно принимал заявления с осуждением ситуации с правами человека в Российской Федерации и в Крыму.

ОБСЕ

Если такая позиция ПАСЕ не вызывала особого удивления вследствие давнего критического отношения к нашей стране, то от Организации по безопасности и сотрудничеству в Европе предположительно можно было ожидать большей объективности.

На начальном этапе конфликта подключение ОБСЕ и отдельных её органов рассматривалось практически всеми заинтересованными сторонами в положительном ключе. В отношении информационного компонента разворачивающегося противостояния основной инстанцией, к которой апеллировали участники конфликта, был Представитель ОБСЕ по свободе СМИ Дунья Миятович.

Ещё во время «евромайдана» Д. Миятович не раз делала заявления, осуждающие случаи применения силы против журналистов и призывающие к их

тщательному расследованию¹⁸⁸. После переворота в феврале 2014 г. она сперва осудила ограничение вещания российских каналов новыми украинскими властями, но затем заняла менее однозначную позицию, посчитав подобное ограничение и блокирование недопустимым только в случае отсутствия законного решения об этом.

Полноценное подключение ОБСЕ к урегулированию затруднялось тем, что большинство участников не были настроены на компромиссное разрешение конфликта, стремясь использовать его как инструмент для подкрепления своих позиций и оценок, в том числе, путём получения поддержки от международных структур. Привлечение Представителя ОБСЕ по свободе СМИ воспринималось украинской стороной как способ придать международное измерение вопросу о деструктивном влиянии «российской пропаганды», тогда как её оппоненты указывали на ограничительные меры, введённые новой украинской властью в отношении российских и пророссийских СМИ на Украине.

Дунья Миятович проявляла немалую активность в первые месяцы конфликта, пытаясь сохранять объективность и непредвзятость. Так, 15 апреля 2014 г. от её имени было обнародовано специальное заявление о пропаганде во время конфликта¹⁸⁹, в котором говорилось, что ввиду расплывчатости термина «пропаганда» стремление её запретить нарушает международные нормы в области защиты свободы слова и свободы СМИ, поэтому государствам-участникам ОБСЕ рекомендовалось воздержаться как от использования СМИ в манипулятивных целях, так и от введения новых ограничений на работу СМИ, а противодействие пропаганде обеспечивать путём усиления плюрализма и свободы СМИ и повышения медиаграмотности граждан. Кроме того, Представитель ОБСЕ указывала, что в соответствии с обязательствами в рамках

¹⁸⁸ См. например Нападения на журналистов в Украине должны быть прекращены, сказала Представитель ОБСЕ по вопросам свободы СМИ и выразила готовность посетить Киев // ОБСЕ. 22 января 2014 г. URL: <https://www.osce.org/ru/fom/110465> (дата обращения: 11.11.2020)

¹⁸⁹ Заявление Представителя ОБСЕ по вопросам свободы СМИ о пропаганде во время конфликта // ОБСЕ. 15 апреля 2014 г. URL: <https://www.osce.org/ru/fom/117734> (дата обращения: 11.11.2020)

ОБСЕ только те ограничения, которые преследуют законную цель и чётко определены законом, являются приемлемыми¹⁹⁰.

Тем самым, Миятович развивала свою компромиссную позицию, выраженную в её твиттере в конце марта¹⁹¹, допускавшую закрытие СМИ на «законном основании», но уходившую от рассмотрения вопроса об объективности «законного основания». В дальнейшем Мьятович также высказывалась против ограничений, накладываемых на свободу слова киевскими властями, например, в сентябре 2015 г. выступила против включения украинским Президентом П.А. Порошенко журналистов в список 400 лиц, которым запрещён въезд на Украину¹⁹², а в апреле 2016 г., после подписания П.А. Порошенко запрета на российские информационные программы и фильмы, созданные с 1 января 2014 г., она призвала Киев воздержаться от ограничений на информацию и масс-медиа¹⁹³.

Как видим, в лице данного представителя ОБСЕ сохраняла общую видимость объективности, однако политический контекст ситуации парализовал конструктивные функции данного международного института, и он не смог воспрепятствовать становлению системы информационного противодействия России со стороны НАТО и ЕС.

НАТО

Как мы уже писали в первой главе, Североатлантический альянс сыграл роль локомотива в вынесении на международную повестку дня концепта «гибридной войны» и «гибридных угроз», признав их вполне реальными и актуальными вызовами безопасности для НАТО в целом и зафиксировав это в документах саммита в Уэльсе 4-5 сентября 2014 г.

¹⁹⁰ Там же.

¹⁹¹ Mijatovic D. Вовсе нет противоречия: <http://osce.org/ru/fom/116314> и <http://osce.org/ru/fom/116900> запрет ТВ каналов без законного основания – вот форма цензуры // Twitter. URL: https://twitter.com/Dunja_Mijatovic/status/449537285592477697 (дата обращения: 11.11.2020)

¹⁹² Poroshenko Should Remove Journalists from Kiev Blacklist // Sputnik International. 17 September 2015. URL: <https://sputniknews.com/society/201509171027130831/> (дата обращения: 11.11.2020)

¹⁹³ OSCE Urges Kiev to Refrain From Media Freedom Ban // Sputnik International. 22 April 2016. URL: <https://sputniknews.com/europe/201604221038452243-osce-ukraine-media-freedom/> (дата обращения: 11.11.2020)

Немалый личный вклад в распространение дискурса о «российский гибридной агрессии» внесли Генеральный секретарь НАТО Йенс Столтенберг и высшие руководители интегрированного командования альянса. Они продолжали поддерживать этот дискурс в публичном пространстве даже при отсутствии новых формальных поводов для обвинения России в информационных атаках. Например, 25 марта 2015 г., выступая на открытии Семинара НАТО по Трансформации, Й. Столтенберг всецело интерпретировал происходящий конфликт в рамках концепции «гибридной войны»: *«Россия использует прокси-отряды, силы специального назначения без знаков различия, методы запугивания и пропаганду – всё для того, чтобы напустить тумана, скрыть свои истинные цели в этом конфликте и сохранить иллюзию невмешательства. Альянс должен быть готов действовать в этой новой реальности. Нужно готовиться к встрече с гибридной войной, учиться противостоять ей и защищаться от неё»*¹⁹⁴. Он указал, что кибервойна является необходимым элементом противостояния гибридным методам.

В оформлении институциональной инфраструктуры системы информационного противодействия России НАТО тоже взяла на себя пионерскую роль, инициировав выделение особых функций по организации такого противодействия и запустив формирование соответствующих им структурных единиц. При этом Альянс не торопился с полноценной институционализацией сферы «гибридных угроз» в своей политической и военной структуре, хотя её закрепление в комплексе стратегического и оперативного планирования НАТО продвигалось довольно быстро. Уже весной-летом 2015 г. Альянс провёл в Польше и Прибалтике серию военных учений «Благородный прыжок», в ходе которых отрабатывался сценарий отражения угрозы вторжения иррегулярных войск в Польшу¹⁹⁵.

¹⁹⁴ Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar // NATO. 25 March 2015. URL: https://www.nato.int/cps/en/natohq/opinions_118435.htm (дата обращения: 11.11.2020)

¹⁹⁵ Oğuz Ş. The new NATO: Prepared for Russian hybrid warfare? / Ş. Oğuz // Insight Turkey. 2016. Vol. 18. No. 4. P. 174.

На момент разворачивания украинского кризиса в рамках НАТО уже действовал упомянутый ранее Центр по сотрудничеству в сфере киберобороны в Таллине¹⁹⁶ – межгосударственный военный орган, аффилированный с НАТО, но не входящий в структуру интегрированного командования Альянса и не подчиняющийся никакому другому органу НАТО. Изначально Центр был основан семью членами НАТО – Эстонией, Латвией, Литвой, Германией, Италией, Испанией и Словакией – в мае 2008 г. В октябре того же года Североатлантический совет решил присвоить Центру полноценную аккредитацию при НАТО в качестве международного военного органа без прямого подчинения интегрированному командованию. На данный момент в работе Центра принимают участие 21 страна, в том числе европейские «нейтралы» – Швеция, Австрия и Финляндия.

С марта 2014 г. Центр подключается к работе по организации сектора кибербезопасности новой украинской власти и становится объектом атаки со стороны предположительно пророссийских хакеров. Также под эгидой данного Центра иницируются¹⁹⁷ экспертные мероприятия и исследования, привлекающие внимание к проблеме используемых Россией инновационных методов ведения войны против Украины.

Однако данный Центр занимается преимущественно техническими вопросами защиты киберпространства, поэтому параллельно для решения проблем непосредственно в сфере пропаганды и дезинформации наряду с ним в Риге создаётся Центр передового опыта НАТО в области стратегических коммуникаций¹⁹⁸. Он был основан в январе 2014 г. как национальный институт при министерстве обороны Латвии. 1 июля 2014 г. учредительные документы центра как органа международного сотрудничества были поданы в штаб Командования НАТО по трансформации в Норфолке представителями Эстонии,

¹⁹⁶ The NATO Cooperative Cyber Defence Centre of Excellence. URL: <https://ccdcoe.org/>

¹⁹⁷ Cyber War in Perspective: Russian Aggression against Ukraine / K. Geers (ed.). NATO CCD COE Publications, Tallinn 2015. 175 p. URL: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf (дата обращения: 11.11.2020)

¹⁹⁸ NATO Strategic Communications Centre of Excellence. URL: <https://www.stratcomcoe.org>

Германии, Италии, Латвии, Литвы, Польши и Великобритании. Первое заседание наблюдательного комитета Центра состоялось 24-25 июля. 1 сентября 2014 г. создание Центра как военного органа НАТО, не входящего в структуру интегрированного командования, было одобрено Североатлантическим советом, а несколько дней спустя на саммите НАТО в Уэльсе было признано весомым вкладом в развитие стратегических коммуникаций Альянса.

Примечательно, что оба центра были созданы не в результате политического консенсуса всех государств-членов Альянса, а вследствие односторонней инициативы отдельных стран, которая получила своеобразный мандат НАТО уже постфактум. Статус военных органов вне интегрированного командования также придаёт их деятельности несколько полуофициальный характер, когда они могут проводить в жизнь различные проекты и мероприятия от имени НАТО, организовывать учения, оказывать поддержку регулярным политическим и военным органам Альянса, распоряжаться бюджетом и издавать материалы, не будучи подотчётными регулярному стратегическому командованию и не подвергаясь политическим ограничениям, обусловленным процедурой принятия решений в НАТО. При этом бюджет центров формируется за счёт взносов участвующих в нём государств, которые и определяют их текущие цели и задачи и утверждают регулярные отчёты об их выполнении. Соответственно, направление кадров для работы в центрах осуществляется лишь от участвующих государств, что непосредственным образом сказывается на общем характере их деятельности и её политических последствиях.

Заявленной миссией Центра стратегических коммуникаций является скоординированное и своевременное использование коммуникационных средств и возможностей альянса для реализации его политических целей. Кроме того, Центр призван способствовать повышению общественной осведомлённости о деятельности НАТО и усилению её позитивного восприятия обществами государств-членов альянса и широкой международной общественностью.

На начальном этапе деятельность Центра, как свидетельствуют его ежегодные публичные отчёты¹⁹⁹, включала сугубо образовательные и исследовательские проекты. Однако среди этих проектов было немало практических тренингов, предназначенных для обучения военных, экспертов и журналистов стран НАТО методам выявления и нейтрализации «российской дезинформации». Так, 8 мая 2015 г. посол Канады в Латвии и латвийский Министр обороны открыли в Риге профинансированную канадским Правительством в рамках Центра стратегических коммуникаций программу обучения²⁰⁰ передовым контрпропагандистским методам, нацеленную на противодействие «российской пропаганде» в Восточной Европе.

Помимо деятельности в рамках стационарных центров, изучение феномена «гибридных войн» было запущено в рамках Кампании по развитию многостороннего потенциала (*Multinational Capability Development Campaign*) – специальной исследовательской структуры при Командовании НАТО по трансформации в Норфолке, разрабатывающей инновационные методы оперативного взаимодействия членов НАТО и партнёров в ходе проведения многосторонних операций в глобальных «общих пространствах», в том числе в информационном и киберпространстве²⁰¹. В рамках плана работы данной структуры на 2015-2016 гг. был развёрнут проект²⁰² по исследованию методов противодействия «гибридным войнам», возглавляемый на том этапе представителями экспертной среды Норвегии и включающий в качестве стран-участниц в первую очередь европейских «нейтралов» – Австрию, Швейцарию, Финляндию.

¹⁹⁹ Report for the period from 1 January 2015 to 31 December 2015 // NATO Strategic Communications Centre of Excellence. 31 March 2016. URL: <https://www.stratcomcoe.org/download/file/fid/75507> (дата обращения: 11.11.2020); Report for the period from 1 January 2016 to 31 December 2016 // NATO Strategic Communications Centre of Excellence. 31 March 2017. URL: <https://www.stratcomcoe.org/download/file/fid/75507> (дата обращения: 11.11.2020)

²⁰⁰ Countering propaganda: NATO spearheads use of behavioural change science // NATO Strategic Communications Centre of Excellence. 12 May 2015. URL: <https://stratcomcoe.org/countering-propaganda-nato-spearheads-use-behavioural-change-science> (дата обращения: 11.11.2020)

²⁰¹ The Multinational Capability Development Campaign (MCDC) // NATO. February 2019. URL: https://www.act.nato.int/images/stories/media/opex/2019_MCDC_FUTLEAD.pdf (дата обращения: 11.11.2020)

²⁰² Multinational Capabilities Development Campaign (MCDC) 15-16. COUNTERING HYBRID WARFARE (CHW) // MCDC. 9 November 2015. URL: https://wss.apan.org/public/MCDCpub/MCDC_2015_16/Shared Documents/MCDC_15-16_Project_Sheet_CHW_09NOV15.pdf (дата обращения: 11.11.2020)

Несмотря на серьёзную активность, развёрнутую на информационном фронте, сторонники ужесточения политики в отношении России не собирались ограничиваться уже достигнутыми масштабами, а задались целью добиться чётко артикулированного политического обязательства НАТО распространить на информационное пространство подход в духе коллективной обороны, включив его таким образом в стратегический ареал Альянса. Эти усилия интенсифицировались в ходе подготовки к саммиту НАТО в Варшаве.

Для педалирования необходимости создания отдельных структур и утверждения конкретных обязательств по защите от «информационной агрессии России» активно использовалась трибуна Парламентской ассамблеи НАТО. Заметным событием в этом плане стал доклад экс-министра иностранных дел Польши Витольда Ващиковского на заседании комитета Парламентской Ассамблеи НАТО под названием «Битва за сердца и умы: противодействие пропагандистским атакам на евроатлантическое сообщество»²⁰³, опубликованный в октябре 2015 г.

Помимо этого, немало усилий со стороны НАТО было направлено на то, чтобы вовлечь Европейский союз в процесс построения и функционирования инфраструктуры конфронтации с Россией в сфере «гибридных угроз» и добиться от него конкретных обязательств в этом отношении, подкреплённых как финансово, так и институционально. Основным аргументом для этого служила большая оснащённость и компетентность ЕС в сфере невоенных и гражданских средств безопасности²⁰⁴. Европейские функционеры при этом, признавая насущность данного вопроса, не спешили брать на себя инициативу, ожидая пока Альянс определится со своей ролью в его продвижении.

²⁰³ Waszczykowski W. The Battle for the Hearts and Minds: Countering Propaganda Attacks Against the Euro-Atlantic Community / W. Waszczykowski // Report for the Committee on the Civil Dimension of Security, NATO Parliamentary Assembly. 20 October 2015. URL: <https://www.nato-pa.int/document/2015-164-cdsdg-15-e-fin-bis-russian-propaganda-waszczykowski-report> (дата обращения: 11.11.2020)

²⁰⁴ Raik K. A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity / K. Raik, P. Järvenpää // International Centre for Defence and Security Report. Tallinn, 2017. URL: https://icds.ee/wp-content/uploads/2018/ICDS_Report_A_New_Era_of_EU-NATO.pdf (дата обращения: 11.11.2020)

На совещании министров иностранных дел НАТО в декабре 2015 г. была принята Стратегия противодействия «гибридным угрозам»²⁰⁵, о чём генсек Й. Столтенберг сообщил на совместной пресс-конференции с Высоким представителем ЕС по внешним делам и политике безопасности Федерикой Могерини, подчеркнув, что *«тесное сотрудничество между ЕС и НАТО [в этой области] может сделать нашу помощь более фокусированной и более эффективной»*²⁰⁶. Это запустило процесс согласования политики в сфере противодействия «гибридным угрозам» внутри Евросоюза и между ЕС и НАТО в преддверии Варшавского саммита НАТО.

Данный процесс продвигался не без проблем. Так, 27 января 2016 г. агентство *Reuters* опубликовало сообщение об утечке 23-страничного документа, ставшего частью длительной дискуссии в НАТО, о намерении НАТО и ЕС совместно бороться с российской дезинформацией и открытой пропагандой путём создания новой более мощной коммуникационной секции и рассекречивания более чувствительных материалов. Альянс изучал возможность разработать *«стратегические нарративы, которые приводят к согласованным словам и действиям ... соответствующим образом адаптированные и культурно настроенные, чтобы резонировать со всей аудиторией и противостоять противоположным нарративам»*. Представители альянса в тот момент поясняли, что документ ещё не означает окончательного решения, его предстоит обсудить в разных странах и принять окончательную стратегию на грядущем саммите НАТО. Согласно сообщениям в СМИ, Великобритания поддерживала такой подход, но США его пока полностью не разделяли и не считали, что противостоять одной пропаганде следует с помощью другой пропаганды. В документе указывалось также на необходимость более быстрого рассекречивания спутниковых изображений (в частности, фотографии

²⁰⁵ Полный текст Стратегии не обнародован, но общие её принципы изложены на веб-странице НАТО, см. NATO's response to hybrid threats // NATO. 8 August 2019. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (дата обращения: 11.11.2020)

²⁰⁶ Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini // NATO. 1-2 December 2015. URL: https://www.nato.int/cps/en/natohq/opinions_125361.htm (дата обращения: 11.11.2020)

российских дислокаций) и других разведданных для борьбы с дезинформацией и отмечалась недостаточная масштабность т. н. стратегических коммуникаций НАТО, включающих координацию различных средств информирования общественности, а также технологии психологических операций, призванных влиять на общественное мнение²⁰⁷.

Как можно понять из сообщения *Reuters*, основная дискуссия внутри Альянса на том этапе разворачивалась вокруг вопроса о возможности и допустимости использования военных средств противодействия в рамках ст. 5 Вашингтонского договора в ответ на угрозы невоенного «гибридного» характера²⁰⁸. Поскольку на Варшавском саммите планировалось «послать чёткий сигнал России» путём создания и постоянного размещения в Польше и Прибалтике дополнительных четырёх многонациональных батальонов, сторонникам жёсткого курса было важно добиться закрепления возможности использования этих сил даже в случае не прямой «гибридной» агрессии и обеспечить поддержку европейских союзников в этом вопросе.

Однако прогресс на этом направлении оказался ограниченным. Решения саммита НАТО в Варшаве 8-9 июля 2016 г., в целом отвечая ожиданиям «ястребов», оставляли немалое пространство для манёвра. С одной стороны, в итоговом коммюнике саммита²⁰⁹ киберпространство было выделено в качестве «оперативной сферы» (*domain of operations*) Альянса, в которой он должен обеспечить коллективную оборону так же эффективно, как на земле, воде и в воздухе, поэтому его следует интегрировать в оперативное планирование НАТО (п. 70). Для подкрепления этого положения был принят специальный документ «Обязательства по обеспечению киберобороны»²¹⁰, в котором отмечалось быстрое нарастание киберугроз и формулировалась приверженность совместно

²⁰⁷ Emmott R. NATO looks to combat Russia's 'information weapon': document / R. Emmott // Reuters. 27 January 2016. URL: <https://www.reuters.com/article/us-nato-reform-idUSKCN0V51RU> (дата обращения: 11.11.2020)

²⁰⁸ Oğuz Ş. The new NATO: Prepared for Russian hybrid warfare? / Ş. Oğuz // Insight Turkey. 2016. Vol. 18. No. 4. P. 176.

²⁰⁹ Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 // NATO. 9 July 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (дата обращения: 11.11.2020)

²¹⁰ Cyber Defence Pledge // NATO. 8 July 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133177.htm (дата обращения: 11.11.2020)

«в первоочередном порядке усилить и укрепить киберзащиту национальных сетей и инфраструктур». Кроме того, в коммюнике отдельно упоминались вызовы гибридной войны, для противостояния которым Альянс разработал специальную стратегию и реалистичные планы действий вплоть до возможности задействовать гарантии статьи 5 Вашингтонского договора (п. 72). С другой стороны, говорилось, что главная ответственность за реагирование на гибридные угрозы и атаки возлагается на подвергшееся им государство, тогда как НАТО готово лишь оказать помощь любому союзнику на любой стадии гибридной кампании. Альянс должен быть готов противостоять гибридной агрессии в рамках своей коллективной обороны, но не обязан это делать автоматически, а задействовать статью 5 Вашингтонского договора можно только решением Североатлантического совета, то есть всех государств-членов НАТО единогласно.

Вопрос о специальном усилении стратегических коммуникаций НАТО в документах Варшавского саммита затронут крайне поверхностно, их координация и интеграция с другими базовыми направлениями деятельности НАТО осталась за рамки непосредственно работы саммита так же, как, собственно, информационная сфера. Официальный дискурс руководящих лиц Альянса на этот счёт сводится к позиции о том, что НАТО необходимо отвечать на пропаганду не другой пропагандой, а излагать правдивые факты и раскрывать истинное положение дел²¹¹.

В то же время в отношении борьбы с «гибридными угрозами» Альянсу удалось добиться некоторого продвижения. Так, к Варшавскому саммиту Евросоюз подошёл уже имея утверждённую Общую рамочную программу по противодействию «гибридным угрозам» и созданный на его основе стационарный орган в этой сфере – Центр анализа «гибридных угроз» в структуре Разведывательного и ситуационного центра Европейской службы

²¹¹ См. например Press conference by NATO Secretary General Jens Stoltenberg ahead of Meetings of NATO Defence Ministers // NATO. 25 October 2016. URL: https://www.nato.int/cps/en/natohq/opinions_136414.htm (дата обращения: 11.11.2020)

внешних действий. Это позволяло вести речь об организации регулярного обмена в данной сфере. Так, в ходе Варшавского саммита была принята совместная декларация председателя Европейского совета, главы Еврокомиссии и Генерального секретаря НАТО²¹², обозначающая основные векторы сотрудничества между ЕС и НАТО на ближайшую перспективу. Противодействие «гибридным угрозам» фигурировало в нём среди наиболее срочных направлений сотрудничества между двумя организациями, включая укрепление устойчивости, совместную работу в сфере анализа, предотвращения и раннего обнаружения, своевременное взаимное информирование и обмен разведданными, сотрудничество в сфере стратегических коммуникаций, выработку скоординированных процедур реагирования на подобные угрозы и проведение совместных учений по их отражению.

Такой формат декларации, сделанной не от имени двух организаций, а от имени их высших должностных лиц, был выбран в связи с тем, что он позволял избежать необходимости в поддержке данного документа всеми государствами-членами. Но при этом заявленные в нём цели и задачи стали основанием для целого спектра конкретных решений и мероприятий, а также регулярных докладов о прогрессе в их выполнении. Сама тематика «гибридных угроз» была вследствие этого превращена в главный предмет сотрудничества между НАТО и Европейским союзом.

В декабре 2016 г. на базе Варшавской совместной декларации в таком же формате заявления трёх должностных лиц был принят перечень задач для имплементации обозначенных в декларации целей²¹³. В сфере противодействия «гибридным угрозам» были поставлены задачи создать в 2017 г. специальный Европейский центр противодействия «гибридным угрозам» и поощрять участие в нём со стороны государств-членов ЕС и НАТО; наладить к маю 2017 г.

²¹² Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization // NATO. 8 July 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133163.htm (дата обращения: 11.11.2020)

²¹³ Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization // NATO. 6 December 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_138829.htm (дата обращения: 11.11.2020)

регулярный и своевременный обмен критической информацией между Центром анализа «гибридных угроз» ЕС и соответствующим органом НАТО, который ещё предстоит создать; наладить сотрудничество между ЕС и НАТО в сфере стратегических коммуникаций, в том числе сообщать о случаях дезинформации, направленных против ЕС и НАТО в соцсетях, активизировать усилия по укреплению стратегических коммуникаций стран-партнёров с помощью совместных тренингов и передачи опыта, поощрять взаимодействие между Центром передового опыта НАТО и Оперативными группами ЕСВД Евросоюза; синхронизировать параллельные антикризисные меры в ответ на возникающие «гибридные угрозы»; сформировать команды экспертов для скоординированного оказания поддержки государствам-членам по их просьбе на любой стадии кризиса, вызванного «гибридными угрозами»; интенсифицировать контакты между штабами.

Благодаря подобным действиям Альянс оформил свою ведущую роль в определении политической и стратегической повестки дня в сфере «гибридных угроз», стимулируя Евросоюз взять на себя ряд конкретных обязательств в этой сфере и выделить значительные ресурсы на их выполнение.

Таким образом, сыграв инициативную роль в дискурсивном введении и документальном закреплении на политическом и стратегическом уровнях концепта «гибридной войны» и «гибридных угроз», НАТО, тем не менее, предприняла лишь ограниченные практические меры для их отражения. Обозначив дезинформацию и пропаганду как оружие «гибридной войны», Альянс не торопился выделить их в самостоятельную сферу политических обязательств и закрепить в своей институциональной архитектуре, а ключевые функции в этой сфере были возложены на пресс-службу НАТО и полуофициальный Центр по стратегическим коммуникациям в Риге.

Европейский союз

Имиджевые и коммуникационные преимущества Европейского союза традиционно считались достаточно весомыми и позволяющими оказывать политическое влияние на общественное мнение третьих стран. Современная

Россия, по мнению многих европейских экспертов²¹⁴ в домайдаанный период, не могла сформировать позитивный образ у внешней аудитории и даже на постсоветском пространстве сохраняла некоторое информационное влияние только благодаря рудиментарной советской ностальгии старшего поколения. Прозападные украинские эксперты часто указывали на российское присутствие в украинском медиапространстве как на вызов украинскому суверенитету и европейскому выбору²¹⁵. Однако пока между Россией и Евросоюзом сохранялась общая кооперативная или, по крайней мере, неконфликтная атмосфера отношений, российское информационное влияние за рубежом не рассматривалось европейской стороной как политическая проблема. Тем более, что российские СМИ долгое время освещали евроинтеграционную тематику в довольно положительном ключе.

Толчком к усилению конкуренции в информационной сфере стало учреждение Евросоюзом программы Восточного партнёрства и поставленная в контексте данной программы задача заключения с сопредельными странами СНГ соглашений об ассоциации и зоне свободной торговли, выступающих препятствием на пути дальнейшего углубления постсоветской интеграции в рамках Таможенного, а затем Евразийского экономического союза. Стремление добиться подписания подобного соглашения с Украиной и не допустить, таким образом, её сближения с Таможенным союзом заставило европейских функционеров усилить давление на украинский правящий класс и подключить к этому давлению общественное мнение. Но, вопреки ожиданиям, общественная поддержка соглашения об ассоциации на Украине не была настолько подавляющей, чтобы оказать решающее влияние на колеблющиеся власти. И

²¹⁴ См. например Makarychev A. Hard Questions About Soft Power: A Normative Outlook at Russia's Foreign Policy / A. Makarychev // DGAPanalyse. 2011. No. 10. 7 p. URL: https://dgap.org/system/files/article_pdfs/2011-10_DGAPanakt_Makarychev_www.pdf (дата обращения: 11.11.2020); Ćwiek-Karpowicz Ja. Limits to Russian Soft Power in the Post-Soviet Area / Ja. Ćwiek-Karpowicz // DGAPanalyse. 2012. No. 8. 16 p. URL: https://dgap.org/system/files/article_pdfs/2012-08_DGAPana_C%CC%81wiek-Karpowicz_www_0.pdf (дата обращения: 11.11.2020); Simons G. Russian public diplomacy in the 21st century: Structure, means and message / G. Simons // Public Relations Review. 2014. Vol. 40, No. 3. P. 440-449.

²¹⁵ Bogomolov A. A Ghost in the Mirror: Russian Soft Power in Ukraine / A. Bogomolov, O. Lytvynenko // Chatham House Briefing Paper. 1 January 2012. URL: [https://www.chathamhouse.org/sites/default/files/public/Research/Russia and Eurasia/0112bp_bogomolov_lytvynenko.pdf](https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0112bp_bogomolov_lytvynenko.pdf) (дата обращения: 11.11.2020)

даже почти единодушная массированная кампания украинских СМИ по продвижению ассоциации с ЕС и критике любых проектов интеграции с Россией в период 2012-2013 гг. не принесла желаемых результатов: к концу октября 2013 г. общественная поддержка подписания ассоциации снизилась даже по сравнению с июлем того же года и едва достигала 50% респондентов²¹⁶, тогда как поддержка общего вектора на вступление в Европейский союз по стране едва превышала 40% опрошенных²¹⁷.

Сторонники скорейшего подписания соглашения в среде украинских чиновников и экспертов объясняли такие тенденции чрезмерным присутствием российских СМИ, особенно телеканалов, в украинском информационном пространстве и тиражированием ими якобы некорректной информации о евроинтеграции в целом и соглашении об ассоциации в частности. Собственно, именно на этой стадии и начинает формироваться дискурс о том, что альтернативный взгляд на продвигаемые Евросоюзом инициативы является пропагандой и дезинформацией, нацеленной на подрыв геополитического влияния ЕС путём дискредитации его ценностно-символической привлекательности. Акцентируя и нередко гиперболизируя возможные негативные последствия для евроинтеграционного объединения от поддержания и распространения пророссийской позиции, заинтересованные местные игроки тем самым активно подталкивали органы ЕС к тому, чтобы включиться в пропагандистскую борьбу с Россией за влияние на общественное мнение стран так называемого «общего соседства».

Отдельные европейские политики и функционеры ЕС довольно рано включились в эту борьбу, однако коммунитарные институты долго оставались в стороне от данного процесса. И только на волне «евромайдана» в Киеве

²¹⁶ Ukrainian support for EU association agreement declines // Deutsche Welle. 13 July 2013. URL: <https://www.dw.com/en/ukrainian-support-for-eu-association-agreement-declines/a-17189085> (дата обращения: 11.11.2020)

²¹⁷ Яким шляхом іти Україні — до якого союзу приєднуватись? // Київський міжнародний інститут соціології. 3 жовтня 2013. URL: <http://www.kiis.com.ua/?lang=ukr&cat=reports&id=196&page=1&y=2013&m=10>, https://dif.org.ua/uploads/pdf/1407765948_3132.pdf (дата обращения: 11.11.2020)

представительство ЕС на Украине начало выпускать специальные памятки²¹⁸, развеивающие «мифы об ассоциации», а фактически нивелирующие любую критику в адрес этого документа как необоснованную и политически ангажированную. Двумя другими поворотными событиями, подстегнувшими резонанс вокруг тематики российской дезинформации в Евросоюзе стали присоединение Крыма и падение малазийского «Боинга» в Донбассе 17 июля 2014 г. Антироссийски настроенные эксперты использовали освещение этих событий в российских СМИ как подтверждение их необъективности и недобросовестности вследствие участия в запущенной Кремлём кампании целенаправленной дезинформации не только русскоязычной, но и западной общественности. Подобные оценки регулярно озвучивались на разных уровнях, и уже осенью на Западе стали выходить полноценные монографии²¹⁹ с хроникой украинского кризиса, в которых российская пропаганда фигурировала как самоочевидный, бесспорный факт.

Кроме того, летом 2014 г., на волне общественно-политического резонанса вследствие падения малазийского «Боинга», Правительство Нидерландов выделило полмиллиона евро на организацию совместного с Польшей и под эгидой Европейского фонда поддержки демократии проекта по изучению методов противодействия российской дезинформации²²⁰, в рамках которого несколько десятков наиболее авторитетных экспертов должны были провести специальное исследование и подготовить конкретные предложения для национальных правительств и органов ЕС по организации альтернативного вещания в противовес «российской пропаганде»²²¹.

Тем не менее, закрепление этого направления деятельности на институциональном уровне ЕС происходило довольно медленно. Частично это

²¹⁸ Myths about the EU-Ukraine Association Agreement. Setting the facts straight // The European Commission. 22 January 2014. URL: http://trade.ec.europa.eu/doclib/docs/2014/january/tradoc_152074.pdf (дата обращения: 11.11.2020)

²¹⁹ См. например Wilson A. Ukraine Crisis: What It Means for the West / A. Wilson. Yale University Press, 2014. 236 p.

²²⁰ Rettman A. Dutch-Polish 'content factory' to counter Russian propaganda / A. Rettman // EU Observer. 21 July 2015. URL: <https://euobserver.com/foreign/129724> (дата обращения: 11.11.2020)

²²¹ Dempsey J. The Kremlin's clampdown on the media and sophisticated propaganda machine are giving the European Endowment for Democracy a new sense of focus / J. Dempsey // Carnegie Europe. 16 March 2015. URL: <https://carnegieeurope.eu/strategiceurope/?fa=59377> (дата обращения: 11.11.2020)

объяснялось общей бюрократической инерцией евроинтеграционного аппарата, частично – отсутствием полного политического консенсуса между государствами-членами относительно целесообразности антагонизировать Россию в этом отношении и переводить деятельность в этой сфере на системную основу, частично – тем обстоятельством, что в 2014 г. истекал срок полномочий действующего состава Европарламента и Еврокомиссии, и коммунитарные институты находились в переходной фазе, когда изменения в их политическую и функциональную конфигурацию, фактически, были заблокированы. Поэтому инициативная кампания с целью заставить Евросоюз признать актуальность «российской информационной угрозы» и включиться в становление системы противодействия ей вышла на официальный уровень только в начале 2015 г.

Она развивалась на трёх основных направлениях – Европарламента, Еврокомиссии и Европейской службы внешних действий (ЕСВД). К каждому из этих органов апеллировали заинтересованные игроки с целью добиться выделения финансовых и административных ресурсов под различные ситуативные проекты и регулярную деятельность по борьбе с российской пропагандой. Ещё одним центром приложений усилий стал формально автономный, но связанный с ЕС Европейский фонд поддержки демократии, созданный по инициативе Польши в 2012 г. для поощрения демократических процессов в восточном и южном соседстве. Основной упор лоббистских усилий приходился всё же на Европейскую службу внешних действий как ключевую политическую структуру, призванную озвучивать позицию Евросоюза в целом.

После целого ряда мероприятий на уровне неправительственных организаций 8 января 2015 г. четыре государства ЕС – Великобритания, Дания, Литва и Эстония – направили новоизначальному Верховному представителю по внешним делам и политике безопасности Федерике Могерини позиционный документ²²², призывающий Евросоюз усилить публичное сопротивление

²²² Lidegaatd M. et al. EU Strategic communication responding to propaganda. Non-paper. 8 January 2015. URL: <http://club.bruxelles2.eu/wp-content/uploads/2015/02/Let-StratCommRussie-DkEstLitUk@UK150108.pdf> (дата обращения: 11.11.2020)

распространению дезинформации и пропаганды в ЕС и в восточных странах-партнёрах, оказать поддержку независимым и альтернативным каналам информации, в том числе в России, и обеспечить достаточную устойчивость жизненно важных систем ЕС к информационным манипуляциям при сохранении базовых ценностей. В этом документе содержался широкий перечень предлагаемых мер, включая создание отдельной веб-платформы для разоблачения «фейков», поддержку альтернативных русскоязычных СМИ, создание специального телеканала с русским языком вещания, разработку специального плана действий в этой сфере на ближайшие два года. Тем не менее, создание отдельного структурного подразделения для борьбы с российской пропагандой там пока не упоминалось.

Неделю спустя к кампании по продвижению темы информационной войны со стороны России подключился Европарламент (ЕП). Традиционный алгоритм, согласно которому ЕП сначала формулирует крайне амбициозную повестку дня, затем Еврокомиссия или другие коммунитарные органы на основе его позиции представляют чуть менее амбициозные, но всё равно далекоидущие проекты решений, к которым некоторые государства-члены ещё не готовы, а потом разворачивается публичное и непубличное обсуждение, в ходе которого колеблющиеся страны вынуждены соглашаться с большей частью предложенных мер под «интеграционным давлением», был реализован и на этот раз²²³. 15 января 2015 г. Европарламентом была утверждена резолюция по ситуации на Украине²²⁴, в которой говорилось, что Европарламент:

«5. решительно осуждает агрессивную и экспансионистскую политику России, которая представляет собой угрозу единству и независимости Украины и представляет потенциальную угрозу для самого ЕС, включая незаконную аннексию Крыма и ведение необъявленной гибридной войны против

²²³ Vilson M. The Europeanization of foreign policy in the face of the Russian disinformation war / M. Vilson // Sõjateadlane (Estonian Journal of Military Studies). 2016. Vol. 2. P. 135.

²²⁴ Resolution of 15 January 2015 on the situation in Ukraine // European Parliament. 15 January 2015. URL: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0011+0+DOC+XML+V0//EN&language=EN (дата обращения: 11.11.2020)

Украины, в том числе информационную войну, сочетание элементов кибервойны, использования регулярных и нерегулярных сил, пропаганды, экономического давления, энергетического шантажа, дипломатии и политической дестабилизации; подчёркивает, что эти действия являются нарушением международного права и представляют собой серьёзную проблему для европейской безопасности; подчёркивает, что нет оправдания использованию военной силы в Европе для защиты так называемых исторических мотивов и мотивов безопасности или для защиты так называемых "соотечественников, живущих за рубежом"; призывает Москву прекратить эскалацию ситуации, немедленно остановив поток оружия, наёмников и войск в поддержку сепаратистских ополченцев и используя свое влияние на сепаратистов, чтобы убедить их участвовать в политическом процессе; <...>

27. Призывает Еврокомиссию и Комиссара по европейской политике соседства и переговорам по расширению подготовить и представить в парламент в течение двух месяцев коммуникационную стратегию по противодействию российской кампании, направленной против ЕС, его восточных соседей и самой России, и разработать инструменты, которые позволили бы ЕС и его государствам-членам противодействовать пропагандистской кампании на европейском и национальном уровнях».

Примечательно, что, признавая российскую «гибридную войну» против Украины угрозой для ЕС, Европарламент возложил задачу формирования стратегии противодействия пропаганде на Еврокомиссию, а не на ЕСВД.

29 января 2015 г. в Брюсселе прошло заседание Совета ЕС по внешним делам, где обсуждалась тематика конфликта на Украине. В пресс-релизе по итогам заседания²²⁵, среди прочего, было сказано, что «Совет возлагает на Высокого представителя задачу нарастить усилия ... для дальнейшего укрепления стратегических коммуникаций ЕС ... и изучить возможность

²²⁵ Outcome of the Council Meeting // Council of the European Union. 29 January 2015. URL: <https://www.consilium.europa.eu/media/23243/st05755en15.pdf> (дата обращения: 11.11.2020)

формирования специальной коммуникационной команды для руководства этими мерами. Такие усилия должны включать проактивное донесение политики ЕС [до общественности], исправление искажённой информации по мере её появления и оказание поддержки дальнейшему развитию независимых СМИ в регионе».

Однако результаты заседания показались недостаточными руководству Латвии, которая по ротации осуществляла председательство в Совете Европейского союза в первой половине 2015 г., и 6 февраля оно направило евроинтеграционным институтам собственный позиционный документ, в котором призывает их перекрыть возможности для «*кампаний дезинформации, проводимых акторами вне ЕС, которые пытаются повлиять, бросить вызов и подорвать наши общества и влияние политики ЕС в нашем соседстве*»²²⁶. В нём также говорится, что комиссия должна как можно скорее завершить процесс пересмотра законодательства в аудиовизуальной сфере и предоставить промежуточный доклад о возможностях обойти национальные законы в сфере медиа для внешних игроков. Отдельно прописывалась²²⁷ необходимость оказать помощь Евросоюзу Грузии, Молдове и Украине в деле укрепления регулярных механизмов контроля и прозрачности собственности СМИ. Для Латвии, уже успевшей ввести ряд ограничений против ряда российских и русскоязычных СМИ, приоритетным был вопрос ухода от ответственности за нарушение свободы слова и прав медиа и получение легальных возможностей беспрепятственно и в сжатые сроки ограничить присутствие в своём информационном пространстве нежелательных СМИ под предлогом борьбы с российской пропагандой.

По этим заявлениям можно также понять, что европейские лидеры на начальном этапе рассчитывали, что ключевой инстанцией «информационного фронта» против России станет НАТО, а Евросоюзу будет отведена вспомогательная роль. Однако ряд заинтересованных государств-членов,

²²⁶ Цит. по Rettman A. EU to strike back at Russian propaganda / A. Rettman // EU Observer. 19 March 2015. URL: <https://euobserver.com/foreign/128071> (дата обращения: 11.11.2020)

²²⁷ Там же.

опираясь на поддержку в Европарламенте, требовал от Евросоюза закрепить свою роль в информационном противодействии России не только в качестве разового политического обязательства и пакета практических мер, но и в качестве систематической институционализированной деятельности от лица коммунитарных институтов.

После эскалации конфликта на Донбассе и заключения вторых Минских соглашений в феврале 2015 г. антироссийские силы активизировали свои усилия, получив возможность утверждать, будто угроза российской агрессии не спадает и может коснуться любой другой европейской территории. Идя на поводу у этих сил, высшие европейские функционеры постепенно репродуцировали её дискурс и выражали готовность реализовать предлагаемые ею меры. Ещё на неформальном саммите министров обороны ЕС, прошедшем в рамках латвийского председательства в Риге 18-19 февраля 2015 г., обсуждалась необходимость усилить потенциал ЕС в отношении «гибридных угроз» и стратегических коммуникаций²²⁸. 6 марта 2015 г., выступая на межпарламентской конференции в Риге, глава дипломатии ЕС Федерика Могерини в ответ на призывы со стороны прибалтийских лидеров заявила, что в Евросоюзе ведётся работа над тем, чтобы противостоять российской пропаганде на русском языке среди русскоязычного населения не только в странах-восточных соседях ЕС и в России, но и в странах-членах ЕС²²⁹.

12 марта 2015 г. в резолюции Европарламента, утверждающей ежегодный отчёт Высокого представителя по внешним делам и политике безопасности²³⁰, были прописаны пункты, призывающие его в качестве приоритетной задачи выработать стратегию ЕС в отношении России, а также подчёркивалась *«необходимость в целостном европейском подходе к кампаниям искажения*

²²⁸ EU Defence Ministers in Riga call for unity in addressing European security threats. Media Release // Latvian Presidency of the Council of the European Union. 19 February 2015. URL: <https://eu2015.lv/news/media-releases/666-eu-defence-ministers-in-riga-call-for-unity-in-addressing-european-security-threats> (дата обращения: 11.11.2020)

²²⁹ Добровольский В. Могерини: ЕС работает над ответом на "пропаганду" на русском языке / В. Добровольский // РИА Новости. 6 марта 2016. URL: <https://ria.ru/20150306/1051245164.html?in=t> (дата обращения: 11.11.2020)

²³⁰ Resolution on the Annual Report from the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament // European Parliament. 12 March 2015. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015IP0075&from=EN> (дата обращения: 11.11.2020)

информации и пропаганды, проводимым Россией как в пределах, так и за пределами ЕС», и содержался призыв к ЕСВД и Еврокомиссии представить план действий с конкретными мерами противодействия российской пропаганде и наладить сотрудничество в этой сфере с Центром стратегических коммуникаций НАТО. Показательно, что в официальных документах европейских структур на том этапе ещё не фигурировало понятие «дезинформации» (*disinformation*), а вместо этого употреблялось понятие «искажение информации» (*misinformation*), что отражало желание некоторых членов ЕС снизить напряжённость вокруг темы информационной войны с РФ.

Зато в принятом по результатам заседания Европейского Совета 19-20 марта 2015 г. Заключении о внешних делах применительно к российско-украинскому вопросу уже чётко говорится о «дезинформации» (и это было представлено в СМИ как компромисс вследствие нежелания некоторых государств-членов утверждать формулировку о «русской пропаганде»²³¹). Так, в п. 13 Заключения Совет *«подчеркнул необходимость противодействовать проводимым Россией кампаниям по дезинформации и предложил Высокому представителю в сотрудничестве с государствами-членами и институтами ЕС подготовить к июню план действий по стратегической коммуникации. Создание коммуникационной команды является первым шагом в этом направлении»*²³². Как легко заметить, ни конкретные функции, ни статус этой коммуникационной команды в данном документе прописаны не были. Несколько недель спустя на базе этого решения в рамках ЕСВД создаётся группа экспертов для разработки соответствующего плана действий.

В прессу²³³ также попала информация о том, что на мартовском саммите Европейского совета лидеры ЕС рассматривали возможность расширить

²³¹ Цит. по Rettman A. EU to strike back at Russian propaganda / A. Rettman // EU Observer. 19 March 2015. URL: <https://euobserver.com/foreign/128071> (дата обращения: 11.11.2020)

²³² Conclusions on external relations // European Council. 19 March 2015. URL: <https://www.consilium.europa.eu/en/press/press-releases/2015/03/19/conclusions-russia-ukraine-european-council-march-2015/> (дата обращения: 11.11.2020)

²³³ Дудина Г. Война до победного слова. Кто и как борется в Европе с «русской пропагандой» / Г. Дудина // Коммерсант. 23 августа 2015. URL: <https://www.kommersant.ru/doc/2795055> (дата обращения: 11.11.2020)

санкции против «медиаструктур и журналистов, активно участвовавших в пропагандистских усилиях в поддержку аннексии Крыма со стороны РФ и российской военной интервенции на Украине», однако от этой меры на том этапе решили воздержаться.

Институционализация инфраструктуры информационной войны с Россией как таковая происходила путём смещения фокуса от собственно России как единственного источника этих угроз и возможности нейтрализовать их путём нормализации отношений с Россией в сторону максимальной генерализации этих угроз как отдельного класса вызовов безопасности в современном мире, в рамках которого угрозы, исходящие от России, являются пусть и наиболее показательными, но далеко не единственными. Поэтому, помимо усилий в сугубо информационной сфере, разворачиваемых в рамках общей внешней политики ЕС и, в частности, его восточной политики, в объединении также закладывается основа для противодействия «гибридным угрозам» как самостоятельному направлению в рамках политики безопасности.

Так, 13 мая 2015 г. Европейская служба внешних действий представила неофициальный доклад «Пища для размышлений – Противодействие гибридным угрозам»²³⁴, в котором под одним ярлыком объединялись угрозы, исходящие от действий России в восточном соседстве ЕС и ИГИЛ в южном, и перечислялись возможные шаги в рамках противодействия данным угрозам в рамках трёх направлений – повышения осознанности собственных уязвимостей, способных стать объектами «гибридных атак», укрепления устойчивости к ним, сдерживания «гибридной агрессии» благодаря неизбежному наказанию агрессора и недопущению получения им ожидаемого выигрыша и усиления потенциала для ответа на подобные атаки. Понятие «уязвимость» в этом документе трактовалось весьма широко: так, в случае Украины критическими уязвимостями были названы, помимо слабости управленческих институтов и дефицита поддержки силовых структур, наличие многочисленного

²³⁴ Food-for-thought-paper “Countering Hybride Threats” // European External Action Service. 13 May 2015. URL: <http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf> (дата обращения: 11.11.2020)

русскоязычного населения, которое ощущало себя маргинализированным, и критическая зависимость от РФ в плане импорта и поставок энергоносителей.

Для выполнения данных задач эксперты ЕСВД предлагали учредить в рамках службы специальную группу, которая бы собирала и обрабатывала данные о текущей ситуации и сигналы о «гибридных угрозах», поступающие от государств и органов ЕС, а также проводила исследования и вырабатывала доктрину противодействия «гибридным угрозам» в масштабе всего Евросоюза. В качестве непосредственных мер авторы документа предлагали прописать необходимость учитывать данное направление в ходе подготовки будущего стратегического обзора ЕС, а также сформулировать отдельную стратегию по борьбе с «гибридными угрозами», комплементарную соответствующей стратегии НАТО, в сотрудничестве с которой ЕС предстоит отражать нынешние и будущие «гибридные угрозы».

18 мая 2015 г. Совет по внешним делам одобрил Выводы по общей политике безопасности и обороны, в которых, среди прочего, содержалось поручение Высокому представителю *«в тесном сотрудничестве со службами Комиссии и Европейским агентством обороны и в консультации с государствами-членами ЕС представить к концу 2015 года согласованный комплекс действенных предложений по противостоянию гибридным угрозам и повышению устойчивости ЕС и его государств-членов, а также стран-партнёров. Должна приниматься во внимание соответствующая работа, касающаяся киберзащиты, раннего предупреждения, стратегических коммуникаций, соответствующая внутренней и внешней политике ЕС... подчеркивается необходимость взаимодополняемости и прозрачного сотрудничества и координации в этой области с соответствующими партнёрскими организациями, включая, в частности, НАТО, а также странами-партнёрами»*²³⁵. Срок до конца 2015 г., по всей видимости, был поставлен из расчёта на то, что до этого времени уже будет подготовлена соответствующая

²³⁵ Council Conclusions on CSDP // Foreign Affairs Council. 18 May 2015. URL: <https://www.consilium.europa.eu/media/24520/st08971en15.pdf> (дата обращения: 11.11.2020)

стратегия НАТО в этой сфере, в которой Альянс возьмёт на себя основную политическую ответственность и материальные расходы на отражение «гибридных угроз», тогда как Евросоюз сможет выполнять в этом отношении вспомогательную функцию.

В преддверии июньского саммита Европейского Совета резонанс антироссийской кампании поддержал Европарламент, приняв развёрнутую и весьма жёсткую резолюцию о состоянии отношений между ЕС и Россией²³⁶, в которой отмечалось, что *«Россия активно использует гибридную войну, намеренно стирая грани между военной / военизированной деятельностью и политической активностью»*, в связи с чем государства-члены ЕС должны эффективно скоординировано устранить слабые места в разных сферах своей политики, включая информационную и кибернетическую безопасность. В резолюции содержатся стандартные обвинения РФ в ограничении свободы слова и насаждении информационной монополии (п. 2), указание на необходимость расширить анализ российской пропаганды на предмет своевременной нейтрализации «дезинформации» в странах ЕС и странах-партнёрах «инструментами для стратегической коммуникации», а также наблюдения за связями России с политическими партиями и другими организациями в странах ЕС (п.13), указание на опасность российских связей с маргинальными политическими течениями в ЕС и принятие контрмер (пп. 15 и 16), критика российских попыток пересмотреть негативное отношение к прошлому своей страны (п. 14), призыв к поддержке российских и русскоязычных журналистов и СМИ, являющихся *«достоверными и независимыми источниками информации»* (п. 17).

К 16 июня 2015 г. Высокий представитель ЕС Ф. Могерини во исполнение поручения Европейского Совета от 19-20 марта 2015 г. предоставила проект плана действий по стратегической коммуникации с целью противодействия

²³⁶ Resolution of 10 June 2015 on the state of EU-Russia relations // European Parliament. 10 June 2015. URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0225+0+DOC+XML+V0//EN> (дата обращения: 11.11.2020)

«российской дезинформации», текст которого был обнародован заранее, а 22 июня план был утверждён, и общая координирующая и контролирующая роль в ходе его реализации была возложена на Оперативную рабочую группу East StratCom Task Force²³⁷.

В этом плане были поставлены задачи налаживания эффективной коммуникации и продвижения политики ЕС в восточном соседстве, усиления медийной среды, включая оказание поддержки независимым СМИ, повышения общественной осведомлённости о дезинформационных действиях внешних акторов и укрепления потенциала ЕС в плане прогнозирования и реагирования на такие действия. Основным шагом на пути к достижению заявленных целей в плане было заявлено наращивание потенциала Евросоюза в сфере стратегических коммуникаций путём развёртывания к сентябрю 2015 г. во внешнеполитической службе ЕС Оперативной рабочей группы по стратегическим коммуникациям (*East StratCom Task Force*). Заметим, что в мартовском поручении Евросовета предполагалось создание *команды East StratCom Team*, однако к моменту реализации поручения в сентябре она уже фигурировала как *оперативная группа* (постоянно действующих) *сил*, что подчёркивало её стационарный статус. Работа группы, как предполагалось, должна быть направлена, прежде всего, на проактивное донесение информации о политике ЕС в восточном соседстве и за его пределами. В частности, группа должна выявлять идущие кампании дезинформации и готовить материалы для лидеров, органов и делегаций ЕС с предложениями об улучшении стратегических коммуникаций с учётом специфики целевой аудитории и её интересов. Для этого предлагалось наладить широкое сотрудничество с неправительственными организациями в этой сфере, независимыми СМИ и гражданским обществом, способствовать повышению медиаграмотности, укрепить координацию с государствами-членами.

²³⁷ Action Plan on Strategic Communications // European External Action Service. 22 June 2015. URL: http://archive.eap-csf.eu/assets/files/Action_Plan.pdf (дата обращения: 11.11.2020)

За обтекаемыми дипломатичными формулировками крылось вполне конкретное содержание. С одной стороны, подавлять российские нарративы предполагалось через создание сети вещания на русском языке в странах Восточного партнёрства. С другой стороны, предполагалось задействовать «возросшую сознательность» самих европейских СМИ, которые должны были отказывать в предоставлении прямого слова российским представителям и придерживаться презумпции подрывных намерений исходящих от России нарративов как «дезинформационных» и направленных на подрыв институтов ЕС. Национальные регуляторы должны были исключать неблагоприятную с точки зрения нарративов ЕС информацию. На национальном уровне предполагалось обучать местных журналистов освещению событий в русле лояльного Евросоюзу «коммуникационного материала», разработать который предполагалось сообща.

В выводах саммита 25-26 июня 2015 г. была прописана необходимость усиления Общей политики безопасности и обороны (ОПБО) ЕС, в том числе путём мобилизации инструментов для противодействия «гибридным угрозам»²³⁸. Однако дальше рядового упоминания данных угроз в перечне потребностей ОПБО Европейский совет не пошёл, даже несмотря на присутствие и участие в обсуждении Генерального секретаря НАТО Й. Столтенберга²³⁹, и оставил открытыми многие вопросы, поднятые в майском докладе ЕСВД.

Таким образом, за сравнительно небольшой, по меркам брюссельской бюрократической машины, промежуток времени с января по июнь 2015 г. Евросоюзом был принят ряд базовых политических решений относительно организации системы информационного противодействия России²⁴⁰. В

²³⁸ Meeting Conclusions // European Council. 26 June 2015. URL: <https://www.consilium.europa.eu/media/21717/euco-conclusions-25-26-june-2015.pdf> (дата обращения: 11.11.2020)

²³⁹ Remarks by President Donald Tusk after the European Council meeting // European Council. 26 June 2015. URL: <https://www.consilium.europa.eu/en/press/press-releases/2015/06/26/tusk-final-remarks-european-council/> (дата обращения: 11.11.2020)

²⁴⁰ Vilson M. The Europeanization of foreign policy in the face of the Russian disinformation war / M. Vilson // Sõjateadlane (Estonian Journal of Military Studies). 2016. Vol. 2. P. 134.

дальнейшем происходило, главным образом, выполнение этих решений, их конкретизация и становление анонсированных структур.

Созданная на волне резонанса текущей политической конъюнктуры, Рабочая группа *East StratCom* изначально не имела ни чётких полномочий, ни собственного бюджета. Из девяти вошедших в её состав русскоязычных экспертов четверо были штатными сотрудниками ЕСВД, а пятеро делегировались национальными правительствами Великобритании, Дании, Чехии, Латвии и Эстонии на основании годичного трудового контракта²⁴¹ (примечательно, что Польша, изначально планировавшая также делегировать своего представителя в группу и претендовавшая на его лидирующую роль в ней, отказалась²⁴² от этого шага, узнав, что руководство группой будет поручено британскому дипломату). Её главная миссия состояла в информировании общественности стран Восточного партнёрства о политике Евросоюза и оказанию поддержки делегациям ЕС в этих странах. Кроме того, в её функции входил мониторинг российских СМИ и выработка предложений ЕС для формирования противодействующей медийной стратегии, но не собственно ведение контрпропаганды, т. е. генерирование медиаконтента и выпуск собственных информационных ресурсов²⁴³. Это означало, что центральная идея многих инициатив в данной сфере – создание отдельного русскоязычного телеканала – оставалась нереализованной.

Такая довольно скромная, по мнению обозревателей, постановка задачи для новой Оперативной группы, ограниченная сугубо пространством восточного соседства, не затрагивающая собственно страны ЕС и не предусматривающая самостоятельной роли в контрпропагандистской деятельности, объяснялась якобы недостаточной приоритетностью сферы борьбы с дезинформацией в

²⁴¹ Panichi J. EU declares information war on Russia / J. Panichi // Politico. 27 August 2015. URL: <https://www.politico.eu/article/russia-propaganda-ukraine-eu-response-disinformation/> (дата обращения: 11.11.2020)

²⁴² Panichi J. EU Splits in Russian media war / J. Panichi // Politico. 17 September 2015. URL: <https://www.politico.eu/article/eu-russia-propaganda-kremlin-media/> (дата обращения: 11.11.2020)

²⁴³ Panichi J. EU declares information war on Russia / J. Panichi // Politico. 27 August 2015. URL: <https://www.politico.eu/article/russia-propaganda-ukraine-eu-response-disinformation/> (дата обращения: 11.11.2020)

глазах Высокого представителя²⁴⁴ и нежеланием многих государств-членов усугублять конфликт с Россией²⁴⁵. Чтобы преодолеть это сопротивление, проводники антироссийской линии представляли эту сдержанную позицию как предвзятость, дефицит солидарности и торможение интеграции на одном из ключевых направлений внешней политики ЕС.

Осенью 2015 г. Оперативная группа *East StratCom* разворачивает конкретную деятельность по мониторингу информационного пространства и выявлению «российской дезинформации». С ноября 2015 г. она начинает издавать регулярный Обзор дезинформации и создаёт специальную базу, регистрирующую случаи появления якобы неправдивой информации о деятельности ЕС. Кроме того, она инициирует создание русскоязычной версии официальных сайтов ЕСВД и других коммунитарных органов ЕС.

Показательно, что практически с самого начала эта работа не была ограничена установленными в решениях ЕС рамками и, самое главное, не была основана на каких-либо строгих критериях объективности и достоверности. В итоге деятельность по выявлению «дезинформации» на деле ожидаемо обернулась деятельностью по выявлению любых отклонений от официальной западной трактовки текущих событий как в российских, так и в европейских СМИ, и стигматизации их в качестве «фейков» и «пропаганды». И хотя её эффективность в плане влияния на русскоязычную общественность с самого начала вызывала сомнения²⁴⁶, запущенные таким образом интерпретации российского нарратива разносились по европейским и украинским масс-медиа, выступая своеобразным эталоном для всех «независимых СМИ». Навешивая ярлык «пропаганды» на те или иные тезисы официальной риторики РФ, Оперативная группа тем самым снимала потребность в оппонировании им с

²⁴⁴ Scheidt M. The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle? / M. Scheidt // EU Diplomacy Paper. 2019. No. 1. P. 13. URL: https://www.coleurope.eu/system/tdf/research-paper/edp_1_2019_scheidt.pdf?file=1&type=node&id=51569&force= (дата обращения: 11.11.2020)

²⁴⁵ Panichi J. EU Splits in Russian media war / J. Panichi // Politico. 17 September 2015. URL: <https://www.politico.eu/article/eu-russia-propaganda-kremlin-media/> (дата обращения: 11.11.2020)

²⁴⁶ Vilson M. The Europeanization of foreign policy in the face of the Russian disinformation war / M. Vilson // Sõjateadlane (Estonian Journal of Military Studies). 2016. Vol. 2. P. 130.

помощью доказательной аргументации. Наконец, постоянно пополняемая база якобы «российских фейков» создавала иллюзию действительно острой и неослабевающей угрозы наступления на европейские ценности со стороны враждебной силы и при этом доказывала необходимость закрепить деятельность Группы на постоянной основе и придать ей самостоятельный институциональный вес в структуре Европейской службы внешних действий.

Создание Оперативной группы, тем не менее, не закрывало вопрос о противодействии «гибридным угрозам» в целом, и после того, как соответствующая стратегия была выработана в рамках НАТО в декабре 2015 г., работа над собственным видением в этой области была активизирована в ЕС.

Эта работа развивалась на двух направлениях: во-первых, в направлении закрепления на формально-дискурсивном и политическом уровнях тезиса о России как о перманентном источнике «гибридных угроз» для ЕС, а, во-вторых, в направлении разработки доктринального обоснования, выявления и обозначения путей борьбы с такими угрозами в целом.

На первом направлении прогресс был достигнут в контексте подготовки визита Ф. Могерини в Москву в конце 2015 г., на фоне которой в ЕС была инициирована кампания по выработке «общего подхода» в отношении России, дабы сформировать политические и институциональные барьеры возможному пересмотру конфронтационного курса со стороны отдельных государств-членов или высших функционеров Союза. В результате 14 марта 2016 г. министры иностранных дел 28 стран-членов ЕС согласовали «пять руководящих принципов политики ЕС в отношении России», одним из которых провозглашалась устойчивость к российским угрозам, таким как энергетическая безопасность, гибридные угрозы и дезинформация²⁴⁷.

Кроме того, новый всплеск интереса к теме «российской дезинформации» в Евросоюзе обозначился после проведенного в Нидерландах 6 апреля 2016 г.

²⁴⁷ The EU's Russia policy: Five guiding principles // European Parliament Think Tank. 8 February 2018. URL: [http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI\(2018\)614698](http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2018)614698) (дата обращения: 11.11.2020)

консультативного референдума по утверждению соглашения об ассоциации ЕС с Украиной. При низкой явке в 32% избирателей соотношение голосов сложилось не в пользу сторонников соглашения, и процесс его вступления в силу был приостановлен²⁴⁸. Это дало дополнительные основания для обвинений России в манипуляциях не только в русскоязычном, но и в европейском информационном пространстве²⁴⁹.

На волне результатов голландского референдума в комитете по внешним делам Европарламента разворачивается кампания за принятие новой резолюции о «российской пропаганде» с требованием ещё больше усилить стратегические коммуникации ЕС. Весной 2016 г. по запросу этого комитета Европейским институтом исследований безопасности (Париж) было подготовлено²⁵⁰ специальное исследование потенциала стратегических коммуникаций ЕС перед вызовами международной пропаганды. Показательно, что в данном исследовании были объединены два вызова – с востока от РФ и с юга от ИГИЛ²⁵¹, – а также прямо говорилось о недостаточности имеющихся возможностей НАТО для отражения данных вызовов. На основе указанного исследования 2 мая 2016 г. депутат от Польши Анна Фотыга выдвинула проект решения комитета, предлагающий вынести на рассмотрение ЕП специальную резолюцию по данному вопросу²⁵². Однако на том этапе данному проекту не был дан ход.

²⁴⁸ Червоненко В. Как Украина проиграла референдум в Нидерландах / В. Червоненко // BBC. Русская служба. 7 апреля 2016. URL: https://www.bbc.com/russian/international/2016/04/160407_netherlands_ukraine_loss (дата обращения: 11.11.2020)

²⁴⁹ Brattberg E. Russian Election Interference. Europe Counter to Fake News and Cyber Attacks / E. Brattberg, T. Maurer // Carnegie Endowment for International Peace. May 2018. 54 p. URL: https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf (дата обращения: 11.11.2020); Coalson R. Russian Disinformation 2.0: Sowing chaos, confusion, and anger in the west / R. Coalson // Radio Free Europe/RadioLiberty. URL: https://internetfreedom.io/rferl_russian-disinformation.html (дата обращения: 11.11.2020); Zhabotynska S. New media and strategic narratives: the Dutch referendum on Ukraine – EU Association Agreement in Ukrainian and Russian Internet blogs / S. Zhabotynska, V. Velivchenko // European Security. 2019. Vol. 28, No. 3. P. 360-381.

²⁵⁰ EU strategic communications with a view to countering propaganda // European Parliament Policy Department, Directorate General for External Policies. May 2016. URL: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA\(2016\)578008_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf) (дата обращения: 11.11.2020)

²⁵¹ Организация, запрещённая в Российской Федерации.

²⁵² Fotyga A. Draft Report on EU strategic communications to counteract propaganda against it by third parties / A. Fotyga // European Parliament. 2 May 2016. 35 p. URL: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA\(2016\)578008_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf) (дата обращения: 11.11.2020)

На втором направлении общего доктринального закрепления «гибридных угроз», ключевым событием стало представление 6 апреля 2016 г. Совместного послания Еврокомиссии и Высокого представителя Европарламенту и Европейскому совету под названием «Общая рамочная программа противодействия гибридным угрозам – ответ Европейского союза»²⁵³. Послание было результатом совместной работы нескольких структур ЕС, прежде всего Еврокомиссии и ЕСВД, а также Европейского оборонного агентства и ряда государств-членов. Это непосредственным образом сказалось на его содержании, в котором присутствовали существенные отличия от майского доклада ЕСВД 2015 г., в частности, явно менее политизированный и антироссийский характер, так как «гибридные угрозы» в нём были представлены как объективно существующий элемент реального стратегического ландшафта. Программа в целом была сформулирована в довольно абстрактных безоценочных категориях.

В данном документе содержался краткий обзор сущности «гибридных угроз» и развёрнутый перечень мер, которые может предпринять ЕС для их слаженного отражения. В нём говорилось, что, хотя концепт «гибридных угроз» пока не имеет единого чёткого определения из-за их меняющего характера, он отражает сочетание принудительной и подрывной деятельности, конвенциональных и неконвенциональных методов воздействия, используемых скоординированным образом государственными или негосударственными акторами для достижения специфических целей, оставаясь при этом вне пределов формально объявленных военных действий. Возможными каналами распространения «гибридных угроз» в документе названы массированные кампании дезинформации с использованием социальных сетей для контроля над политическим нарративом, его радикализации, рекрутирования или непосредственного руководства «прокси-субъектами». Однако примечательно,

²⁵³ Joint Framework on countering hybrid threats a European Union response. Joint Communication to the European Parliament and the Council // European Commission. 6 April 2016. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016JC0018> (дата обращения: 11.11.2020)

что в этом контексте отсутствовало какое-либо упоминание о России как о главном источнике «гибридных угроз», использовании ею инструментов дезинформации в украинском кризисе как примере подобного использования.

Основная ответственность за отражение «гибридных угроз» возлагалась на государства-члены с учётом их потенциальных уязвимостей, но поскольку многие из них сталкиваются с общими угрозами и вызовами, признавалось целесообразным сформировать набор возможных инструментов на уровне Евросоюза и его механизмов.

В институциональном плане предлагалось, во-первых, формирование в рамках Разведывательного и ситуационного центра ЕСВД специального Центра по анализу гибридных угроз (*EU Hybrid Fusion Cell*) как основного локуса сбора информации о текущих и потенциальных «гибридных угрозах» от различных игроков – органов и государств-членов ЕС – и координации их действий, а, во-вторых, создание отдельного или межведомственного Центра передового опыта для противодействия «гибридным угрозам», который бы осуществлял стратегическую оценку и выработку стратегий отражения «гибридных угроз». Тем самым (и в этом заключалось ещё одно отличие от проекта 2015 г.) разводились по разным инстанциям функции непосредственного ситуативного реагирования и принятия решений и функции стратегической оценки, планирования и разработки возможных сценариев.

В формально-правовом плане выдвигалась инициатива рассмотреть возможность задействования ст. 222 Договора о ЕС о солидарности в ситуации террористических актов и природных катастроф на случаи особо серьёзных «гибридных атак», и ст. 42(7) о взаимопомощи на случаи, когда множественные «гибридные атаки» могут привести к вооружённой агрессии против государства-члена ЕС. Отдельно была прописана возможность направления миссий ЕС в рамках Общей политики безопасности и обороны для нейтрализации «гибридных угроз». Кроме того, инициировались обзоры возможных «гибридных угроз» в ряде критических отраслей инфраструктуры, а также

упоминалась необходимость налаживания сотрудничества с НАТО в этом вопросе.

Ещё один показательный момент – при том, что общий подход к противодействию «гибридным угрозам», изложенный в «Пище для размышлений» 2015 г., с акцентом на повышении осознанности и укреплении устойчивости, был, в целом, сохранён, раздел о сдерживании агрессии был заменён на раздел о предотвращении, реагировании на кризис и восстановлении. Таким образом, применение к данной сфере понятия «агрессия» было замещено более нейтральными с политической и правовой точек зрения формулировками.

В информационной сфере программа содержала предложения по укреплению стратегических коммуникаций государств-членов и их координации в целях адекватного мониторинга СМИ с учётом лингвистических возможностей, а также удаления нелегального контента экстремистского характера из информационного пространства.

По сути, в Рамочной программе европейские функционеры перенесли в сферу «гибридных угроз» многие методы и механизмы, сформированные в ходе борьбы с терроризмом, придав тем самым данному документу максимально формальный и «доктринообразный» вид. Европейский союз, тем самым, признавал свою компетенцию в этой политически чувствительной сфере, но при этом основные непосредственные рекомендации Программы сводились к проведению тщательной оценки потенциальных рисков и уязвимостей с последующей выработкой возможных мер и средств противодействия. Однако оценка конкретных рисков и уязвимостей была возложена на отдельные государства, что оставляло значительное пространство для различных подходов и интерпретаций. Некоторые из упомянутых в программе мер были реализованы в очень сжатые сроки. Так, к организации Центра по анализу гибридных угроз (*EU Hybrid Fusion Cell*) в ЕС приступили уже в мае 2016 г., хотя в полном объёме его работа была налажена лишь год спустя. В программе акцентировалась роль информационной сферы для распространения «гибридных угроз», но чётких мер

в этой связи не предлагалось, более того, не упоминались даже уже созданные в этой сфере органы, включая Оперативную группу *East StratCom*.

Значение данного документа с точки зрения выстраивания инфраструктуры информационного противодействия России весьма амбивалентно. С одной стороны, его менее политизированный и идеологизированный характер несколько снижал общий градус истерии и переводил дискуссию в более абстрактную плоскость. Но, с другой стороны, происходила рутинизация сферы «гибридных угроз» в бюрократическом аппарате Евросоюза, превращение её в отдельное направление деятельности как таковое, вне зависимости от реального наличия данного типа угроз и степени их актуальности. В отличие от ситуативных единичных решений, данная программа предусматривала не разовые меры, а запускала продолжительный процесс с участием государств и институтов ЕС, регулярной оценкой прогресса и отчётами о выполнении. Тем самым создавались бюрократические возможности, которыми государства-члены и другие акторы могли бы воспользоваться, исходя из своих политических мотивов.

В ещё большей степени линия на снижение политического резонанса вокруг данной тематики проявилась в ходе запущенного ранее стратегического обзора, вылившегося в разработку ЕСВД Глобальной стратегии Европейского союза «Общее видение, общие действия: более сильная Европа»²⁵⁴. Высокий представитель ЕС Ф. Могерини презентовала этот документ 28 июня 2016 г. Несмотря на то, что в нём воспроизведены базовые дискурсивные маркеры общей позиции ЕС в отношении России в духе мартовских «пяти принципов», Россия там не названа источником «гибридных угроз», и сами эти угрозы не выделяются в отдельное направление деятельности, а только перечисляются в общем списке новых трансграничных вызовов, наряду с терроризмом, кибер- и организованной преступностью. Зато в отдельное направление выделены

²⁵⁴ Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy // European External Action Service. June 2016. 60 p. URL: https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf (дата обращения: 11.11.2020)

стратегические коммуникации, усиление которых фигурирует, правда, последним пунктом в перечне приоритетов политики безопасности ЕС. В этом пункте, среди прочего, сказано, что ЕС будет *«давать быстрые фактические опровержения дезинформации»* и *«продолжать укреплять открытую критическую медиасреду внутри ЕС и за его пределами, в том числе работая с местными игроками и через социальные сети»*.

Аналогичная тенденция прослеживается и в Имплементационном плане по безопасности и обороне²⁵⁵, обнародованном ведомством Ф. Могерини 14 ноября 2016 г. в качестве пакета предложений по имплементации Глобальной стратегии ЕС. «Гибридные угрозы» упоминаются там, опять-таки, в перечислении новых вызовов, с которыми сталкивается ЕС в текущем международном окружении, в особенности тех, которые требуют координации внутренних и внешних аспектов безопасности. В этом же контексте упомянуто и противодействие дезинформации. При этом в конце документа в числе мер, которые могут внести вклад в защиту безопасности ЕС и его граждан, указаны, среди прочего, обеспечение выполнения Рамочной программы по противодействию «гибридным угрозам» и приоритезация стратегического анализа и ситуационного контроля, осуществляемого, в том числе, Центром анализа гибридных угроз.

Таким образом, на уровне ключевых доктринальных позиционных документов Евросоюз не стал придавать тематике «гибридных угроз» и дезинформации излишний политический приоритет и снизил градус антироссийского накала в своей официальной риторике, воспроизводя, вместе с тем, базовые формулировки и характеристики, выработанные на пике украинского кризиса.

Недостаточный энтузиазм Ф. Могерини и её ведомства в деле поддержания конфронтации с Россией в информационной сфере побудил адептов жёсткого курса добиться дополнительного «резервирования» полномочий в данной сфере

²⁵⁵ Implementation Plan on Security and Defence // European External Action Service. 14 November 2016. URL: https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en16_0.pdf (дата обращения: 11.11.2020)

в рамках Еврокомиссии. Так, в середине 2016 г. в связи с отставкой британского представителя в этом органе лорда Хилла вследствие голосования британских избирателей за выход из Евросоюза, глава Еврокомиссии принял решение учредить новую должность Комиссара по Союзу безопасности и назначить на неё другого британского представителя сэра Джулиана Кинга на тот период, пока Лондон и Брюссель будут вести переговоры по дальнейшему характеру взаимоотношений. Примечательно, что ни проект Союза безопасности, разработанный Еврокомиссией весной 2016 г.²⁵⁶, ни открытое письмо Жан-Клода Юнкера с описанием мандата нового комиссара²⁵⁷ не содержали упоминания «гибридных угроз», хотя содержали обстоятельные разъяснения порядка работы в области миграции, терроризма и кибербезопасности. Однако среди полномочий Кинга на его странице на сайте Еврокомиссии фигурировала борьба с террористической пропагандой²⁵⁸, а в штатном расписании сфер ответственности его команды значились, в том числе, и «гибридные угрозы»²⁵⁹. Сам же сэр Джулиан с самого начала активно включился в публичную кампанию по преувеличению значимости данных угроз и необходимости выработки общего европейского ответа на них, в некоторой степени беря на себя функции Высокого представителя и ЕСВД.

Новая волна обвинений в адрес российского руководства в связи с предполагаемым вмешательством «русских хакеров» в американскую избирательную кампанию осенью 2016 г. дала повод русофобским силам в Европе вновь вынести данную тематику на повестку дня. Роль локомотива здесь опять сыграл Европарламент. По его заказу в этот период публикуются новые

²⁵⁶ Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union // European Commission. 20 April 2016. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0230&from=EN> (дата обращения: 11.11.2020)

²⁵⁷ Juncker J.-C. Mission Letter / J.-C. Juncker // European Commission. 2 August 2016. URL: https://ec.europa.eu/commission/sites/beta-political/files/king_en.pdf (дата обращения: 11.11.2020)

²⁵⁸ Commissioner (2016-2019) Julian King // European Commission. URL: https://wayback.archive-it.org/12090/20191119121331/https://ec.europa.eu/commission/commissioners/2014-2019/king_en#responsibilities (дата обращения: 11.11.2020)

²⁵⁹ Julian King's team // European Commission. URL: https://wayback.archive-it.org/12090/20191120072730/https://ec.europa.eu/commission/commissioners/2014-2019/king/team_en (дата обращения: 11.11.2020)

специальные исследования²⁶⁰, доказывающие, в том числе, что информационная агрессия Кремля не является и не может ответом на потенциально аналогичную угрозу со стороны Запада или действия, воспринимаемые как таковая.

Вообще, довольно значимой линией западного нарратива о российской «гибридной войне» выступает обоснование того, почему эта война не может рассматриваться как закономерный ответ на недружественные шаги со стороны Запада, а выступает именно что следствием злонамеренного и глубоко укоренённого антизападного настроения российской политики, связанного с неприятием либеральных свобод и ценностей.

На фоне подобного всплеска интереса Комитет по внешним делам вернулся к рассмотрению выдвинутого за полгода до этого проекта евродепутата Анны Фотыги о противодействии внешней пропаганде. И 10 октября 2016 г. комитет одобрил предлагаемый А. Фотыгой проект. А уже 23 ноября 2016 г. Европарламент 304 голосами против 179 при 208 воздержавшихся принял резолюцию «Стратегические коммуникации ЕС как противодействие пропаганде третьих сторон».

В ней излагаются стандартные обвинения в том, что Россия и ИГИЛ атакуют ЕС, ведут враждебную пропаганду, стремятся расколоть ЕС, но отвечать на пропаганду надо не пропагандой, а *«повышением способности граждан к критическому мышлению»*²⁶¹. При этом фокус внимания постепенно смещается от стран Восточного партнёрства на западное сообщество в целом. Так, согласно резолюции, Москва *«активно использует широкий спектр средств и инструментов, включая специальные фонды, многоязычные телевизионные каналы, информационные агентства, социальные медиа и интернет-троллей для нападок на западные ценности, разъединения Европы, обеспечения внутренней поддержки и создания восприятия, что страны (программы)*

²⁶⁰ Russel M. Russia's information war: Propaganda or counter-propaganda? / M. Russel // European Parliament. October 2016. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589810/EPRS_BRI\(2016\)589810_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589810/EPRS_BRI(2016)589810_EN.pdf) (дата обращения: 11.11.2020)

²⁶¹ Be aware of Russian and ISIS propaganda, warn foreign affairs MEPs // European Parliament. 10 October 2016. URL: <http://www.europarl.europa.eu/news/en/press-room/20161010IPR46530/be-aware-of-russian-and-isis-propaganda-warn-foreign-affairs-meps> (дата обращения: 11.11.2020)

«Восточного партнерства» являются несостоявшимися»²⁶². Европарламент также призвал увеличить финансирование «демократических инструментов ЕС», увеличить персонал и бюджет Оперативной группы *EastStratCom*, преобразовав её в полноправный отдел ЕСВД и обеспечить её собственным веб-сайтом.

Примечательным в этой резолюции является также то, что она не содержит никаких критериев или предварительных условий, выполнение которых сделало бы возможным снятие предъявленных России обвинений и возврат к нормальным отношениям с ней²⁶³.

2.2. Особенности реагирования на «российскую информационную угрозу» органами власти государств Запада

США

Ещё на этапе так называемого «евромайдана» на Украине некоторые аффилированные и спонсируемые органами власти США неправительственные организации начали поднимать вопрос о предвзятом освещении украинских событий российскими СМИ. На этой волне появляются даже отдельные аналитические публикации, указывающие на политическую роль информационного влияния на соседние страны во внешней политике РФ. Так, 3 января 2014 г. выходит доклад высланного из России журналиста Д. Сэттера «Последняя судорога империи: попытки России контролировать медиа в бывших советских республиках»²⁶⁴, где утверждается, что попытки Москвы контролировать СМИ в обозначенных странах варьируются от непрямого финансирования до культурного программирования и продвижения лояльных специалистов на руководящие должности в филиалах ведущих

²⁶² European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties // European Parliament. 23 November 2016. URL: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0441&format=XML&language=EN> (дата обращения: 11.11.2020)

²⁶³ Риччери М. Стратегическая коммуникация на службе совместного проекта развития отношений между ЕС и Россией. Утопия или действительность? / М. Риччери // Государственное управление. Электронный вестник. 2018. Выпуск 68. С. 90.

²⁶⁴ Satter D. The Last Gasp of Empire: Russia's Attempts to Control the Media in the Former Soviet Republics / D. Satter // CIMA report. 8 January 2014. URL: https://www.cima.ned.org/wp-content/uploads/2015/02/CIMA-Russia-report_David_Satter.pdf (дата обращения: 11.11.2020)

международных информационных агентств. Подобное воздействие осуществляется в рамках более широкой стратегии, конечной целью которой является геополитическое доминирование и создание буферного региона, отделяющего РФ от европейского и западного воздействия, подобно ОВД во времена «холодной войны».

Тем не менее, на официальном уровне угроза, исходящая от российской информационной политики, на том этапе не рассматривалась как отдельный, требующий особых контрмер вызов. Администрация Б. Обамы отреагировала на события в Крыму громким осуждением и введением ряда персональных санкций против причастных к этим событиям граждан РФ. Перечисленные в соответствующих исполнительных указах Президента этой страны лица обвинялись в препятствовании демократическим процессам на Украине и в Крыму в целом, без выделения конкретных сфер их якобы злонамеренной деятельности. Однако на уровне законодательной власти тема «российской информационной угрозы» довольно быстро приобрела самостоятельное значение.

Вопрос о мерах противодействия российской пропаганде был вынесен на повестку дня Конгресса США уже в марте 2014 г., когда глава комитета по иностранным делам Палаты представителей Эд (Эдвард) Ройс (Ed Royce) подал проект Закона о поддержке Украины, содержащий положения и касательно информационной сферы. В частности, речь шла об увеличении финансирования Радио «Свобода» и «Голос Америки» для расширения их вещания на русском, украинском и крымскотатарском языках, а также увеличения числа корреспондентов на восточной Украине и в Крыму. Кроме того, в законопроекте говорилось об угрозах, которым подвергаются «свободные медиа» в сопредельных регионах, и указывалось на необходимость оказать превентивную поддержку странам, особенно уязвимым к российской пропаганде, в том числе Республике Молдова и балканским государствам²⁶⁵.

²⁶⁵ H.R.4278 – Ukraine Support Act. Draft law introduced by E. Royce on 21 March 2014 // US Congress. URL: <https://www.congress.gov/bills/113th-congress/house-bill/4278> (дата обращения: 11.11.2020)

Законопроект о поддержке Украины был оперативно одобрен Палатой представителей уже 2 апреля 2014 г., но его рассмотрение в Сенате затормозилось. Однако упомянутые положения в информационной сфере были вынесены в отдельный законопроект о международном вещании США на Украину и соседние регионы²⁶⁶, предполагающий выделение на эти цели дополнительно 10 млн. долларов. Он был одобрен Конгрессом и подписан Президентом Обамой 3 апреля 2014 г.

Однако Э. Ройс, ставший одним из главных рупоров Конгресса в вопросе борьбы с «российской пропагандой», пошёл дальше и летом 2014 г. под предлогом неэффективности информационной системы США и её слабости в конкуренции с российскими источниками выдвинул в Палате представителей специальный закон о реформе международных коммуникаций США²⁶⁷, согласно которому должно было создаваться новое Агентство по международным коммуникациям США, а три основные вещательные службы страны – Радио «Свобода», Радио «Свободная Азия» и Ближневосточная вещательная сеть – должны были быть объединены в единую структуру – Сеть свободных новостей. Как и многие «ястребиные» инициативы конгрессменов в 2014 г., этот законопроект, пройдя голосование в Палате представителей, так и не был утверждён Сенатом.

Вместо этого Сенат параллельно разработал и утвердил Акт в поддержку суверенитета, целостности, демократии и экономической стабильности Украины, где упоминался только факт «физической и экономической» агрессии РФ, тогда как информационная составляющая ограничивалась пунктом о том, что Госсекретарь должен прямо или с помощью неправительственных организаций «расширить свободный и неограниченный доступ к независимым СМИ любых типов на Украине и содействовать в деле защиты журналистов и

²⁶⁶ S.2183 - A bill entitled "United States International Programming to Ukraine and Neighboring Regions". Introduced by M. McConnell on 3 April 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/senate-bill/2183> (дата обращения: 11.11.2020)

²⁶⁷ H.R.4490 - United States International Communications Reform Act of 2014. Draft law introduced by E. Royce on 28 April 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/house-bill/4490> (дата обращения: 11.11.2020)

гражданских активистов, преследуемых за проявления свободы слова». Рекомендация общая и крайне неконкретная, причём она охватывала только внутренний аспект информационной политики на Украине, без какого-либо упоминания «российской пропаганды». Данный документ был введён в силу решением Президента Обамы уже 3 апреля 2014 г..

Лето и осень 2014 г. – период активной раскрутки «российской информационной угрозы» в американском экспертном и академическом сообществе. Различные аналитические структуры составляли и презентовали материалы, призванные привлечь внимание к опасности, исходящей от российской пропаганды, и увязать её с более масштабным вызовом мировому порядку и его либеральным принципам. Многие подобные материалы и их презентации спонсировались правительственными фондами, в том числе Национальным агентством в поддержку демократии США, или же околопартийными структурами. Основную роль в продвижении этого дискурса на том этапе сыграли такие организации, как Атлантический совет²⁶⁸, фонд «Наследие», Институт современной России, основанный М. Ходорковским. Параллельно эта тема подхватывается и тиражируется в СМИ.

4 декабря 2014 г. Палата представителей Конгресса США принимает резолюцию 758 «О решительном осуждении действий Российской Федерации, руководимой Владимиром Путиным, проводящей политику агрессии против соседних стран на основе политического и экономического доминирования»²⁶⁹, где, среди прочего, утверждалось, что 1) Правительство РФ неоднократно предпринимало попытки инфильтрации и атак против компьютерных сетей правительства США, частных лиц и компаний с целью незаконного сбора информации и подрывных операций, а также оказывало поддержку лицам,

²⁶⁸ О роли Атлантического совета в продвижении дискурса о «гибридной войне» см. Tsygankov A. P. Putin's "Global Hybrid War": U.S. Experts, Russia, and the Atlantic Council / A. P. Tsygankov, P. A. Tsygankov, H. Gonzales // *Russia in Global Affairs*. 2021. Vol. 19, No. 1. P. 147-172.

²⁶⁹ H.Res.758 - Strongly condemning the actions of the Russian Federation, under President Vladimir Putin, which has carried out a policy of aggression against neighboring countries aimed at political and economic domination. Resolution introduced by A. Kinzinger on 18 November 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/house-resolution/758/> (дата обращения: 11.11.2020)

причастным к подобным действиям; 2) РФ продолжает вести агрессивную пропаганду на Украине, в которой ложная информация используется для подрыва авторитета легитимного национального правительства, дестабилизации, провоцирования этнических противоречий и их насильственных проявлений; 3) РФ расширила присутствие спонсируемых государством СМИ в странах Центральной и Западной Европы на местных языках с целью использования новостных и информационных возможностей для искажения общественного мнения и создания прикрытия для усиления российского политического и экономического влияния в Европе; 4) США необходимо предпринять дополнительные усилия для расширения своего международного вещания во всех форматах на русском и украинском языках для того, чтобы противодействовать российской пропаганде и предоставить народу Украины и сопредельных регионов доступ к достоверной и сбалансированной информации. Одним из пунктов резолюции прописан призыв к Президенту и Госдепу США разработать стратегию многосторонней координации для производства и распространения новостей и информации на русском языке среди стран со значительным русскоговорящим населением, максимально используя существующие платформы создания контента, такие, как Голос Америки и Радио «Свобода», местные каналы государственно-частного партнёрства в информационной сфере, а также средства местных и региональных органов власти. Правда, эта резолюция имеет сугубо декларативную силу.

Зато более весомым документом является Акт о поддержке свободы Украины, проект которого был представлен в обеих палатах Конгресса ещё летом, а окончательно утверждён и подписан Президентом 18 декабря 2014 г.²⁷⁰. В разделе 8 в нём прописаны меры по расширению вещания в странах бывшего Советского Союза. В частности, он обязывает главу подчинённого Госдепу Совета управляющих по вопросам вещания (*Broadcasting Board of Governors – BBG*) в течение 90 дней подать план незамедлительного и существенного

²⁷⁰ H.R.5859 - Ukraine Freedom Support Act of 2014. Public Law No: 113-272. Enacted on 18 December 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/house-bill/5859> (дата обращения: 11.11.2020)

расширения объёма русскоязычного вещания для стран бывшего Советского Союза, включая страны Прибалтики, с целью противодействия пропаганде Российской Федерации. Приоритет при этом должен отдаваться вещанию на Украину, Грузию и Молдавию, поэтому необходимо сделать упор, в том числе, на вещании на украинском и румынском языках. Для этих целей в законе прописано выделение 10 млн. долларов ежегодно в течение трёх лет – с 2016 по 2018 гг. Также в разделе 9, посвящённом поддержке гражданского общества в РФ, упоминалась необходимость развития свободного Интернета в России, обеспечения доступа к независимым СМИ и поддержки журналистов и гражданских активистов, ратующих за свободу слова.

Таким образом, в законе была чётко прописана угроза «российской пропаганды», но только в отношении русскоязычной аудитории постсоветских стран. Противодействие ей предусматривает, фактически, лишь усиление контрпропаганды за счёт расширения вещания, речь пока не идёт о «наказании» России за подобные действия путём введения отдельных санкций.

Дальнейшее развитие данной тематики в американском политическом поле происходит на трёх основных направлениях – дискурсивном, военно-стратегическом и институциональном.

На дискурсивном направлении заинтересованные силы в Конгрессе, с одной стороны, и аффилированные с Госдепартаментом правительственные и неправительственные организации, с другой, запускают целую кампанию, призванную повысить значимость «российской информационной угрозы» для внешней политики США и западного сообщества в целом и подтолкнуть действующую администрацию к созданию специальных органов и выделению дополнительных бюджетных средств на борьбу с этой «угрозой». Для этого проводится серия публичных мероприятий различного уровня с участием как авторитетных экспертов и медиа, так и официальных лиц, а также иницируется ряд законопроектов, выделяющих иностранную дезинформацию и пропаганду в самостоятельную сферу государственной политики США.

Так, 14 апреля 2015 г. в газете *Wall Street Journal* вышла статья уже упомянутого главы комитета по иностранным делам Палаты представителей Эда Ройса²⁷¹, в которой наличие секретной «путинской армии троллей» подавалось как самоочевидный факт, а исходящая от неё угроза гипертрофировалась до уровня, превышающего уровень военной угрозы, хотя и презентовалась как актуальная только для союзников США по НАТО, имеющих значительную часть русскоязычного населения. Противодействие этой угрозе предлагалось организовать путём усиления зарубежного вещания американских СМИ, правда, при этом признавалась недостаточность подобных мер для пресечения «распространению подрывной лжи» о дискриминации русских в странах НАТО.

На следующий день, 15 апреля 2015 г., в комитете по иностранным делам Палаты представителей были организованы слушания на тему «Противостояние информационной войне России» под председательством Эда Ройса и с участием таких знаковых для антироссийской информационной кампании фигур, как Питер Померанцев и Хелле Дэйл²⁷². Их выступления были направлены на укрепление иллюзии о якобы уже ведущейся Россией информационной войне против Запада в целом, в условиях которой нет смысла вести диалог с российским руководством, поскольку в нём невозможно опираться на объективно установленные реальные факты.

3 ноября 2015 г. в подкомитете по делам Европы комитета Сената по иностранным делам прошли открытые слушания по теме «Путинское вторжение на Украину и пропаганда, угрожающая Европе»²⁷³, на которых выступил заместитель помощника госсекретаря США Б. Зифф. В его выступлении был

²⁷¹ Royce E. Countering Putin's Information Weapons of War / E. Royce // *Wall Street Journal*. 14 April 2015. URL: <https://www.wsj.com/articles/countering-putins-information-weapons-of-war-1429052323> (дата обращения: 11.11.2020)

²⁷² Confronting Russia's Weaponization of Information. Hearing before the Committee on Foreign Affairs House of Representatives, 15 April 2015 // US House of Representatives. URL: <https://docs.house.gov/meetings/FA/FA00/20150415/103320/HHRG-114-FA00-Transcript-20150415.pdf> (дата обращения: 11.11.2020); Нельсон Дж. Информация превращается в оружие / Дж. Нельсон // ИноСМИ. 26 апреля 2015. URL: <https://inosmi.ru/world/20150426/227717819.html> (дата обращения: 11.11.2020)

²⁷³ Putin's Invasion of Ukraine and the Propaganda that Threatens Europe. Hearing before the Subcommittee on Europe and regional security cooperation of the Committee on foreign relations United States Senate, 3 November 2015 // US Senate. URL: https://www.foreign.senate.gov/imo/media/doc/11_03_15_Putin's_Invasion_of_Ukraine_and_the_Propaganda_that_Threatens_Europe.pdf (дата обращения: 11.11.2020)

сделан акцент на том, что российское руководство ежегодно выделяет 1,4 млрд. долларов на поддержание огромной пропагандистской машины, вещающей на 30 языках в 130 странах, *«чтобы способствовать достижению своих целей по продвижению лживых нарративов Кремля, изобразить Запад как угрозу и подорвать доверие к независимым СМИ, а также к западным институтам и ценностям»*. Для сдерживания российского влияния, продолжил Зифф, в 2015 г. Госдепартамент и USAID выделили 66 млн. долл. на становление гражданского общества и независимые медиа в Евразии, в 2016 финансовом году предполагался рост этой суммы до 83 млн. долл. Отмечалось, что особая поддержка нужна для предотвращения попадания в сети российской пропаганды стран бывшей Югославии, на которые нацелена российская дезинформация, а спасение от российской дезинформации русскоязычной аудитории актуально на Украине и в Прибалтике. Для реализации последней цели в девяти странах формируются русскоязычная новостная программа, противостоящая кремлёвским нарративам²⁷⁴. Помимо Б. Зиффа на слушаниях выступили также приглашённые эксперты П. Померанцев, Л. Арон, М. Чуперски и Х. Конли.

16 марта 2016 г. сенатор-республиканец Роб Портман и сенатор-демократ Криса Мерфи внесли в Сенат США законопроект «Акт о противодействии информационной войне 2016 года», направленный на активизацию усилий Вашингтона по противодействию «пропаганде и дезинформации», распространяемой Россией, Китаем и другими странами. В соответствии с ним, среди прочего, предполагалось создание Центра информационного анализа и реагирования для анализа *«усилий правительства в области информационной войны»*. Центр должен бы разрабатывать и распространять *«основанные на фактах нарративы и анализ для противодействия пропаганде и дезинформации, направленным на союзников и партнёров Соединенных Штатов»*²⁷⁵. 10 мая 2016 г. он был одобрен Палатой представителей как закон О противодействии

²⁷⁴ Там же.

²⁷⁵ U.S. Senators Seek New Center To Counter Russian, Chinese 'Propaganda' // Radio Free Europe / Radio Liberty. 16 March 2016. URL: <https://www.rferl.org/a/us-senators-seek-to-counter-russia-china-propaganda/27617521.html> (дата обращения: 11.11.2020)

иностранный пропаганде и дезинформации при поддержке конгрессмена-республиканца Адама Кинзиндгера и конгрессмена-демократа Тедом Лие и одобрен Сенатом США 14 июля 2016 г. при поддержке сенатора Роба Портмана.

Довольно активно на этом поприще проявляют себя и представители американского дипломатического аппарата. Одним из наиболее показательных примеров служит выступление посла США в Германии Дж. Эмерсона на конференции, посвящённой российской дезинформации, которую организовали Атлантический совет и фонд Генриха Бёлля в Берлине в конце июня 2015 г. В своей вступительной речи²⁷⁶ посол углубился в работу «российской дезинформации»: упомянул бюджет в 400 млн. долл., выделяемый на вещание в 100 странах мира с включением развлекательных программ, работу кремлёвских троллей, ведущих работу в западных соцсетях и комментирующих гостевые книги западных СМИ, искажение действительности на официальном уровне в конкретных сюжетах (пребывание войск РФ в Крыму и на Украине, отвлечение от трагедии малайзийского «Боинга», угрозы ядерным ударом по странам НАТО). По его утверждению, российское руководство преследует цель *«вызвать разногласия среди союзников и подорвать глобальную систему, основанную на правилах»*, Западу же в ответ надо проявить солидарность тем, кто разделяет идеалы свободного информационного пространства. Поэтому Правительство США поддерживает журналистские расследования, призванные разоблачить российские манипуляции, выделяет дополнительное финансирование для обучения журналистов в рамках специальных курсов, помогает российским журналистам, порывающим с официальной линией.

На военно-стратегическом направлении в это время предпринимаются усилия, во-первых, по укреплению киберобороны, а, во-вторых, по введению в доктринальный аппарат концепта «гибридной войны» и «гибридной угрозы» и способов их нейтрализации.

²⁷⁶ Emerson J. B. Exposing Russian Disinformation / J. B. Emerson // Atlantic Council UkraineAlert Blog. 29 June 2015. URL: <https://www.atlanticcouncil.org/blogs/ukrainealert/exposing-russian-disinformation> (дата обращения: 11.11.2020)

Так, 5 февраля 2015 г. появилось сообщение²⁷⁷ о решении Пентагона расширить киберсилы, насчитывающие 6000 человек, ещё на 39 команд из 200 военнослужащих, которые войдут в разные рода вооружённых сил США и будут подразделяться на:

- *«Команды национальных миссий», которые будут противостоять иностранным хакерам, стремящимся повредить критически важной инфраструктуре США;*
- *Команды киберзащиты, которые защищают домен dot-mil, где хранятся военные секреты;*
- *Команды боевых миссий, которые помогают географически отдалённо расположенным войскам боевого командования атаковать зарубежных противников».*

В апреле 2015 г. была обнародована киберстратегия министерства обороны США²⁷⁸, где указывалось, что Россия и Китай наработали существенный потенциал и стратегии использования кибероружия, причём российские акторы проявляют особую ловкость в своей киберразведывательной деятельности и их намерения иногда трудно чётко распознать²⁷⁹. Что интересно, на том этапе американские стратеги ещё допускали гипотетическую возможность преодоления возникших противоречий и возвращения к двустороннему сотрудничеству с Москвой. Так, в примечаниях к стратегии говорилось, что если и когда американо-российские отношения в военной сфере будут возобновлены, Пентагон в рамках широкого межведомственного диалога будет стремиться наладить прямой диалог по кибервопросам между военными представителями двух стран для укрепления стратегической стабильности в киберпространстве²⁸⁰.

²⁷⁷ Sternstein A. The Pentagon Wants To Expand Its Cyber Forces / A. Sternstein // Defense One. 4 February 2015. URL: <https://rosecov.eredglasses.wordpress.com/2015/02/05/pentagon-to-expand-cyber-forces/> (дата обращения: 11.11.2020)

²⁷⁸ The Department of Defense Cyber Strategy. April 2015 // US Department of Defense. URL: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf (дата обращения: 11.11.2020)

²⁷⁹ Op. cit. P. 9.

²⁸⁰ Op. cit. P. 28.

Параллельно 1 апреля 2015 г. был издан специальный исполнительный указ Президента о блокировании собственности лиц, причастных к действиям в киберпространстве, нацеленным на нанесение ущерба критически значимым секторам экономики или объектам инфраструктуры США²⁸¹. Однако он касался атак сугубо на материальные и административные ресурсы страны без упоминания политических и институциональных целей. Невключение последних в перечень потенциальных мишеней врагов Америки на раннем этапе станет впоследствии одной из серьёзных претензий Б. Обаме в контексте избирательной кампании 2016 г.

В доктринальном отношении показательной стала опубликованная 1 июля 2015 г. обновлённая Национальная военная стратегия США²⁸², содержащая термины «гибридный конфликт» и «гибридная угроза» с прямым указанием на то, что угрозы такого рода исходят от России и проявлены в ходе её действий на Украине, что им особо трудно противодействовать из-за неопределённости при принятии решений по нейтрализации.

Кроме того, в октябре 2015 г. был обнародован специальный доклад военной разведки США «Тактика ответа на угрозу: Россия»²⁸³. В нём анализировался опыт конфликтных ситуаций 2008 г. в Грузии и 2014 г. в Крыму как гибридных войн с использованием «непрямых действий», в том числе пропагандистских кампаний, главным образом, с помощью трансляции российских телевизионных каналов. На основании полученных выводов американское военное ведомство открыло ряд двусторонних программ подготовки подразделений по реагированию на подобные угрозы в странах – возможных объектах новой «гибридной агрессии» России²⁸⁴.

²⁸¹ Executive Order 13694 of April 1, 2015. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities // US Treasury. URL: https://home.treasury.gov/system/files/126/cyber_eo.pdf (дата обращения: 11.11.2020)

²⁸² The National Military Strategy of the United States of America 2015 // National Security Strategy Archive. 1 July 2015. P. 4-5. URL: http://nssarchive.us/wp-content/uploads/2020/04/2015_National_Military_Strategy.pdf (дата обращения: 11.11.2020)

²⁸³ Threat Tactics Report: Russia // Public Intelligence. October 2015. URL: <https://info.publicintelligence.net/USArmy-RussiaTactics.pdf> (дата обращения: 11.11.2020)

²⁸⁴ США создают информационные войска в Турции: мишень – Россия // Военно-политическая аналитика. 14 июня 2016. URL: <http://vpoanalytics.com/2016/06/14/ssha-sozdayut-informacionnyye-vojska-v-turcii-mishen-rossiya/> (дата обращения: 11.11.2020)

В середине 2016 г. администрация Б. Обамы предприняла шаги по усилению военно-стратегического и бюрократического потенциала в информационной сфере и киберпространстве. В июне 2016 г. Пентагон опубликовал Стратегию оперирования в информационной среде²⁸⁵, в которой нет прямого упоминания «гибридных угроз» или «гибридной войны» и обвинений России в её ведении, однако констатируется всё более широкое применение государственными и негосударственными акторами информационных и цифровых технологий для распространения правдивой, ангажированной и ложной информации с целью оказать влияние на невоенную аудиторию с помощью мощных символических и стратегических коммуникаций в сочетании с соответствующими физическими методами воздействия. Исходя из этого, военное ведомство США заявило о готовности взять на себя ведущую роль в ходе реализации операций США и их союзников в информационной сфере как в условиях открытого конфликта, так и вне его. Как видно из этой формулировки, речь шла об организации внешних операций за пределами США, а не о влиянии на американское общество и внутривнутриполитические процессы. Для реализации поставленных целей – оказания влияния на принятие решений и поведение противника и получения преимущества в ходе военных операций – в стратегии предлагался ряд шаблонных мер, а именно усиление мониторинга информационной среды, подготовка концепции оперирования в информационной среде, оценка существующего потенциала в данной сфере, налаживание партнёрства с союзниками и гражданским обществом. Фактически, рассматриваемая стратегия укрепляла общую тенденцию к милитаризации информационной сферы, резко усилившуюся благодаря распространению дискурса о «гибридной войне» и «российской пропаганде».

Параллельно 26 июля 2016 г. Президент США утвердил директиву относительно координации действий органов власти в случае

²⁸⁵ Strategy for Operations in the Information Environment // US Department of Defense. June 2016. 20 p. URL: <https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf> (дата обращения: 11.11.2020); Подробнее о содержании стратегии см. Соколов Р. Стратегия действий Министерства обороны в информационной сфере / Р. Соколов // Зарубежное военное обозрение. 2017. № 8. С 10-12.

киберинцидентов²⁸⁶, в которой вводилось понятие «значительного киберинцидента» как одной или нескольких кибератак, способных нанести ущерб интересам национальной безопасности, внешним сношениям или экономике Соединённых Штатов либо общественному доверию, гражданским свободам, здравоохранению и безопасности американского народа. Для эффективного реагирования на подобные киберинциденты директивой создавалась подотчётная помощнику Президента по внутренней безопасности и контртерроризму Группа киберреагирования при Совете национальной безопасности с полномочиями координации общей политики и стратегии государства относительно подобных киберинцидентов, а также Объединённая группа киберкоординации как межведомственная структура, осуществляющая оперативную координацию работы по реагированию на значительные киберинциденты между государственными органами и партнёрами из частного сектора. При этом основная ответственность за работу по отражению угроз подобных киберинцидентов возлагалась на Министерство юстиции посредством Федерального бюро расследований и Национальную объединённую рабочую группу по киберрасследованиям, за защиту объектов и инфраструктуры – на Министерство внутренней безопасности посредством Национального интегрированного центра кибербезопасности и коммуникаций, а за разведывательную поддержку и связанные меры – на Офис начальника национальной разведки посредством Интегрированного центра разведки в сфере киберугроз.

На институциональном направлении, тем не менее, процесс продвигался не так стремительно, как того желали антироссийские представители американского истеблишмента. Администрация Б. Обамы продолжала реализацию уже принятых законодательных актов, но не спешила с созданием новых официальных структур по борьбе с российской пропагандой и

²⁸⁶ Presidential Policy Directive -- United States Cyber Incident Coordination // The White House. 26 July 2016. URL: <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident> (дата обращения: 11.11.2020)

дезинформацией. Основная часть принимаемых мер касалась выделения финансирования на работу с медиасферой и гражданским обществом стран, потенциально подверженных российской пропаганде, однако это происходило преимущественно по двусторонним, как правило, неправительственным каналам и на ситуативной основе. К примеру, 10 августа 2015 г. было сообщено о выделении американским Правительством полумиллиона долларов на 12-месячный тренинг для обучения русскоязычных журналистов Прибалтики противостоять «российской пропаганде», ориентированной на русскоязычные меньшинства Прибалтики²⁸⁷.

Параллельно, в американских СМИ набирает обороты кампания по раскрыванию темы «русских ботов и троллей», якобы используемых Кремлём для оказания подрывного влияния на западное информационное пространство и общественное мнение. Летом 2015 г. газета New York Times опубликовала весьма спорное расследование Адриана Чена²⁸⁸, увязывающее косвенным образом распространение неправдивых слухов о техногенных авариях в США с деятельностью расположенного в Санкт-Петербурге «Агентства Интернет-исследований», спонсором которого называли якобы приближённого к Президенту Российской Федерации В.В. Путину ресторатора Е.В. Пригожина. Незадолго до этого Агентство получило скандальную известность благодаря обнародованию взломанной внутренней документации и разоблачению со стороны внедрённой активистки Л. Савчук²⁸⁹. На самом деле, акцентирование будто бы заказного и управляемого размещения комментариев с пророссийской позицией по украинскому вопросу в СМИ и соцсетях стало эффективным приёмом по дискредитации данной позиции в целом как недобровольной, не разделяемой даже российским обществом и не соответствующей

²⁸⁷ U.S. to Spend \$500,000 Training Baltic Journalists to Counter Russian Propaganda // The Moscow Times. 10 August 2015. URL: <https://www.themoscowtimes.com/2015/08/10/us-to-spend-500000-training-baltic-journalists-to-counter-russian-propaganda-a48855> (дата обращения: 11.11.2020)

²⁸⁸ Чен А. Агентство / А. Чен // The New York Times Magazine. 4 June 2015. URL: <https://www.nytimes.com/2015/06/07/magazine/the-agency-russian.html> (дата обращения: 11.11.2010)

²⁸⁹ Люда и тролли: Как петербурженка борется с «фабрикой кремлеботов» Петербурженка Людмила Савчук судится с «фабрикой троллей» на улице Савушкина. The Village узнал, как живёт женщина, решившая сломать систему пропаганды// The Village. 11 июня 2015. URL: <https://www.the-village.ru/village/city/situation/216161-fabrika-trolley> (дата обращения: 11.11.2020)

действительности. Расширение этой технологии и приписывание заказного и управляемого характера практически любым критическим для западного мейнстрима точкам зрения стало логическим продолжением уже запущенной кампании, а скомпрометированное Агентство с чуть ли не прямым, по мнению расследователей, кремлёвским подчинением превратилось в удобную мишень для обвинений сначала на уровне масс-медиа, а затем и на уровне политической экспертизы.

Резонанс вокруг данной тематики, спровоцированный ходом президентской гонки в США, вынуждал действующую американскую администрацию идти на хотя бы формальные шаги по нейтрализации предполагаемой угрозы.

Так, к концу своего второго президентского срока Обама санкционировал формирование специальной структуры по противодействию «российской информационной угрозе». В марте 2016 г. исполнительным Указом Президента был учреждён Центр глобального взаимодействия (*GEC*), призванный отвечать за руководство усилиями правительства США по борьбе с пропагандой и дезинформацией со стороны международных террористических организаций и зарубежных стран²⁹⁰. Центр создавался как самостоятельный орган, подотчётный Госсекретарю. В тексте Указа изначально российская пропаганда среди объектов работы Центра не упоминалась.

Одновременно с этим, 16 марта 2016 г., в Сенат был подан законопроект Р. Портмана «Акт о противодействии информационной войне»²⁹¹, а 10 мая 2016 г. он поступил на рассмотрение Палаты представителей от группы конгрессменов-республиканцев под названием «Акта о противодействии иностранной пропаганде и дезинформации»²⁹². В нём предлагалось

²⁹⁰ Executive Order 13721 of March 14, 2016 Developing an Integrated Global Engagement Center to Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584 // US Government Information. URL: <https://www.govinfo.gov/content/pkg/CFR-2017-title3-vol1/pdf/CFR-2017-title3-vol1-eo13721.pdf> (дата обращения: 11.11.2020)

²⁹¹ S. - 2692. To counter foreign disinformation and propaganda, and for other purposes. Draft law introduced by R. Portman on 16 March 2016 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/senate-bill/2692/> (дата обращения: 11.11.2020)

²⁹² H.R.5181 - Countering Foreign Propaganda and Disinformation Act of 2016. Draft law introduced by M. Kinzinger et al. on 10 May 2016 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/house-bill/5181/> (дата обращения: 11.11.2020)

зафиксировать в качестве позиции Конгресса положения о том, что руководство РФ и КНР используют дезинформацию и другие инструменты пропаганды для нарушения целей национальной безопасности США, их ключевых союзников и партнёров; что РФ, в частности, недавно провела сложную и масштабную дезинформационную кампанию с целью произвести дестабилизирующий эффект в отношении союзников и интересов США; что за последнее десятилетие дезинформация превратилась в ключевую особенность реализации политических, экономических и военных целей политики Правительства Российской Федерации на Украине, в Молдавии, Грузии, на Балканах и по всей Центрально-Восточной Европе; что вызов, связанный с противодействием дезинформации, выходит за рамки налаживания эффективных стратегических коммуникаций и публичной дипломатии и требует применения всех элементов национального могущества; что Правительство США должно разработать всеобъемлющую стратегию противодействия иностранной дезинформации и пропаганде и утвердить своё лидерство в выработке *«стратегического нарратива, основанного на фактах»*; что важным элементом этой стратегии должна стать защита и поддержка независимых СМИ в странах, уязвимых перед иностранной пропагандой. В практическом плане в законопроекте выдвигалась инициатива создания Центра информационного анализа и реагирования как межведомственного органа, призванного координировать сбор и анализ сведений об информационных кампаниях иностранных государств, сформировать методику интеграции критически важных данных для выработки национальной стратегии и разрабатывать государственную политику в сфере выявления и противодействия иностранной пропаганде. Непосредственно руководить Центром, по замыслу конгрессменов, должен был назначаемый Госсекретарём координатор, а общие рамки его деятельности должны были задаваться управляющим комитетом с участием представителей всех задействованных в этой сфере органов власти. Центру предлагалось выделить 20 млн. долларов на ближайшие два года для организации грантового

взаимодействия с организациями гражданского общества стран, наиболее подверженных влиянию деструктивной пропаганды.

Прохождение данного законопроекта в комитетах по иностранным делам обеих палат оказалось весьма проблематичным, и 14 июля 2016 г. те же авторы подают в Сенат обновлённый проект²⁹³ того же акта с некоторыми немаловажными коррективами. Так, из него уже был изъят раздел с общей позицией Конгресса, несущий слишком резкие политические оценки. И, в то же время, в описании функций предлагаемого Центра информационного анализа и реагирования было зафиксировано, что деятельность Центра будет направлена исключительно на оказание влияния на зарубежные аудитории, тогда как никакие средства или виды работы Центра не могут иметь намерением повлиять на общественное мнение в самих Соединённых Штатах. Это приводило данный законопроект в соответствие с другими правовыми актами США, в частности с законом о праве на неприкосновенность частной жизни 1974 г. и др., запрещающими органам государственной власти собирать персональные данные граждан и проводить скрытые операции по воздействию на общественное мнение внутри страны²⁹⁴. Значительно, до 250 млн. долларов, увеличивалась сумма средств, которые могли быть выделены Центру для осуществления его функций. А назначение межведомственного управляющего Центром было возложено на Президента США.

Тем не менее, даже в откорректированном виде проект Акта о противодействии иностранной пропаганде и дезинформации некоторое время оставался без продвижения, и только подключение к этой теме военного и разведывательного сообществ в начале ноября 2016 г. дало толчок активизации его рассмотрения в Конгрессе. Так, 9 ноября, сразу после оглашения итогов президентских выборов, в Пентагоне прошло масштабное обсуждение тематики

²⁹³ S.3274 - Countering Foreign Propaganda and Disinformation Act. Draft law introduced by R. Portman on 14 July 2016 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/senate-bill/3274> (дата обращения: 11.11.2020)

²⁹⁴ Tucker P. The US Is Losing at Influence Warfare. Here's Why // Defense One. 5 December 2016. URL: <https://www.defenseone.com/threats/2016/12/us-losing-influence-warfare-heres-why/133654/> (дата обращения: 11.11.2020)

информационно-психологических операций с участием ведущих представителей академических и экспертных кругов, на которой был поднят вопрос о необходимости совершенствования государственной политики в сфере противодействия иностранной пропаганде с использованием не только рациональных аргументов убеждения аудитории, но и психоэмоциональных манипуляций и приёмов²⁹⁵. Благодаря этому уже к концу ноября 2016 г. Сенат с подачи комитета по разведке включил основные положения законопроекта в текст закона об ассигнованиях на национальную оборону на 2017 г.²⁹⁶, 2 декабря 2016 г. он был принят в целом Палатой представителей, а 8 декабря 2016 г. - Сенатом. 23 декабря 2016 г. закон подписал Президент США Б. Обама.

В содержательном плане принятые в законе положения (раздел 1287) несколько отличались от предложенного в июльском (2014 г.) варианте проекта. В законе речь шла об учреждении не самостоятельного межведомственного органа, а подразделения Госдепартамента США, коим уже являлся Центр глобального взаимодействия. Его цель была прописана скромнее: направлять, синхронизировать и координировать усилия федерального правительства по распознаванию, пониманию, разоблачению иностранной государственной и негосударственной пропаганды и дезинформации, подрывающей интересы национальной безопасности США. Глава Центра должен был назначаться Президентом, вопрос о межведомственном управляющем комитете также был вынесен за рамки закона. Бюджет Центра предполагалось установить на уровне 160 млн. долларов на два года, причём эта сумма должна была быть передана из бюджета Министерства обороны. В тексте также наличествует ряд ограничителей, предотвращающих использование полномочий и ресурсов Центра в целях оказания влияния на внутреннюю американскую аудиторию. Примечательно, что в ходе обсуждения данного закона потерпевшая поражение

²⁹⁵ Там же.

²⁹⁶ S.2943 - National Defense Authorization Act for Fiscal Year 2017 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/senate-bill/2943> (дата обращения: 11.11.2020) ; Timber C. Effort to combat foreign propaganda advances in Congress / C. Timber // The Washington Post. 30 November 2016. URL: https://www.washingtonpost.com/business/economy/effort-to-combat-foreign-propaganda-advances-in-congress/2016/11/30/9147e1ac-e221-47be-ab92-9f2f7e69d452_story.html (дата обращения: 11.11.2020)

на президентских выборах Хиллари Клинтон заявила, что ожидающий принятия законопроект *«усилит реакцию правительства на иностранную пропаганду»*, по её словам, было *«крайне важно, чтобы лидеры как частного, так и государственного секторов предприняли шаги для защиты нашей демократии и невинных жизней»*²⁹⁷.

Подобный приём, с включением спорных законодательных инициатив в закон об ассигнованиях на национальную оборону, будет в дальнейшем неоднократно применяться американским Конгрессом для «пакетного» продвижения данных инициатив вопреки позиции отдельных комитетов или администрации Президента.

Несмотря на то, что создание Центра глобального взаимодействия и наделение его конкретными полномочиями в сфере противодействия иностранной пропаганде представляло собой значительный шаг вперёд в плане развития институциональной инфраструктуры борьбы с «российской информационной угрозой», принятые в законе на 2017 г. положения получили немалую долю критики как потенциально способные привести к усилению правительственного контроля за независимыми СМИ. Прямо или косвенно данная критика была направлена на то, чтобы максимально передать полномочия в области борьбы с иностранной пропагандой негосударственным организациям и представителям гражданского общества, якобы не имеющим непосредственного политического интереса и работающим только ради защиты демократических ценностей как таковых²⁹⁸.

Помимо учреждения Центра глобального взаимодействия и утверждения его бюджета, Б. Обама под занавес своего срока одобрил ещё две меры, имеющие прямое отношение к борьбе с «российской информационной угрозой». Во-первых, он поручил разведслужбам страны подготовить специальный доклад о

²⁹⁷ Robertson A. Hillary Clinton says 'lives are at risk' because of fake news / A. Robertson // The Verge. 8 December 2016. URL: <https://www.theverge.com/2016/12/8/13893000/hillary-clinton-pizzagate-fake-news-lives-at-risk> (дата обращения: 11.11.2020)

²⁹⁸ Hall H. K. The new voice of America: Countering Foreign Propaganda and Disinformation Act / H. K. Hall // First Amendment Studies. 2017. Vol. 51, No. 2. P. 56.

вмешательстве в прошедшие президентские выборы. А, во-вторых, 28 декабря 2016 г. он подписал Указ, дополняющий перечень действий в киберсфере, подлежащих санкциям со стороны Вашингтона, пунктом о манипуляции информацией с целью вмешательства или подрыва избирательного процесса или институтов²⁹⁹.

Таким образом, на этапе 2014-2016 гг. в США при значительном присутствии дискурса о «российской информационной угрозе» в публичном пространстве на официальном национальном уровне были предприняты лишь ограниченные действия в направлении нейтрализации данной «угрозы». Она была частично закреплена на законодательном уровне и на уровне общего военно-стратегического мышления, однако не стала отдельным поводом для санкций и долгое время не была полноценно институционализована в системе исполнительной власти страны. В рамках данной системы функции, связанные с отражением гипотетической «российской информационной угрозы», в различной мере распределялись между тремя узловыми центрами – Госдепартаментом, Пентагоном и разведывательным сообществом. Решающую роль в продвижении данной «угрозы» в американском публичном и политическом пространстве сыграл Конгресс, инициативы которого в данной сфере были поддержаны администрацией Б. Обамы по мере роста резонанса этой тематики на фоне избирательной кампании 2016 г.

Европейские государства

Европейские члены ЕС и НАТО более или менее активно следовали общей линии на развязывание информационной войны, иногда опережая союзников и подавая пример, иногда подчиняясь общему вектору. Среди европейских государств выделяется группа наиболее активных участников антироссийской кампании, которые не только инициировали принятие соответствующих решений на международном уровне, но и сами прибегли к ограничительным

²⁹⁹ Executive Order 13757 of December 28, 2016. Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities // US Treasury. URL: https://home.treasury.gov/system/files/126/cyber2_eo.pdf (дата обращения: 11.11.2020)

мерам в отношении российских медиа задолго до того, как общие решения были претворены в жизнь. В эту группу входят страны Прибалтики, Польша, Великобритания, Швеция, Нидерланды. Однако нужно признать, что на этапе 2015-2016 гг. такие меры носили преимущественно ситуативный, точечный характер и не приобрели повсеместного масштаба. В этот период происходило публичное дискурсивное признание политическими лидерами отдельных стран наличия вызова «кремлёвской пропаганды», выдвигались инициативы и принимались базовые решения о необходимости выработки способов реагирования на него, как правило, во взаимодействии с экспертами из негосударственных аналитических структур.

Ограничительные меры были приняты главным образом восточноевропейскими странами, тогда как государства Западной Европы только инициировали рассмотрение этого вопроса.

Так, 21 марта 2014 г. комиссия по теле- и радиовещанию *Литвы* ограничила вещание на территории страны телеканала *НТВ-мир* на три месяца, а 6 марта 2015 г. Президент Литвы Д. Грибаускайте сообщила в интервью ВВС, что её страна уже подвергается российской атаке, поскольку имеет место первая фаза конфронтации – информационная война, пропаганда и кибератаки³⁰⁰.

8 апреля 2014 г. Национальный совет по электронным масс-медиа *Латвии* ограничил на три месяца трансляцию телеканала *Россия*. Оправдывая своё решение тем, что российское телевидение распространяет неверную либо полную ненависти информацию, они сожалели, что законодательство всего ЕС не позволяет отдельным членам блокировать нелегальную информационную активность, если её распространитель регистрируется в какой-то другой стране Евросоюза³⁰¹. 29 марта 2016 г. власти Латвии предприняли новый шаг по

³⁰⁰ Lithuania 'already under attack' - President Grybauskaitė // BBC News. 6 March 2015. URL: <https://www.bbc.com/news/av/world-europe-31773941/lithuania-already-under-attack-president-grybauskaitė> (дата обращения: 11.11.2020); Collier M. Nato allies come to grips with Russia's 'hybrid warfare' / M. Collier, M. Sibierski // The Nation. 19 March 2015. URL: <https://nation.com.pk/19-Mar-2015/nato-allies-come-to-grips-with-russia-s-hybrid-warfare?show=836> (дата обращения: 11.11.2020)

³⁰¹ В Латвии на три месяца ограничат трансляцию телеканала "Россия" // РИА Новости. 3 апреля 2014. URL: <https://ria.ru/20140403/1002422950.html> (дата обращения: 11.11.2020)

перекрытию доступа к материалам российских СМИ – заблокировали сайт агентства *Sputnik* в национальной доменной зоне *.lv*, сославшись на постановления Совета ЕС «Об ограничительных мерах в связи с угрозой территориальной целостности, суверенитета и независимости Украины»³⁰².

В сентябре 2015 г. *Эстония* запустила новый русскоязычный телеканал»³⁰³, нацеленный на местное русское население.

Также страны Балтии объявили персонами нон-грата целый ряд известных российских экспертов, политтехнологов и звёзд шоу-бизнеса в связи с их якобы «империалистическими заявлениями».

В июле 2015 г. Национальный совет по телерадиовещанию *Польши* принял решение инициировать процедуру отзыва лицензии у *Радио Хобби* за ретрансляцию новостных блоков агентства *Sputnik*.

14 апреля 2016 г. сайты *Sputnik* на английском и турецком языках были заблокированы Управлением по телекоммуникации и связи *Турции* (доступ к сайтам был восстановлен 8 августа 2016 г., после потепления в отношениях между Россией и Турцией)³⁰⁴. В промежутке между этими двумя событиями, 14 июня 2016 г., было объявлено о том, что США помогут Турции создать «информационные войска гибридной войны с Россией», возьмут на себя часть финансирования и проведут обучение этих войск на Украине и в Прибалтике. В данном случае под информационными войсками имелись в виду не силы киберзащиты, а собственно силы информационного противостояния в узком понимании контроля за распространяемыми нарративами и пропагандой. Предполагалось, что свои операции турецкие инфовойска будут переносить на

³⁰² Власти Латвии заблокировали сайт *Sputnik* // Коммерсант. 29 марта 2016. URL: <https://www.kommersant.ru/doc/2950533> (дата обращения: 11.11.2020)

³⁰³ Ёлкина А. Общественное ТВ на русском: мост между общинами в Эстонии? / А. Ёлкина // Deutsche Welle. 26 ноября 2015. URL: <https://www.dw.com/ru/общественное-тв-на-русском-мост-между-общинами-в-эстонии/a-18875503> (дата обращения: 11.11.2020)

³⁰⁴ Турция стала второй страной после Латвии, которая заблокировала сайт российского информационного агентства *Sputnik* // Роскомсвобода. 15 апреля 2016. URL: <https://roskomsvoboda.org/16149/> (дата обращения: 11.11.2020)

территорию России, в них набирались лица, владеющие русским языком, а подчиняться они должны были турецкому Генштабу³⁰⁵.

Наиболее знаковой двусторонней инициативой в сфере борьбы с «российской информационной угрозой» стал совместный голландско-польский проект, выполненный по заказу Правительства *Нидерландов* командой медиа-экспертов Европейского фонда поддержки демократии. Его результаты были опубликованы в июне 2015 г. в виде документа «Обеспечение плюрализма и баланса в средствах массовой информации на русском языке – итоговые рекомендации», содержащий «Технико-экономическое обоснование инициатив СМИ на русском языке». Главным пунктом этих рекомендаций было предложение о создании пяти «строительных блоков» укрепления русскоязычных СМИ в регионе, а именно региональный новостной центр, «фабрику контента» развлекательного характера, центр совершенствования СМИ для мониторинга СМИ и подготовки журналистов, базовый фонд для финансирования данных структур из государственных и частных средств, и объединяющая все «блоки» платформа для распространения контента на максимально широкую аудиторию³⁰⁶.

Сформулированные предложения были приняты к исполнению. Уже 20 июля 2015 г. было объявлено о создании к последующему году русскоязычного информационного агентства – голландско-польской «фабрики контента» для противостояния российской пропаганде. Министр иностранных дел Нидерландов Берт Кёндерс заявил, что проект *«даст инструменты и возможности для работы русскоязычных [СМИ] и российских социальных сетей на основе объективной информации... с обменом разными точками зрения»*, а его польский коллега Гжегож Щетина пояснил, что проект предоставит ТВ, радио и онлайн-контент для использования русскоязычными

³⁰⁵ США создают информационные войска в Турции: мишень – Россия // Военно-политическая аналитика. 14 июня 2016. URL: <http://vpoanalytics.com/2016/06/14/ssha-sozdavut-informacionnye-vojska-v-turcii-mishen-rossiya/> (дата обращения: 11.11.2020)

³⁰⁶ Bringing Plurality & Balance to Russian Language Media - Final Recommendations // European Endowment for Democracy. 25 June 2015. URL: <https://www.democracyendowment.eu/en/news/551-bringing-plurality-balance-to-russian-language-media-final-recommendations.html> (дата обращения: 11.11.2020)

СМИ в Восточной Европе и в самой России. Этот проект был представлен двумя министрами на встрече министров иностранных дел ЕС в Брюсселе и получил поддержку коллег³⁰⁷, тогда как предложение Латвии об учреждении полноценного русского телеканала как альтернативного источника новостей было отклонено³⁰⁸.

Уже через две недели, 10 сентября, МИД Польши организовал конференцию доноров, посвящённую борьбе с российской пропагандой и призванную выполнить июньские рекомендации Европейского фонда поддержки демократии. Во встрече приняли участие делегаты из 35 стран ЕС, США и Канады. Нидерланды пообещали выделить 1,5 млн. евро, Польша – ещё 1 млн. евро. Нехватка средств снова заставила участников отказаться от создания полноценного русскоязычного телеканала и ограничиться запуском «фабрики контента»³⁰⁹, состоящей из трёх взаимосвязанных сайтов – Контент-Фонда для стран Восточного партнёрства³¹⁰, Балтийского центра развития СМИ³¹¹ и до сих пор не сформированной Платформы русскоязычных независимых СМИ³¹². Как представляется, результат более чем скромный по сравнению с заявленными амбициями.

Кроме того, некоторые европейские государства предприняли шаги по закреплению якобы исходящих от России «гибридной» и информационной угроз в своих доктринальных позиционных документах.

Так, в ноябре 2015 г. был опубликован обзор о Стратегии национальной безопасности *Великобритании* за 2015 г.³¹³, в котором упоминалось о

³⁰⁷ Rettman A. Dutch-Polish 'content factory' to counter Russian propaganda / A. Rettman // EU Observer. 21 July 2015. URL: <https://euobserver.com/foreign/129724> (дата обращения: 11.11.2020)

³⁰⁸ Panichi J. EU declares information war on Russia / J. Panichi // Politico. 27 August 2015. URL: <https://www.politico.eu/article/russia-propaganda-ukraine-eu-response-disinformation/> (дата обращения: 11.11.2020)

³⁰⁹ Rettman A. Poland hosts meeting on countering Russian propaganda / A. Rettman // EU Observer. 10 September 2015. URL: <https://euobserver.com/foreign/130192> (дата обращения: 11.11.2020)

³¹⁰ Фонд поддержки креативного контента/ URL: <https://contentfund.org/ru/> (дата обращения: 11.11.2020)

³¹¹ Балтийский центр развития СМИ. URL: <https://bcme.eu/ru/home> (дата обращения: 11.11.2020)

³¹² Free Press Unlimited. URL: <https://www.freepressunlimited.org/en/projects/russian-language-news-exchange-supports-independent-media> (дата обращения: 11.11.2020)

³¹³ A Secure and Prosperous United Kingdom. National Security Strategy and Strategic Defence and Security Review 2015 // UK Government. November 2015. 96 p. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf (дата обращения: 11.11.2020)

применяемой России манипуляции в медийном пространстве, однако более прямой увязки между Россией и информационной и киберугрозами в нём не содержится, несмотря на постоянные апелляции к «гибридной» тематике. При этом милитаризация информационной сферы в Великобритании обозначилась ещё раньше, когда в начале 2015 г. было объявлено о формировании так называемой 77-й бригады вооружённых сил – подразделения, призванного *«бросить вызов трудностям современной войны, с использованием как нелетальных действий, так и легитимных летальных невоенных рычагов в качестве средств изменения поведения противоборствующих сил и противников»*³¹⁴, а по сути - специального отряда информационно-пропагандистского воздействия, в том числе с помощью социальных сетей. Хотя в презентационных документах бригады нет прямого упоминания «российской информационной угрозы», её деятельность с самого начала включала изучение и анализ русскоязычной аудитории, в том числе, на примере стран Прибалтики³¹⁵.

Кроме того, Великобритания оказалась единственной западноевропейской страной, применившей негласные ограничительные меры в отношении российских СМИ уже на начальном этапе разворачивания системы противодействий «российской информационной угрозе». В конце 2014 г. британский медиарегулятор Офис коммуникаций (Ofcom) по итогам расследования жалоб телезрителей нашел «предвзятым» освещение телеканалом *RT* ряда тем, в том числе касательно ситуации на Украине³¹⁶. А в 2015 г. МИА «Россия сегодня» получило уведомление от банка *Barclays* о замораживании счёта в Соединённом Королевстве. В сентябре 2016 г. британский банк *Nat West* без всяких объяснений принял решение закрыть счета российского телеканала

³¹⁴ 77th Brigade. Influence and Outreach // UK Ministry of Defense. URL: <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/> (дата обращения: 11.11.2020)

³¹⁵ Свиридов В. Секретная британская 77-я бригада орудует на Украине? / В. Свиридов // Звезда. 7 декабря 2018. URL: <https://zvezdaweekly.ru/news/t/20181261330-nlqd7.html> (дата обращения: 11.11.2020); Miller C. Inside the British Army's secret information warfare machine / C. Miller // Wired. 14 November 2018. URL: <https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military> (дата обращения: 11.11.2020)

³¹⁶ Ofcom Broadcast Bulletin. Issue number 266 // UK Office of Communications. 10 November 2014. URL: https://www.ofcom.org.uk/_data/assets/pdf_file/0025/47635/obb266.pdf (дата обращения: 11.11.2020)

Russia Today (RT) в Великобритании, при этом ни в аппарате Премьера, ни в МИД, ни в Министерстве финансов фактически не стали комментировать сложившуюся ситуацию³¹⁷. Через несколько месяцев решение было отменено, но это не помешало Лондону предпринимать иные меры давления на канал *RT*.

Наряду с этим, гораздо более взвешенную позицию в отношении текущего конфликта продемонстрировали представители британского Парламента. Так, 10 февраля 2015 г., накануне подписания вторых Минских соглашений, Комитет по европейским делам Палаты Лордов выпускает доклад о состоянии и перспективах развития отношений между РФ и ЕС после украинского кризиса³¹⁸, в котором содержатся весьма объективные оценки и разумные рекомендации относительно необходимости договорного решения спорных вопросов при должном учёте интересов России и русского населения стран Восточного партнёрства, но ни разу не встречается упоминание российской «гибридной агрессии» или «дезинформации». Появление такого содержательного контента на уровне Комитета по европейским делам Палаты Лордов представляется нам довольно неожиданным, поскольку в нём отсутствует употребление пропагандистских клише и неадекватных реальности заявлений, которые в этот момент уже стали постепенно внедряться в английскую парламентскую риторику при изучении и анализе внешнеполитических процессов с участием России. 28 июня 2016 г. в Комитете по обороне Палаты Общин британского парламента был представлен доклад «Россия: выводы для обороны и безопасности Соединённого Королевства»³¹⁹. При том, что в нём воспроизведены все базовые элементы дискурса о «гибридной войне», включая пропаганду, дезинформацию и киберугрозы, а в качестве экспертов выступают П. Померанцев, Б. Ниммо и Дж. Шерр, итоговые рекомендации содержат не

³¹⁷ Гаврилина С. Государство и СМИ Великобритании: форма взаимодействия / С. Гаврилина, И. Сурма // Современная Европа. 2020. № 1. С. 53.

³¹⁸ The EU and Russia: before and beyond the crisis in Ukraine // House of Lords European Union Committee 6th report of Session 2014–15. 10 February 2015. URL: <https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/115/115.pdf> (дата обращения: 11.11.2020)

³¹⁹ Russia: Implications for UK defence and security // UK House of Commons Defence Committee. First Report of Session 2016–17. 28 June 2016. URL: <https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf> (дата обращения: 11.11.2020)

только конфронтационные призывы к выработке многоаспектной стратегии Великобритании и НАТО по эффективному противостоянию российской пропаганде и дезинформации, но и более конструктивные констатации необходимости уделять больше внимания пониманию российских интересов и проработке возможностей для сохранения каналов взаимодействия с РФ в приоритетных сферах сотрудничества.

Значительно более радикальный подход демонстрировали представители британских неправительственных экспертных кругов. Примерно в то же время, в октябре 2016 г. в помещении британского Парламента был представлен доклад британской НКО Общество Генри Джексона «Путинские полезные идиоты: левые, правые и Россия»³²⁰. В докладе клеймились любое взаимодействие британских политических деятелей с Россией, любые их высказывания с оправданием политики России на Ближнем Востоке и на Украине, выступления британских деятелей на телеканале *RT*, за которые они получали гонорары. Докладчики призвали к строгому контролю подобных связей.

29 июня 2016 г. Министерство обороны *Бельгии* опубликовало «Стратегическое видение обороны», в котором рассматривались «гибридные угрозы» на примере якобы дестабилизации Россией Украины и Грузии через поддержку противников местных режимов (с. 28), говорилось о дополнении натовского арсенала сдерживания невоенными средствами, которые позволяют бороться с гибридными угрозами (с. 41), и о том, что эти средства должны быть использованы для влияния на отношение и поведение специфических целевых групп, с целью локального и глобального выигрыша в военном плане (с. 102)³²¹.

По всей видимости, совпадение подобных документов по времени было приурочено к саммиту НАТО в Варшаве 8-9 июля 2016 г. Сразу после него, 13 июля, была опубликована «Белая книга по безопасности» *Германии*, в которой

³²⁰ Foxall A. Putin's Useful Idiots: Britain's Left, Right and Russia / A. Foxall // The Henry Jackson Society Russia Studies Centre. Policy Paper No. 10 (2016). 17 p. URL: <http://henryjacksonsociety.org/wp-content/uploads/2016/10/Putins-Useful-Idiots.pdf> (дата обращения: 11.11.2020)

³²¹ La vision stratégique pour la Défense (2016-2030) par CPV BEM Renaud FLAMANT Cellule Stratégie // Cabinet de la Défense et de la Fonction Publique. 8 juillet 2016. URL: https://www.cgsp-defense.be/Datas/Documents/Mil/Vision_Strategique_2030.pdf (date d'accèsion 11.11.2020)

говорилося, що з допомогою наростаючого використання гібридних інструментів, намеренно призваного стереть границі между войной и миром, Россия создаёт неопределённость в отношении своих намерений³²². Як видим, німецькі формулювання відносно намерень Росії залишалися більш м'якими, ніж у країн, ініціювавших інформаційну війну, однак німецькі політики вже були готові прийняти обвинительную в отношении Кремля інтерпретацію подій.

В жовтні 2015 г. Президент **Фінляндії** Саулі Нііністє признав реальність інформаційної війни для своєї країни і призвав кожного громадянина поучаствовать в її отраженні. В січні 2016 г. адміністрація Прем'єр-міністра країни оголосила про залученні додатково близько ста чиновників для участя в програмі по виявленню і розпізнаванню дезінформації в фінському публічному просторі³²³.

Наконець, 20 жовтня 2016 г. Міністр внутрішніх справ **Чехії** оголосив про створенні підрозділу з 20 співробітників для боротьби з «російською пропагандою» і *«другими спробами ззовні впливати на громадське мнієння в країні, являючоїся членом Європейського Союзу і НАТО»*³²⁴. Заявлення він зробив на конференції, присвяченій «стратегічним комунікаціям» з участю гостей з Великобританії, Німеччини, Швеції, Фінляндії, США, Словаччини, Польщі, Нідерландів, Прибалтики, НАТО і ЄС, представителів силових структур, наукових кіл, дипломатів і НКО. Завданням підрозділу повинна була стати боротьба з *«ложными сведениями в открытом доступе»*, а також навчання чиновників швидкому реагуванню на випадки

³²² White Paper on German Security Policy and the Future of the Bundeswehr 2016 // The Federal Government. 13 July 2016. URL : [https://issat.dcaf.ch/download/111704/2027268/2016 White Paper.pdf](https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf) (дата звернення: 11.11.2020)

³²³ Standish D. Why Is Finland Able to Fend Off Putin's Information War? / D. Standish // Foreign Policy. 1 March 2017. URL : <https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/> (дата звернення: 11.11.2020)

³²⁴ Вендик Ю. Кремлевская пропаганда и тщетность борьбы с ней / Ю. Вендик // BBC News. Русская служба. 30 ноября 2016. URL: <https://www.bbc.com/russian/features-38145898> (дата звернення: 11.11.2020) ; Шаталін В. В Чехії починають боротьбу з російською пропагандою / В. Шаталін // Deutsche Welle. 21 жовтня 2016. URL: <https://www.dw.com/ru/в-чехии-начинают-борьбу-с-российской-пропагандой/a-36108805> (дата звернення: 11.11.2020) ; Centre Against Terrorism and Hybrid Threats // Czech Republic Ministry of Interior Affairs. URL: <https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx> (дата звернення: 11.11.2020)

«дезинформации» путём их удаления из публичного доступа. К работе предполагалось привлекать соцсети.

Выводы по главе 2

1. Период 2014-2016 гг. стал начальным этапом построения системы противодействия «российской информационной угрозы» на Западе, в ходе которого генерируемый номинально независимыми экспертами дискурс был довольно быстро поддержан сначала правительствами отдельных европейских государств, а затем и структурами НАТО. Давление со стороны обеих групп акторов привело к подключению Европейского союза к процессу создания институциональной инфраструктуры для борьбы с «российской информационной угрозой». При том, что после украинского кризиса значимость и деструктивный потенциал данной угрозы в восприятии западного политического класса резко возросли, формирование институциональной инфраструктуры для её нейтрализации происходило в ориентации на её ограниченный масштаб: она воспринималась как непосредственно затрагивающая только русскоязычное пространство и страны с многочисленным русским населением.
2. Международные организации, призванные контролировать соблюдение свободы слова и независимости СМИ в Европе, на начальном этапе сыграли деструктивную роль в разворачивании конфронтации в информационной сфере, способствовав вынесению тематики «российской пропаганды» на международную повестку дня уже весной 2014 г. и не препятствуя её дальнейшему продвижению в ущерб общепринятым демократическим правам и свободам. Совет Европы в лице своей Парламентской Ассамблеи принял резолюции, отвергающие пророссийскую трактовку событий украинского кризиса и осуждающие якобы предвзятую позицию российских СМИ в ходе их освещения. Представитель ОБСЕ по свободе СМИ, призывая все заинтересованные стороны сохранять объективность и не прибегать к ограничению работы медиа, не осудила ограничительные меры в отношении

российских СМИ, введенные новыми властями Украины и правительствами стран Балтии уже весной 2014 г.

3. Выступив в качестве локомотива в дискурсивном признании и утверждении якобы исходящих от России «гибридных угроз» безопасности Запада летом-осенью 2014 г., Североатлантический альянс пошёл по пути частичной институционализации в своей структуре функций, связанных с отражением данных угроз, в том числе в их информационной составляющей. С одной стороны, для противодействия «российской информационной угрозе» были задействованы уже существующие органы – открытый в 2008 г. Центр по сотрудничеству в сфере киберобороны в Таллине и открытый в 2014 г. Центр передового опыта в области стратегических коммуникаций в Риге. Оба центра были созданы по решению отдельных государств-членов НАТО и имеют статус военных органов вне интегрированного командования, утверждённый уже после их создания. С другой стороны, высшие чиновники НАТО в рассматриваемый период прикладывали основные усилия к тому, чтобы стимулировать Европейский союз взять на себя ведущую ответственность за отражение «гибридных угроз» и тем самым максимально вовлечь его в организацию сдерживания и противодействия России в информационной и других невоенных сферах.

При этом Альянс включил киберпространство и «гибридные угрозы» в сферу своей оперативной ответственности, но отвёл себе лишь вспомогательную роль в процессе реагирования на них. Так, в документах Варшавского саммита НАТО 2016 г. была прописана возможность задействовать гарантии статьи 5 Вашингтонского договора в ответ на вызовы «гибридной войны», но, в то же время, говорилось, что главная ответственность за реагирование на «гибридные угрозы и атаки» возлагается на подвергшееся им государство, тогда как НАТО готово лишь оказать помощь любому союзнику на любой стадии гибридной кампании.

4. Включение Евросоюза в систему противодействия «российской информационной угрозе» происходило постепенно, начиная с весны 2015 г.,

под влиянием немалого публичного давления со стороны некоторых государств-членов, НАТО и ряда негосударственных аналитических организаций и «мозговых центров». Работа по определению функций ЕС в рамках данной системы и закреплению их в институциональной структуре Евросоюза проводилась на двух направлениях: реагирование на вызов «российской пропаганды и дезинформации» для политики ЕС в восточном соседстве и создание потенциала для отражения «гибридных угроз» в целом. На первом направлении институционализация произошла довольно быстро, путём формирования летом 2015 г. Оперативной рабочей группы по стратегическим коммуникациям *East Stratcom* в рамках Европейской службы внешних действий, однако задачи данной группы формально были ограничены выявлением «российской дезинформации» в русскоязычном информационном пространстве. На втором направлении процесс продвигался медленнее ввиду необходимости концептуального осмысления феномена «гибридных угроз» как таковых и привлечения к этой работе Еврокомиссии.

Из всех коммунитарных органов Европейского союза наиболее активную роль в продвижении дискурса о «российской информационной угрозе» после украинского кризиса сыграл Европарламент, выступавший основной площадкой для вынесения данной тематики на уровень европейского публичного пространства и политической повестки дня ЕС. Наиболее значимый практический эффект в плане доктринального и институционального закрепления данного дискурса на уровне ЕС произвела Европейская служба внешних действий, функционеры которой в сжатые сроки подготовили доклады и планы действий касательно организации работы по противодействию «российской пропаганде» и отражению «гибридных угроз». Наименьшую активность в деле усиления конфронтации с Россией в информационной сфере на начальном этапе проявила Еврокомиссия.

В доктринальном плане в 2015-2016 гг. Евросоюз значительно продвинулся по пути признания актуальности информационных и «гибридных» угроз, однако на уровне базовых позиционных документов, принятых в рассматриваемый период (в первую очередь Глобальной стратегии ЕС 2016 г.), прямая увязка этих угроз с Россией была ослаблена. Тем не менее, эти документы институционализировали механизм информационного противостояния, создавая дополнительные каналы влияния и аргументационную базу для антироссийских сил, заинтересованных в усилении и поддержании конфронтации Запада с Россией в информационной сфере.

5. Борьба с «российской пропагандой и дезинформацией» в НАТО и Европейском союзе, согласно официальным заявлениям их высших функционеров, была организована не вокруг императивных ограничительных мер или ведения ответной контрпропаганды, а вокруг выявления фактов и источников распространения подобной «дезинформации», их своевременного опровержения, повышения «сознательности» самих СМИ и «медиаграмотности» общественности. На практике подобный подход означал регулярную публичную стигматизацию любых фактов и оценок, не вписывающихся в западный нарратив украинского кризиса и последующих событий, в том числе, официальной позиции российского руководства, как ложных, не заслуживающих внимания, основанных на недостоверной информации и «пропагандистских мифах».
6. На этапе 2014-2016 гг. в США при значительном присутствии дискурса о «российской информационной угрозе» в публичном пространстве на официальном национальном уровне были предприняты лишь ограниченные действия в направлении нейтрализации данной угрозы. Она была частично закреплена на законодательном уровне и на уровне общего военно-стратегического мышления, однако не стала отдельным поводом для санкций и долгое время не была полноценно институционализирована в системе

исполнительной власти страны. В рамках данной системы функции, связанные с отражением гипотетической «российской информационной угрозы», в различной мере распределялись между тремя узловыми центрами – Госдепартаментом, Пентагоном и разведывательным сообществом. Решающую роль в продвижении данной угрозы в американском публичном и политическом пространстве сыграл Конгресс, инициативы которого в данной сфере были поддержаны администрацией Барака Обамы по мере роста её резонанса на фоне избирательной кампании 2016 г. Наиболее значимой стала инициатива создания в структуре Госдепартамента специального органа для противодействия иностранной пропаганде – Центра глобального взаимодействия, принятая законодательно путём включения в закон о военном бюджете на 2017 г.

7. На уровне национальных государств на начальном этапе оформления системы противодействия «российской информационной угрозе» можно было наблюдать четыре типа предпринимаемых шагов: а) публичное дискурсивное признание политическими лидерами отдельных стран наличия вызова «кремлёвской пропаганды», б) доктринальное закрепление в позиционных и программных документах общеполитического или, чаще, военно-стратегического характера, в) создание специальных постоянных органов или ситуативных рабочих групп, г) введение ограничительных мер в отношении российских СМИ, общественных организаций или отдельных граждан. Данные шаги, впрочем, носили преимущественно ситуативный, точечный характер и не приобрели повсеместного масштаба. Ограничительные меры были приняты главным образом восточноевропейскими странами, тогда как государства Западной Европы только инициировали рассмотрение этого вопроса и, в некоторых случаях, признавали факт наличия якобы исходящих от России «гибридных угроз» в позиционных и доктринальных документах.
8. Среди европейских государств систематические усилия по формированию системы противодействия «российской информационной угрозе» прилагали

Польша, страны Прибалтики, Великобритания, Нидерланды и скандинавские страны. Они не только первыми приняли ограничительные или запретительные меры в отношении российских СМИ, но и регулярно инициировали рассмотрение данного вопроса на уровне ведущих межправительственных органов ЕС и НАТО, настаивали на создании в рамках западных межгосударственных институтов специальных подразделений, призванных осуществлять информационное противодействие России, оперативно организовали финансирование этих подразделений и направили в них своих представителей.

Глава 3. Развитие институционального измерения западной системы противодействия «российской информационной угрозе» после президентских выборов в США (2017-2019 гг.)

Драматические перипетии президентских выборов в США в 2016 г. привели к значительному повышению внимания к теме «российской пропаганды и дезинформации» и переводу её из разряда вызовов политике Запада на русскоязычном пространстве в разряд угроз непосредственно самому западному сообществу, его ценностям и безопасности. Утверждение концепта «гибридной войны» и «гибридных угроз» в качестве элемента политического дискурса и доктринального аппарата в предшествующий период, а также формирование базовых политических и институциональных рамок для отражения подобных угроз на международном уровне в 2015-2016 гг. создали бюрократические возможности и каналы, которые позволили антироссийским силам добиваться поддержания и дальнейшего продвижения данной тематики в политической повестке Запада и включения в неё всё большего круга акторов различного уровня.

Развитие событий в период 2017-2019 гг. отличалось тремя магистральными тенденциями.

Во-первых, переходом от общих концептуальных дебатов о сущности «гибридной агрессии» России к выработке практических мер в конкретных областях. Причём в условиях затухания военных действий на Донбассе и отсутствия явных признаков агрессивных военных планов Москвы в других регионах информационная сфера вышла на первый план как основное поле предполагаемого задействования «гибридных» методов против западных государств и обществ, тогда как тема использования непосредственно военных инструментов «гибридного» арсенала, парамилитарных формирований и так называемых «прокси-сил» несколько отошла на второй план.

Во-вторых, переходом от общих политических обвинений России в ведении «гибридной войны» в информационной сфере и распространении деструктивной пропаганды к инициированию конкретных санкций против лиц и компаний, якобы причастных к этому процессу, и введению иных ограничительных мер по отношению к российским СМИ.

И, в-третьих, активизацией усилий по выстраиванию соответствующей инфраструктуры на национальном уровне системы противодействия «российской информационной угрозе». Необходимость вовлечь в активизацию данной системы ведущие западные государства и добиться от них решений по формализации и институционализации обязательств по противодействию России побуждала её архитекторов делать упор на тех событиях и процессах, которые можно было бы представить как угрозу национальной безопасности конкретного государства и потребовать от его правительства соответствующей реакции. Увязывание «российской информационной угрозы» с электоральными процессами выступало весьма эффективным инструментом решения данной задачи.

Поэтому в данном разделе мы рассмотрим сначала ход эволюции западной системы информационного противодействия России на национальном уровне, а затем - на уровне международных структур.

3.1. Развитие механизмов противодействия «российской информационной угрозе» в США после избрания Д. Трампа

Ход избирательной кампании в США в 2016 г. с самого начала ознаменовался повышенным вниманием к российской тематике. В условиях, когда конфронтационный курс по отношению к России едва закрепился как элемент общезападного политического консенсуса, даже минимальные сомнения относительно оправданности этого курса в публичном пространстве представлялись недопустимым отклонением и чуть ли не нарушением этого консенсуса в целом. Вполне закономерно, что часть политических сил Запада,

противопоставляющих себя так называемому «мейнстриму», взяла на вооружение менее агрессивную риторику в отношении России с открытым оспариванием действующего конфронтационного курса для того, чтобы дополнительно обозначить свою оппозицию либеральному консенсусу, в том числе, и в вопросах внешней политики.

Подобную тактику демонстрировали так называемые ультрарадикальные силы в ряде стран Евросоюза, её же взял на вооружение в ходе своей избирательной кампании Дональд Трамп. Причём в его исполнении критика российской политики администрации Обамы велась по двум, не во всём согласованным между собой линиям: с одной стороны, критиковался излишне конфронтационный характер отношений с Россией после украинского кризиса, с другой – недостаточная жёсткость в ходе самого кризиса, благодаря которой Россия якобы и получила возможность беспрепятственно нарушить международное право и присоединить Крым. Успехи Д. Трампа в ходе президентской кампании и его выдвижение единым кандидатом от Республиканской партии обострили споры вокруг его позиции в отношении России, в том числе в рядах его однопартийцев. Скомпрометировать Д. Трампа прямыми связями с российским руководством и возможной российской поддержкой в ходе избирательной кампании казалось выигрышным ходом для лишения его электоральных перспектив.

Разразившийся летом 2016 г. скандал со взломом сервера Национального комитета Демократической партии позволил противникам Д. Трампа задействовать подобную тактику и обвинить «русских хакеров» и непосредственно Кремль в прямом вмешательстве в избирательный процесс. Однако представить убедительные доказательства данного факта было трудно, поэтому ближе к самим выборам в американских СМИ, наряду с обвинениями во взломе сервера, была раскручена идея о влиянии на электоральные предпочтения граждан США с помощью распространения неправдивых сведений в социальных сетях «русскими ботами и троллями». Таким образом, Россия получила обвинения в применении двух новых методов из арсенала

«гибридной войны» в информационной сфере – киберагрессии на техническом уровне и использовании ботов и троллей на коммуникационном уровне.

На официальном уровне обвинение в адрес Москвы было выдвинуто в начале октября 2016 г. в совместном заявлении министерства внутренней безопасности и офиса директора национальной разведки³²⁵. Однако только после выборов Президент Б. Обама дал официальное поручение органам разведки провести и представить до окончания его срока расследование фактов российского вмешательства в избирательный процесс³²⁶.

Таким образом, был сформирован общий контекст нового витка раздувания «российской информационной угрозы» в период после избрания Дональда Трампа. Механизмом её раздувания в этот период стали регулярные нападки и обвинения Д. Трампа и некоторых его соратников в связях с Россией и отстаивании её интересов с якобы корыстными мотивами, озвучиваемые как на медийном и экспертном уровнях, так и на уровне официальных структур законодательной, а, в некоторых случаях, и исполнительной власти, а также силовых ведомств. Со своей стороны, администрация Д. Трампа и умеренные представители Республиканской партии, как будто стремясь показать несостоятельность этих обвинений, рано или поздно соглашались на очередной шаг в дальнейшей институционализации системы противодействия России – наложение новых санкций, принятие новых антироссийских законов, уход с занимаемых постов кадров, настроенных на сотрудничество с РФ.

Такое информационное сопровождение институционализации антироссийского курса дало ряду российских политиков основание для заявлений, будто российско-американские отношения стали заложником внутривнутриполитического противоборства в США³²⁷. Однако искусственность

³²⁵ Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. October 7, 2016. URL: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> (дата обращения: 11.11.2020)

³²⁶ Ahmed A. Sh. Obama To Receive A Report On Russia's 2016 Election Meddling Before Leaving Office / A. Sh. Ahmed // Huffpost. Dec 09, 2016. URL: https://www.huffpost.com/entry/obama-report-election-meddling-russia_n_584ad081e4b0e05aded380ff (дата обращения: 11.11.2020)

³²⁷ Путин назвал причину ухудшения российско-американских отношений // Известия. 17 июля 2018. URL: <https://iz.ru/767662/2018-07-17/putin-nazval-prichinu-ukhudsheniia-rossiisko-amerikanskikh-otnoshenii> (дата обращения: 11.11.2020)

обвинений в пособничестве России со стороны противников Д. Трампа и стабильное согласие обвинённых «доказать» своё враждебное отношение к России участием в укреплении антироссийского курса (вместо того, чтобы разобрать изначальную нелепость антироссийских конструкторов) показывают, что, скорее, наоборот: внутривластное противоборство в США накладывалось на относительно независимую от него и более мощную антироссийскую кампанию, лишь в какой-то мере выступив её катализатором. Тем более, что в самой администрации Д. Трампа единой позиции по «российскому вопросу» с самого начала не существовало, а среди назначенных Трампом высших должностных лиц присутствовали давние сторонники «жесткого курса» в отношении России.

В медийной сфере ведущими движущими силами этой кампании стали отдельные разведывательные, силовые и правоохранительные структуры, присоединившиеся к уже сформированному симбиозу антироссийски настроенных представителей законодательной власти, экспертной среды и СМИ. В рамках проводимой кампании упомянутые силы, во-первых, инициировали и реализовывали несколько одновременных расследований предполагаемого российского вмешательства в выборы и российских связей Дональда Трампа, наиболее резонансным из которых стало расследование спецпрокурора Роберта Мюллера³²⁸; во-вторых, оказывали давление на новую администрацию с тем, чтобы она воспользовалась санкционными механизмами в информационной сфере, введёнными Бараком Обамой на исходе его президентского срока; и, в-третьих, продвигали в Конгрессе законопроекты, нацеленные на закрепление действующих санкций против России и недопущение их ослабления без согласия Конгресса.

Представители разведсообщества играли в этом процессе роль источников «проверенной» информации касательно потенциала, намерений и практических

³²⁸ Хронику проводимых расследований в отношении избрания Д. Трампа см. в Кошкин П.Г. «Российское досье» как внутривластное фактор в США / П.Г. Кошкин // Россия и Америка в XXI веке. 2019. Специальный выпуск. URL: <https://rusus.jes.su/s207054760005318-6-1/> (дата обращения: 11.11.2020)

действий России, на основании которой сначала журналисты и эксперты, а затем и конгрессмены начинали требовать определённых шагов от новой администрации и выдвигать законопроекты, налагающие на неё правовые ограничения в сфере отношений с Россией. При этом обвинения в адрес России не ограничивались конкретным случаем вмешательства в американские выборы, наоборот, этот случай вписывался в уже выстроенный контекст «гибридной войны», якобы ведущейся Кремлём против Запада по всем фронтам, в рамках которой манипуляции в американском информационном пространстве выставлялись логическим продолжением стратегии использования пропаганды и дезинформации в русскоязычном пространстве.

Первым в серии шагов представителей разведсообщества стало обнародование 6 января 2017 г. доклада управления директора Национальной разведки США, в котором «с высокой степенью уверенности» утверждалось о личном указании В.В. Путина осуществить хакерские атаки на американские сети, что отражало *«давнее стремление Москвы подорвать общественное доверие к демократическому процессу в США»* и помочь победе Трампа над Клинтон³²⁹. Несмотря на отсутствие каких-либо доказательств, этот доклад придал доносившимся и ранее обвинениям о недопустимом вмешательстве России в дела Запада «официальный» статус и, в совокупности с обеспокоенной риторикой американских политиков, послужил достаточным обоснованием для повышения градуса противостояния с РФ³³⁰.

9 марта 2017 г. в Комитете по внешним делам Палаты представителей под председательством Эда Ройса прошли слушания на тему «Подрыв демократических институтов и раскалывание НАТО: цели российской дезинформации»³³¹, на которые в качестве свидетелей были приглашены

³²⁹ Как Россию обвиняли во вмешательстве в американские выборы. Досье // ТАСС. 31.10.2017. URL: <https://tass.ru/info/4324773> (дата обращения: 11.11.2020)

³³⁰ Fridman O. Russian "Hybrid Warfare": Resurgence and Politicization. Oxford: Oxford University Press, 2018.

³³¹ hearing before the committee on foreign affairs house of representatives one hundred fifteenth congress first session. March 9, 2017. Serial No. 115–7. URL: <https://docs.house.gov/meetings/FA/FA00/20170309/105674/HHRG-115-FA00-Transcript-20170309.pdf> (дата обращения: 11.11.2020)

представители американских «мозговых центров», разрабатывавшие концепции «российской гибридной войны», и бывший Президент Эстонии Томас Хендрик Ильвес, занимавший пост в 2007 г. Уже открывая собрание, Ройс задал основные параметры предстоящего обсуждения, целью которого было «подверстать» ранее разработанную концепцию «гибридной войны» и российских информационных операций к теме российских попыток нанести ущерб не только США, но и другим ключевым странам НАТО через вмешательство в их политическую систему. Единичный недоказанный случай вмешательства России в американские выборы, таким образом, вписывался в якобы уже реализуемую деструктивную стратегию и автоматически проецировался на остальные государства Запада.

Прогрессирующей раскрутке «российской информационной угрозы» не помешало даже признание директора ФБР Джеймса Коми и главы АНБ Майкла Роджерса об отсутствии у них прямых доказательств вмешательства России в американские выборы в ответ на вопрос главы комитета по разведке Палаты представителей Дэвида Ньюнса 20 марта 2017 г.³³² Несмотря на то, что Коми так и не смог предъявить доказательства вмешательства России и на слушаниях в юридическом комитете 3 мая³³³, деятельность заинтересованных сил смогла дать нужный импульс американской законодательной машине для форсированного формирования и финансирования борьбы с «российской информационной угрозой».

В начале мая 2017 г. обе палаты Конгресса одобрили бюджет американских разведывательных структур (закон подписан Президентом США 5 мая), предусматривающий создание спецкомитета для борьбы со «скрытым влиянием» России³³⁴. А 28 июня 2017 г. Агентство военной разведки (DIA) США

³³² Rogers, Comey say no evidence vote tallies were changed in 2016 election // The Washington Post. March 20, 2017. URL: https://www.washingtonpost.com/video/national/rogers-comey-say-no-evidence-vote-tallies-were-changed-in-2016-election/2017/03/20/9a764e16-0d8f-11e7-aa57-2ca1b05c41b8_video.html?noredirect=on&utm_term=.b8d09aeeceb9 (дата обращения: 11.11.2020)

³³³ Как Россию обвиняли во вмешательстве в американские выборы. Досье // ТАСС. 31.10.2017. URL: <https://tass.ru/info/4324773> (дата обращения: 11.11.2020)

³³⁴ Там же.

выпустило отчёт о военной мощи России, указывавший в качестве серьёзной проблемы для США со стороны России *«формирование информационной среды в соответствии с её интересами»* и пояснявший: *«Разнообразные инструменты распространения российской пропаганды включают прокремлёвские «новостные» сайты и теле- и радиоканалы, такие как Russia Today и Sputnik News, ботов и троллей в социальных сетях, поисковую оптимизацию и платных журналистов в западных и других зарубежных СМИ»*³³⁵. Тем самым осуществлялась гиперболизация российского стратегического потенциала за счёт включения в него инструментов «гибридной войны» на доктринальном уровне политики безопасности США.

Весна-лето 2017 г. стали периодом активизации законодательных инициатив, направленных на ограничение возможностей администрации Трампа в деле налаживания контактов с российским руководством и укрепление системы сдерживания и противодействия России. Так, 24 мая 2017 г. в Сенате США среди прочих был представлен законопроект *«О противодействии влиянию Российской Федерации в Европе и Евразии»*³³⁶, предусматривающий выделение 250 млн. долларов ежегодно в качестве фонда противодействия российскому влиянию, предназначенного для помощи *«наиболее уязвимым»* восточноевропейским и балканским странам (таким как: Украина, Румыния, Молдавия, Косово) в *«защите критической инфраструктуры и электоральных механизмов от российской киберпреступности, преодолении коррупции, укреплении законности, повышении возможностей гражданского общества, СМИ и НГО противодействовать влиянию пропаганды от Российской Федерации»*. По сути, речь шла о направлении дополнительных средств в рамках двусторонних программ сотрудничества со странами Восточной Европы в сфере

³³⁵ Russian Military Power Assessment // Defence Intelligence Agency. 2017 / p. 39. URL: <https://www.dia.mil/News/Articles/Article-View/Article/1232488/defense-intelligence-agency-releases-russia-military-power-assessment/> (дата обращения: 11.11.2020)

³³⁶ Countering Russian Influence in Europe and Eurasia Act of 2017. S.1221 // 115th Congress (2017-2018). URL: <https://www.congress.gov/bill/115th-congress/senate-bill/1221/text/is?overview=closed&format=txt> (дата обращения: 11.11.2020)

информационного противодействия России, а не на усиление соответствующих органов НАТО и ЕС.

После успешной личной встречи Президентов Д. Трампа и В.В. Путина на саммите Большой двадцатки в Гамбурге в июле 2017 г. Конгресс перешёл к окончательному утверждению уже частично одобренных законопроектов в этой области. Итогом необычайной активности законодателей стало принятие 2 августа комплексного законопроекта «О противодействии противникам Америки посредством санкций»³³⁷, сочетавшего в себе меры, предлагаемые во всех выдвинутых на тот момент антироссийских законопроектах. В приложении к информационной сфере санкционный закон, с одной стороны, закреплял уже действующие к тому моменту указы Барака Обамы от 1 апреля 2015 г. и 28 декабря 2016 г. и определял условия, при которых Президент может отменить введённые на основании данных указов санкции (раздел 222), а, с другой стороны, предписывает ему наложить санкции на а) любое физическое или юридическое лицо, целенаправленно предпринимающее серьёзные действия, которые подрывают кибербезопасность других лиц и демократических институтов и выступающее от имени Правительства Российской Федерации либо прямо или косвенно контролируется последним; б) любое физическое или юридическое лицо, целенаправленно оказывающее материальную, спонсорскую помощь, финансовую или технологическую поддержку вышеописанной деятельности; в) любое физическое или юридическое лицо, целенаправленно оказывающее финансовые услуги в поддержку вышеописанной деятельности (раздел 224). Конкретные санкции, которые могут применяться по данной статье, включают, во-первых, блокировку американской собственности и сделок в интересах попавших под санкции лиц и, во-вторых, депортацию с территории США и отзыв визы. Отмена данных санкций возможна на основании той же процедуры, что прописана в отношении санкций по указам Б. Обамы. Также в данном разделе приведено разъяснение относительно того, что подразумевается

³³⁷ H.R. 3364 (115th): Countering America's Adversaries Through Sanctions Act. URL: <https://www.govtrack.us/congress/bills/115/hr3364> (дата обращения: 11.11.2020)

под понятием *«серьёзные действия, которые подрывают кибербезопасность»*, а именно: значительные усилия, направленные на то, чтобы лишить доступа, нарушить работу или уничтожить информационную и коммуникационную технологическую систему или сеть либо добыть, изменить, нарушить или обнародовать информацию из такой системы или сети без надлежащего разрешения с целью проведения операций влияния или кражи фондов, экономических ресурсов, торговых секретов, личных данных либо финансовой информации ради коммерческой выгоды, получения конкурентного преимущества или частной финансовой выгоды. Примечательно, что в приведённом определении акцент сделан на экономико-технологическом аспекте кибербезопасности, тогда как информационно-политический аспект не получил серьёзного самостоятельного закрепления в качестве основания для введения санкций, хотя и косвенно подпадает под прописанные критерии.

Кроме того, в санкционном законе воспроизводились базовые положения законопроекта «О противодействии влиянию Российской Федерации в Европе и Евразии», фиксируя в качестве доказанных фактов стандартные обвинения в подрыве российским Правительством западных демократических институтов, в насаждении вражды и ксенофобии на Западе, в попытках расширения своего влияния на всю Евразию, в использовании коррупционных методов, в широком распространении дезинформации с помощью контролируемых российским Правительством медиасредств внутри и за пределами РФ на фоне подавления независимых *«основанных на фактах»* источников, в дестабилизирующей деятельности за границей в виде присоединения Крыма, активности на Донбассе, оккупации Южной Осетии и Абхазии, в нарушении Будапештского меморандума, Хельсинских соглашений и договоров по ограничению и контролю над вооружениями (раздел 252). Утверждалось выделение 250 млн. долларов в специальный Фонд противодействия российскому влиянию на следующие цели:

- защита критически важной инфраструктуры от кибератак;

- помощь странам НАТО, ЕС и партнёрским с ними Восточноевропейским странам, уязвимым для российского влияния;
- борьба с (поощряемой Россией) коррупцией;
- реагирование на возникающие из-за действий России кризисы;
- стимулирование совместной законодательной деятельности различных стран, направленных на противодействие России;
- финансирование «институтов гражданского общества», неправительственных организаций, «юридического образования»;
- оказание помощи Госсекретарю в задачах распознавания, понимания, раскрытия и противодействия пропаганде и дезинформации зарубежных правительств (раздел 254).

Указанных целей предполагалось достигать посредством инициатив Правительства США, федеральных грантовых программ или работы через неправительственные либо международные организации.

Отдельно прописывалось поручение Президенту США в 90-дневный срок подать в соответствующие комитеты Конгресса отчёт о выполнении положений санкционного закона, а также ежегодно – доклады о контролируемых российским Правительством либо аффилируемыми с ним лицами СМИ (раздел 255) и о фондах, используемых Правительством РФ или любыми гражданами РФ с намерением повлиять на результаты любой избирательной кампании в любой стране Европы или Евразии за предшествующий год, включая прямую поддержку любой политической партии, кандидата, лоббистской кампании, неправительственной или гражданской организации (раздел 256).

Санкционный закон создал рамки для координации с американскими сателлитами совместного давления на Россию с особым акцентом на информационное давление, включая возможность новых санкций против РФ, предусматривающие, среди прочего, наказание за «кибервмешательство» и

адресные санкции против тех, кто помогает России «подорвать кибербезопасность любого демократического института»³³⁸.

После принятия санкционного закона американские органы власти получили возможность осуществлять конкретные ограничительные меры в рамках борьбы с российским информационным влиянием, причём администрация Д. Трампа, как правило, этим мерам не препятствовала, а иногда и открыто поддерживала. Подобные меры включали создание барьеров для вещания отдельным российским СМИ в американском информационном пространстве, давление на администрации социальных сетей с целью добиться блокировки и удаления нежелательных аккаунтов и контента, а также введение санкций против российских граждан и компаний, якобы причастных к вмешательству в выборы.

Первыми под удар ожидаемо попали крупные российские СМИ с иностранным вещанием – канал *Russia Today* и агентство «Спутник». 13 ноября 2017 г., подчиняясь требованию Минюста США, руководство телеканала *RT America* было вынуждено зарегистрировать его в качестве иностранного агента (в соответствии с законом FARA), что повлекло необходимость раскрывать все источники финансирования и выходить в эфир с пометкой «иноагент»³³⁹. 15 ноября 2017 г. в качестве иноагента был также зарегистрирован транслятор «Радио Спутник»³⁴⁰. В начале января 2018 г. требование о регистрации в

³³⁸ Blackwill R. Containing Russia, Again. An Adversary Attacked the United States—It's Time to Respond / R. D. Blackwill, Ph. H. Gordon // Foreign Affairs. January 18, 2018. URL: <https://www.foreignaffairs.com/articles/russian-federation/2018-01-18/containing-russia-again> (дата обращения: 11.11.2020)

³³⁹ Stubbs J. Russia's RT America registers as 'foreign agent' in U.S. / J. Stubbs, G. Gibson // Reuters. November 13, 2017. URL: <https://www.reuters.com/article/us-russia-usa-media-restrictions-rt/russias-rt-america-registers-as-foreign-agent-in-u-s-idUSKBN1DD25B> (дата обращения: 11.11.2020); Симоньян сообщила о регистрации RT в качестве иностранного агента в США // Новая газета. 13 ноября 2017. URL: <https://www.novayagazeta.ru/news/2017/11/13/136972-simonyan-soobschila-o-registratsii-rt-v-kachestve-inostrannogo-agenta-v-ssha> (дата обращения: 11.11.2020)

³⁴⁰ Транслятор «Радио Спутник» зарегистрировался в качестве иноагента в США // Новая газета. 17 ноября 2017. URL: <https://novayagazeta.ru/news/2017/11/17/137122-translyator-radio-sputnik-zaregistrovalsya-v-kachestve-inoagenta-v-ssha> (дата обращения: 11.11.2020)

соответствии с законом FARA получило агентство *RIA Global*, поставляющее контент для новостного агентства *Sputnik*³⁴¹.

На следующем этапе были выдвинуты адресные обвинения против отдельных российских частных организаций и граждан. Так, 16 февраля 2018 г. спецпрокурор США Роберт Мюллер в рамках расследования «вмешательства России в американские выборы» выдвинул обвинения тринадцати гражданам России и трём юридическим лицам, включая «Агентство Интернет-исследований» из Санкт-Петербурга и его сотрудников.

Вскоре после этого представители администрации Трампа подняли вопрос о необходимости наказания России как государства. Уже 27 февраля 2018 г. Министр финансов США Стивен Мнучин сообщил о намерении Вашингтона ввести против РФ новые санкции в наказание за «вмешательство»³⁴². Однако реализация этого намерения происходила не сразу, а поэтапно. 13 июля 2018 г. Минюст США опубликовал официальное обвинение в причастности к взлому серверов Демократической партии во время предвыборной кампании 2016 г. в адрес двенадцати граждан РФ, будто бы являющихся сотрудниками ГРУ, приписанными к войсковой части, которая ранее фигурировала в расследовании издания *The Insider* касательно взлома электронной почты Президента Франции Э. Макрона³⁴³.

Тем не менее, точечные шаги отдельных американских органов власти не придавали антироссийской кампании должный размах до тех пор, пока к ней не был подключён лично Президент США, и пока он не утвердил правовые рамки для подобных шагов. Только 13 сентября 2018 г., на фоне медийной истерии по поводу предполагаемого отравления Скрипалей и других якобы враждебных действий Москвы, Дональд Трамп подписал указ, которым санкционировалось

³⁴¹ Российское посольство в США возмутилось давлением на партнера Sputnik // Новая газета. 11 января 2018. URL: <https://www.novayagazeta.ru/news/2018/01/11/138531-rossiyskoe-posolstvo-v-ssha-vozmutilos-davleniem-na-partnera-sputnik> (дата обращения: 11.11.2020)

³⁴² США выделяют 40 млн. долларов на борьбу с дезинформацией // DW. 27.02.2018. URL: <https://www.dw.com/ru/сша-выделят-40-млн-долларов-на-борьбу-с-дезинформацией/a-42752523-0> (дата обращения: 11.11.2020)

³⁴³ США выдвинули обвинения в адрес хакеров из войсковой части ГРУ, ранее засвеченной в расследовании The Insider // The Insider. 13 июля 2018. URL: <https://theins.ru/news/109925> (дата обращения: 11.11.2020)

отслеживание сразу несколькими американскими спецслужбами вмешательства в американские выборы через кибератаки на «избирательную инфраструктуру», принятие ответных действий в случае подтверждения факта вмешательства, в том числе, введение ограничений на возможность брать кредиты в американских банках, замораживание активов физических и юридических лиц и другие санкции³⁴⁴. Тем самым американский Президент автоматически одобрял все действия на данном направлении, которые были или могли быть предприняты другими органами власти.

После принятия данного указа деятельность Министерства юстиции и Министерства финансов США на данном направлении приняла регулярный характер. 4 октября 2018 г. Министерство юстиции США предъявило обвинения ещё семи россиянам, предположительно являвшимся сотрудниками ГУ Генштаба ВС РФ (ранее ГРУ), якобы причастными к попыткам взлома сети Организации по запрету химического оружия и серверов Демпартии США³⁴⁵. 19 октября американский Минюст обвинил гражданку России Елену Хусьянову, работавшую бухгалтером проекта «Лахта», в попытке повлиять на выборы в Конгресс, которые должны были пройти в ноябре 2018 г.: якобы Хусьянова выдавала себя за американскую политическую активистку в американских соцсетях и активно участвовала в дискуссиях³⁴⁶.

³⁴⁴ Рубченко М. Трамп обхитрил сенаторов. Что это значит для России / М. Рубченко // РИА. 13.09.2018. URL: https://ria.ru/economy/20180913/1528464933.html?utm_source=smi2obmen&utm_medium=banner&utm_campaign=ri_an_partners (дата обращения: 11.11.2020)

³⁴⁵ Минюст США предъявил обвинения семерым россиянам // РБК. 4 октября 2018. URL: <https://www.rbc.ru/politics/04/10/2018/5bb615fd9a7947871ec01702> (дата обращения: 11.11.2020), U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations // Department of Justice. October 4, 2018. URL: <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and> (дата обращения: 11.11.2020); Russian Hackers Indicted. GRU Military Intelligence Officers Targeted Anti-Doping Organizations, Other International Agencies // FBI. October 4, 2018. URL: <https://www.fbi.gov/news/stories/russian-gru-officers-charged-with-hacking-100418> (дата обращения: 11.11.2020); Они все взломали. США и Нидерланды представили отчеты о причастности офицеров военной разведки России к хакерским атакам // Фонтанка.ру. 04.10.2018. URL: <https://www.fontanka.ru/2018/10/04/101/?ref=t> (дата обращения: 11.11.2020)

³⁴⁶ Россиянку обвинили во вмешательстве в выборы США 2018 года // Lenta.ru. 19 октября 2018. URL: <https://lenta.ru/news/2018/10/19/onemore/> (дата обращения: 11.11.2020); Justice Dept. charges Russian woman with interference in midterm elections / M.Zapotosky et al. // The Washington Post. Oct. 19, 2018. URL: https://www.washingtonpost.com/world/national-security/director-of-national-intelligence-warns-of-ongoing-campaigns-to-interfere-with-elections/2018/10/19/64973a7a-d3b4-11e8-b2d2-f397227b43f0_story.html?utm_term=.413f385d43b5&noredirect=on (дата обращения: 11.11.2020)

19 декабря 2018 г. Минфин США расширил санкционные списки, введённые на основании конфликта на Украине, и внёс туда, наряду с подозреваемыми в отравлении Сергея Скрипаля Анатолием Чепигой и Александром Мишкиным, медиакомпания «Экономика сегодня», «Федеральное агентство новостей», «Невские новости», а также петербургскую компанию *USA Really*, связанную с «Конкорд менеджмент и консалтинг»³⁴⁷ (месяцем ранее в США был задержан по вопросу российского вмешательства главный редактор издания *USA Really*, первый зампредседателя комиссии Общественной палаты по развитию информационного сообщества Александр Малькевич³⁴⁸). Также 20 ноября 2018 г., Федеральный суд округа Колумбия отклонил ходатайство компании «Конкорд менеджмент энд консалтинг» о закрытии дела по обвинению во вмешательстве в президентские выборы 2016 г.³⁴⁹.

18 апреля 2019 г. генеральный прокурор США У. Барр опубликовал незначительно отцензурированную версию итогового доклада специального прокурора Роберта Мюллера, посвящённого якобы имевшему место «российскому вмешательству» в американские выборы 2016 г.³⁵⁰ Доклад не ставил под сомнение наличие вмешательства, якобы осуществлённого через сетевую активность Агентства Интернет-исследований и хакерские атаки из «связанных с ГРУ» источников и содействовавшего победе Д. Трампа на президентских выборах. Фокус расследования был перемещён на установление фактов сговора или сотрудничества окружения Д. Трампа с российскими представителями, якобы участвовавшими во «вмешательстве», а также на попытки Д. Трампа и его администрации воспрепятствовать расследованию указанных действий. По заключению Р. Мюллера, многочисленные контакты

³⁴⁷ И Петров, и Боширов. Под новые санкции США попали 18 российских хакеров и разведчиков. Полный список / Strana.ua. 19 декабря 2018. URL: <https://strana.ua/news/177445-i-petrov-i-boshirov-pod-novye-sanktsii-ssha-popali-18-rossijskikh-khakerov-i-razvedchikov-polnyj-spisok.html> (дата обращения: 11.11.2020)

³⁴⁸ МИД увидел подтекст в задержании российского журналиста в США / Lenta.ru. 11 ноября 2018. URL: <https://lenta.ru/news/2018/11/11/predlog/> (дата обращения: 11.11.2020)

³⁴⁹ Козловский В. Если не мы — то кто? Американский суд не внял доводам компании Евгения Пригожина / В. Козловский // Новая газета. 18 ноября 2018. URL: <https://www.novayagazeta.ru/articles/2018/11/18/78631-esli-ne-my-to-kto> (дата обращения: 11.11.2020)

³⁵⁰ Mueller R. S. Report On The Investigation Into Russian Interference In The 2016 Presidential Election / R. S. Mueller // Washington, D.C. March 2019. URL: <https://www.justice.gov/storage/report.pdf> (дата обращения: 11.11.2020)

окружения Д. Трампа с российскими представителями действительно имели место, имели место передача компромата на Х. Клинтон и обсуждение будущей нормализации отношений между США и РФ, однако координации действий между представителями РФ и Д. Трампом по осуществлению предвыборной кампании установить не удалось. Последующее обсуждение доклада свелось к определению степени личной вины Д. Трампа и его окружения, в ходе которого версия о «российском вмешательстве» окончательно приобрела статус самоочевидной, не нуждающейся в обосновании и поисках некриминализирующей трактовки³⁵¹.

Таким образом, реальные правовые ограничения и санкции по вопросу о вмешательстве в президентские выборы 2016 г. сводились к давлению на ряд российских СМИ и компаний, ассоциируемых в западной прессе с Евгением Пригожиным, обвинению нескольких десятков частных лиц и, предположительно, сотрудников российских спецслужб. Обвинения против конкретных российских органов власти или силовых структур в целом на данном этапе официально предъявлены не были.

Одновременно с этим продолжалась работа по созданию новой и наполнению содержанием уже созданной институциональной инфраструктуры по противодействию «российской информационной угрозе» на национальном уровне и на уровне двустороннего сотрудничества с некоторыми европейскими государствами. В первую очередь, это касалось усиления и наполнения содержанием созданного в 2016 г. Центра глобального взаимодействия, призванного стать основным органом по противодействию «российской информационной угрозе». Несмотря на значительный резонанс от факта его создания, Центр долгое время оставался в полуподвешенном состоянии, без определённых текущих задач, не располагая достаточными средствами и ресурсами для выполнения своих функций. Администрация Д. Трампа на первых

³⁵¹ Смирнов В. «Игра окончена»: опубликован доклад Мюллера о «российском вмешательстве» / В. Смирнов, А. Лушникова // RT, 18 апреля 2019 г. URL: <https://russian.rt.com/world/article/622799-rossiiskoe-vmeshatelstvo-vybory-prezident-ssha> (дата обращения: 11.11.2020), В США опубликовали доклад Мюллера // ТАСС. 18/19 апреля 2019 г. URL: <https://tass.ru/mezhdunarodnaya-panorama/6350715> (дата обращения: 11.11.2020)

порах не спешила использовать данную структуру в полном объёме, но с течением времени другие органы исполнительной и законодательной власти США предприняли ряд шагов по её активизации и ресурсному насыщению.

Так, 27 февраля 2018 г. было подписано партнёрское соглашение о выделении Пентагоном 40 млн. долл. Центру для дальнейшего распределения среди негосударственных организаций (медиакомпаний, НГО, исследовательских институтов и т.п.) в виде грантов на борьбу с зарубежной пропагандой и дезинформацией³⁵². А в начале марта 2018 г. конгрессмены-демократы Тед Льё и Хоакин Кастро направили запрос госсекретарю Рексу Тиллерсону о причинах недостаточно эффективного, по их мнению, расходования государственных ресурсов на борьбу с иностранной пропагандой в рамках Центра глобального взаимодействия. Ни один из 23 его аналитиков не говорил по-русски, хотя *«это язык одного из главных спонсоров дезинформационных кампаний в мире»*, на противодействие собственно российскому вмешательству не были потрачены 120 млн. долларов, выделенные Конгрессом, и т. д.³⁵³ 16 марта 2018 г. шесть членов Комитета по международным отношениям Сената США, представляющие обе партии, запросили график расходов выделенных Конгрессом на нужды Центра средств, отметив, что *«деятельность [России] является частью продолжающихся долгосрочных усилий по подрыву американских институтов, ослаблению наших альянсов и манипулированию общественным восприятием»*³⁵⁴.

³⁵² США выделяют \$40 млн на борьбу с дезинформацией // Ліга.Новости. 27.02.2018. URL: https://news.liga.net/world/news/ssha_vydelyat_40 mln_na_borbu_s_dezinformatsiey (дата обращения: 11.11.2020); Пудовкин Е. Миллионы на борьбу с российской пропагандой. Госдеп и Пентагон придумали, как противостоять иностранной дезинформации / Е. Пудовкин // Независимая газета. 27.02.2018. URL: http://www.ng.ru/world/2018-02-27/1_7181_propaganda.html (дата обращения: 11.11.2020); State-Defense Cooperation on Global Engagement Center Programs and Creation of the Information Access Fund to Counter State-Sponsored Disinformation // Department of State. February 26, 2018. URL: <https://www.state.gov/state-defense-cooperation-on-global-engagement-center-programs-and-creation-of-the-information-access-fund-to-counter-state-sponsored-disinformation/> (дата обращения: 11.11.2020)

³⁵³ Reps Lieu and Castro question why state department funds for countering election meddling are unspent // Ted Leu. March 6, 2018. URL: <https://lieu.house.gov/media-center/press-releases/rep-lieu-and-castro-question-why-state-department-funds-countering> (дата обращения: 11.11.2020)

³⁵⁴ Bipartisan Senators question State and Defense Departments on funding delays, inadequate staffing for efforts to counter Russian propaganda and disinformation // Todd Young. March 16, 2018. URL: <https://www.young.senate.gov/newsroom/press-releases/bipartisan-senators-question-state-and-defense-departments-on-funding-delays-inadequate-staffing-for-efforts-to-counter-russian-propaganda-and-disinformation-> (дата обращения: 11.11.2020)

Это разбирательство, впрочем, не слишком ускорило запуск реальной работы Центра, тем более что выделенные Пентагоном средства поступили к нему только осенью 2018 г. В мае 2018 г. было объявлено о запуске Технологического курса Центра, в рамках которого ведущие специалисты в этой сфере должны были в течение полугода собираться и проводить демонстрационные мероприятия, разъясняя приёмы и методы противодействия враждебной пропаганде и дезинформации. Тем не менее, даже на этапе конца октября 2018 г. Госдепартамент только формировал перспективные направления работы Центра, утверждая, что выделенное ему финансирование пойдет, в том числе, на *«разработку технологий, которая позволит предупреждать о появлении пропаганды на ранних этапах»*, будут налажены контакты с местными блогерами и лидерами общественного мнения для ретрансляции американской позиции на целевые аудитории, обучение представителей местных НГО и журналистов³⁵⁵. Фактически, только с назначением специального посланника Ли Габриэль на должность координатора Центра в феврале 2019 г. его деятельность приобрела регулярный характер, а ещё год спустя Центром был создан специальный ресурс *Disinfo Cloud*³⁵⁶, работающий во многом по лекалам портала *EUvsDisinfo*.

Помимо активизации Центра глобального взаимодействия, немалые ресурсы продолжали направляться на усиление присутствия американских СМИ в русскоязычном информационном пространстве. Так, 13 марта 2019 г. стало известно, что Госдепартамент запросил на 2020 финансовый год выделение 500 млн. долл. на *«противостояние российскому злонамеренному влиянию»* в странах Европы, Евразии и Центральной Азии; в рамках этой программы такие американские проекты, как «Голос Америки» и «Радио Свобода», должны были

³⁵⁵ В Госдепартаменте заявили, что США выделили \$40 млн на борьбу с иностранной пропагандой // ТАСС. 30 окт 2018. URL: <https://tass.ru/mezhdunarodnaya-panorama/5739346> (дата обращения: 11.11.2020)

³⁵⁶ <https://disinfocloud.com/>

«удвоить еженедельную аудиторию, потребляющую контент на русском языке»³⁵⁷.

Более серьёзные подвижки в развитии правовых рамок и практической инфраструктуры для информационного противодействия России происходили на военно-стратегическом направлении. Здесь ведущую инициативную роль взял на себя Конгресс, представители которого по уже отработанной в конце 2016 г. схеме регулярно вносили предложения по предоставлению дополнительных полномочий силовым структурам в данной сфере в ходе подготовки и обсуждения закона об ассигнованиях на национальную оборону на следующий год (по сути, военных бюджетов). Многие из этих предложений поддерживались Пентагоном и утверждались в его позиционных документах в качестве доктринальных элементов.

Так, в утверждённом в декабре 2017 г. Законе об ассигнованиях на национальную оборону на 2018 г.³⁵⁸ предписывалось объединить в едином подразделении управление стратегическими информационными операциями и информационными операциями в киберпространстве под руководством чиновника на уровне заместителя Министра обороны (раздел 1637). Также Министру обороны предписывалось дать поручение командующим оперативными частями подготовить в координации с Госдепартаментом и его Центром глобального взаимодействия региональные информационные стратегии и план межведомственного сотрудничества в сфере проведения информационных операций вовне и сдерживания враждебных информационных атак на США (раздел 1637). Кроме того, в законе содержался прямой запрет на использование государственными органами США продуктов Лаборатории Касперского (раздел 1634). Это означало, что информационные операции

³⁵⁷ Госдеп: борьба с "деятельностью РФ в Европе" является приоритетом бюджета на 2020 год. Ведомство рассчитывает получить на эти цели \$661 млн. // ТАСС. 11 мар 2019. URL: <https://tass.ru/mezhdunarodnaya-panorama/6207314> (дата обращения: 11.11.2020)

³⁵⁸ Public Law 115–91—DEC. 12, 2017. URL: <https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf> (дата обращения: 11.11.2020)

интегрировались в единую сферу стратегической деятельности с кибероперациями и передавались в непосредственное ведение Пентагона.

Более далекоидущие положения относительно полномочий военного ведомства в информационной среде содержались в Законе об ассигнованиях на национальную оборону на 2019 г., проект которого был подан 24 июля 2018 г., а был подписан Президентом и вступил в силу уже 13 августа 2018 г.³⁵⁹ Он предоставлял главе Пентагона полномочия вести военные кибермеры или операции в киберпространстве, в том числе скрытые и ответные, для защиты Соединённых Штатов и их союзников (раздел 1631). Такие меры предусматривали среди прочего операции в киберпространстве, не достигающие порога боевых действий или ведущиеся в их отсутствие, с целью подготовки контекста, проведения информационных операций, защиты военных контингентов, сдерживания враждебных действий или проведения контртеррористических операций с задействованием вооружённых сил США. Причём подобные меры юридически приравнивались к традиционной военной деятельности и не требовали более согласования со стороны иных государственных органов.

Закон определял политику США в области кибербезопасности, позволяя Вашингтону использовать все имеющиеся силовые инструменты, включая наступательный киберпотенциал, для сдерживания и реагирования на все типы кибератак и враждебных действий внешних сил, нарушающие интересы США с целью нанесения ущерба гражданам США и их союзников, значительно подрывающие нормальное функционирование демократического общества или Правительства США, включая атаки на критическую административную инфраструктуру, несущие угрозу командованию и контролю вооружёнными силами и военно-промышленному потенциалу США или преследующие цель добиться на разовой или систематической основе эффекта, сопоставимого с вооружённой атакой на жизненно важные интересы США (раздел 1636).

³⁵⁹ John S. McCain National Defense Authorization Act for Fiscal Year 2019. Public Law 115–232—AUG. 13, 2018. URL: <https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf> (дата обращения: 11.11.2020)

Ещё более однозначно прописано положение о том, что в случае, если командование национальными силами установит, что Российская Федерация, Китайская Народная Республика, КНДР или Исламская Республика Иран ведут активную, систематическую и длительную кампанию атак против Правительства или народа Соединённых Штатов в киберпространстве, включая попытки повлиять на американские выборы и демократические политические процессы, командование может уполномочить Министра обороны и командующего национальными кибервойсками предпринять надлежащие пропорциональные действия в киберпространстве для разрушения, отражения и сдерживания таких атак (раздел 1642).

Тем самым закон не только санкционировал значительное расширение диапазона угроз, способных повлечь задействование военного потенциала США в киберпространстве, и расширение полномочий оборонного ведомства, но и предписывал принять непосредственные меры в случае деструктивных действий со стороны ряда стран, включая Россию³⁶⁰.

25 июля 2018 г. Объединённый комитет начальников штабов (американский аналог Генштаба) опубликовал финальную редакцию Общей концепции оперирования в информационной среде³⁶¹, в которой развивались и совершенствовались заложенные Пентагоновской концепцией 2016 г. идеи о необходимости интеграции физической и информационной мощи. На этот раз в тексте концепции содержались прямые обвинения России, представленные в качестве самоочевидного факта. В частности, констатировалось, что российские операции на Украине демонстрировали приверженность способу ведения конфликта, который включает в себя операции по оказанию воздействия на эмоции для управления поведением [целевой аудитории] в желаемую сторону, а также для разрушения и подрыва выбранных целей³⁶². Для обеспечения

³⁶⁰ Chesney R. The Law of Military Cyber Operations and the New NDAA / R. Chesney // Lawfare. July 26, 2018. URL: <https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa> (дата обращения: 11.11.2020)

³⁶¹ Joint Concept for Operating in the Information Environment (JCOIE). 25 July 2018. 62 p. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.pdf (дата обращения: 11.11.2020)

³⁶² Там же., Р. 7

конкурентоспособности в информационной среде армия США, подчёркивалось в концепции, должна встроить информационный компонент в планирование своих операций таким образом, чтобы информационные аспекты военной деятельности были непосредственно увязаны с физическими. Вместо того, чтобы полагаться на физическую мощь как форму деструктивной или подрывной силы, США должны получать преимущество от конструктивных и информационных аспектов военного могущества.

Помимо закона и концепции, осенью 2018 г. были приняты два доктринальных документа, непосредственно касающихся информационной сферы: утверждённая Президентом Национальная киберстратегия США³⁶³ и киберстратегия Министерства обороны.

Во введении Национальной киберстратегии говорилось, что Россия, Иран и Северная Корея предприняли безответственные кибератаки, которые нанесли ущерб американскому и международному бизнесу, а также американским союзникам и партнёрам и не заплатили за это цену, способную удержать их от вероятной киберагрессии в будущем³⁶⁴. Кроме того, утверждалось, что Россия, Китай, Иран и Северная Корея используют киберпространство как средство для того, чтобы бросить вызов США, их союзникам и партнёрам, *«с решительностью, которую они бы никогда бы не рассматривали применительно к иным сферам»*.

Далее стратегия намечала базовые приоритеты в защите американской политической системы и экономической инфраструктуры от существующих и потенциальных киберугроз и определяла магистральные принципы работы государственного аппарата на данном направлении. И хотя основной упор в стратегии сделан на обеспечении экономического благополучия страны и её граждан, в ней, вместе с тем, прописан ряд положений относительно международно-политических аспектов реализации поставленных задач. Так, в

³⁶³ National Cyber Strategy of the United States of America // The White House. September 2018. 29 p. URL: https://digital.library.unt.edu/ark:/67531/metadc1259394/m2/1/high_res_d/National-Cyber-Strategy.pdf (дата обращения: 11.11.2020)

³⁶⁴ Ibid., P. 1-2.

третьем разделе данного документа «Поддержание мира благодаря использованию силы» сказано, что постоянное вовлечение государств в киберпространство уже влияет на стратегический баланс сил в мире, поэтому киберпространство больше не будет рассматриваться как отдельная, не связанная с другими составляющими национальной мощи, среда. Для нейтрализации вызовов американскому лидерству в этой среде и укрепления глобальной киберстабильности администрация намерена, с одной стороны, способствовать выработке и поддержанию норм ответственного поведения государств в киберпространстве, а, с другой, своевременно выявлять и сдерживать проявления недопустимого поведения. Это предусматривает гарантированное наступление последствий для безответственного поведения, наносящего ущерб США и их партнёрам. Все инструменты национальной мощи, включая дипломатические, информационные, военные, финансовые, разведывательные и правовые, могут быть задействованы для предотвращения, отражения и сдерживания зловредной киберактивности. США намерены формализовать и рутинизировать совместно со своими партнёрами интегрированные стратегии, налагающие быстрые, обременительные и прозрачные последствия для враждебно настроенных акторов. При этом противодействие будет оказываться не только «вредоносному влиянию» в сетях, но и информационным кампаниям, негосударственной пропаганде и дезинформации. Реализация этой задачи потребует, в том числе, организации сотрудничества с государствами-партнёрами, частными компаниями, научными, образовательными учреждениями и гражданским обществом в целях выявления, противодействия и предотвращения попыток использования цифровых платформ для оказания вредоносного воздействия из-за рубежа при должном уважении гражданских прав и свобод³⁶⁵.

Как следует из этих положений Национальной киберстратегии, Белый дом декларировал политическую готовность расценивать угрозы в

³⁶⁵ Там же. Р. 20-21. См. также Баталов А. Национальная киберстратегия США / А. Баталов // Зарубежное военное обозрение. 2019. № 2 (863). С.8-10.

киберпространстве в качестве первоочередных вызовов американскому могуществу, рассматривать дезинформацию и пропаганду как элемент диапазона угроз в киберпространстве и отражать их с использованием всего спектра силовых инструментов, включая военные. Однако в содержательной части документа не описывались конкретные меры, которые будут предприняты в ответ на зловредную деятельность данных государств.

В более чётких категориях этот вопрос был освещён в киберстратегии Пентагона, краткое изложение которой было опубликовано вскоре после обнародования Национальной киберстратегии осенью 2018 г.³⁶⁶ В нём, в частности, утверждалось, что Соединённые Штаты пребывают в состоянии долгосрочного стратегического противостояния с Китаем и Россией, которые распространили данное противостояние на киберпространство, проводя систематические кампании, представляющие долговременный стратегический риск для США, их союзников и партнёров. Россия уличалась в использовании киберориентированных информационных операций для оказания влияния на американское население и подрыва демократических процессов³⁶⁷. Среди практических мер в ответ на данные действия в документе указывались проведение киберопераций, сбор разведданных и подготовка потенциала для «передовой обороны» с целью срыва или остановки зловредной киберактивности на раннем этапе, в том числе деятельности, не достигающей уровня вооружённого конфликта.

Продолжая и развивая положения Национальной киберстратегии, стратегия военного ведомства недвусмысленно постулировала возможность применения всего спектра вооружений в ответ на совершённые или возможные атаки в киберпространстве. В отличие от аналогичной стратегии 2015 г., в действующей стратегии делался эксплицитный акцент на принципах наступательности, превентивности, тотальности и независимости от формальной стадии конфликта.

³⁶⁶ Summary. Department of defense cyber strategy. 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (дата обращения: 11.11.2020)

³⁶⁷ Там же. Р. 1.

Бросается в глаза более расширительная трактовка объекта вероятных киберугроз и круга инструментов, которые могут быть применены для их нейтрализации, а также проактивная, если не сказать агрессивная, риторика в отношении возможности их применения вне географических границ США и их союзников и вне зависимости от формального состояния конфликта³⁶⁸.

Принятый в декабре 2019 г. Закон об ассигнованиях на национальную оборону на 2020 г.³⁶⁹ дополнял уже сформированную доктринальную инфраструктуру информационного противостояния некоторыми институциональными новациями. Так, в нём вводилась должность Главного советника по информационным операциям при Министре обороны США, ответственного за планирование, обеспечение и проведение информационных операций военного ведомства, координацию с Государственным департаментом и его Центром глобального взаимодействия, принятие решений относительно публичного признания фактов проведения информационных операций, организацию сотрудничества с частным сектором и академической наукой (раздел 1631). В нём ещё раз уточнялись формальные полномочия главы оборонного ведомства в сфере ведения информационных операций, в том числе скрытых, а также вменялись обязанности в течение 270 дней со дня принятия закона подготовить стратегию ведения информационных операций, составить отчёт об имеющихся недостатках и пробелах в имеющихся в распоряжении США силах ведения информационных операций, разработать перечень необходимых силовых инструментов и способов их подготовки и в течение 90 дней подготовить план организации работы Пентагона и его соответствующих подразделений в ходе реализации задач, связанных с проведением информационных операций.

³⁶⁸ Kollars N. Defending Forward: The 2018 Cyber Strategy Is Here / N. Kollars, J. Schneider // War on the rocks. September 20, 2018. URL: <https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/> (дата обращения: 11.11.2020)

³⁶⁹ National Defense Authorization Act for Fiscal Year 2020. S. 1719. // 116th Congress. URL: <https://www.govinfo.gov/content/pkg/BILLS-116s1790enr/pdf/BILLS-116s1790enr.pdf> (дата обращения: 11.11.2020)

Подводя итог проведённому анализу, можно констатировать, что за три года после избрания Д. Трампа информационная сфера подверглась полной милитаризации на доктринальном и институциональном уровнях, будучи интегрирована в компетенцию военного ведомства в рамках его полномочий в области кибербезопасности и отражения киберугроз. На законодательном уровне были прописаны широкие полномочия и обязанности Пентагона в отношении проведения военных информационных операций, в том числе превентивных, скрытых и не достигающих порога прямых боевых действий. Причём были сняты действовавшие ранее ограничения, связанные с необходимостью межведомственной координации таких операций, а сами они были юридически приравнены к традиционным военным действиям, не требующим особых процедур согласования на уровне политического руководства страны. При этом в утверждённых в 2018 г. киберстратегиях были сформулированы расширительные трактовки объекта вероятных киберугроз и круга инструментов, которые могут быть применены для их нейтрализации.

На уровне двустороннего сотрудничества США в данный период развивали соответствующие программы помощи странам Балтии, Украине, Грузии, Молдове, а также балканским государствам, находящимся в процессе вступления в НАТО. 4 декабря 2017 г. Министр обороны Литвы сообщил о намерении США выделить дополнительные 100 млн. долл. республикам Балтии на защиту от угроз со стороны России с опорой на противодействие кремлёвской пропаганде³⁷⁰. 8 августа 2018 г. Агентство по международному развитию (USAID) заявило о выделении Македонии гранта в 5 млн. долл. *«на внедрение этических стандартов в редакционную политику СМИ Македонии, а также на работу с независимыми журналистами»* в целях борьбы с *«распространением дезинформации»*³⁷¹. А 5 июля 2019 г. было объявлено о запуске агентством

³⁷⁰ США подкинут странам Балтии \$100 миллионов на борьбу с российской пропагандой. // Наш город – новости Даугавпилса. 21 марта 2020 г. URL: <http://www.gorod.lv/novosti/288554-ministr-oborony-litvy-poradovol-ssha-podkinut-stranam-baltii-100-millionov-na-borbu-s-rossiiskoi-propagandai> (дата обращения: 11.11.2020)

³⁷¹ В США намерены принять меры против «российской дезинформации» в Македонии // Газета.ру. 08.08.2018. URL: https://www.gazeta.ru/politics/news/2018/08/08/n_11884033.shtml?updated (11.11.2020)

USAID очередной программы противодействия злонамеренному влиянию Кремля в отношении партнёров США в Европе и Евразии³⁷², включающей помощь в защите демократических институтов, свободы СМИ, энергетической и экономической независимости. Основными получателями помощи по этой программе на начальном этапе выступали Украина, Молдова и Грузия.

При этом важность поддержки европейских партнёров и союзников в борьбе против «российской угрозы» регулярно подчёркивалась на уровне Конгресса. К примеру, 9 января 2018 г. сенатскому Комитету по внешним сношениям был представлен доклад членов Конгресса «Путинская асимметричная атака на демократию в России и Европе: выводы для национальной безопасности США»³⁷³.

Кроме того, на фоне резонанса от дела о попытке отравления Сергея Скрипаля значительно интенсифицировалось сотрудничество спецслужб США и Великобритании в сфере обеспечения кибер- и информационной безопасности. 17 апреля 2018 г. ФБР, Министерство внутренней безопасности (МВБ) США и Национальный центр кибербезопасности Великобритании выпустили совместное заявление о *«злонамеренной киберактивности российского Правительства»*, в котором сообщалось об угрозах для организаций и компаний Интернет-сектора, якобы исходящих от спонсируемых Правительством РФ хакеров. В предупреждении отмечено, что первоочередные цели киберактивности РФ – *«правительственные и частные организации, поставщики критической инфраструктуры и Интернет-провайдеры, обеспечивающие их работу»*³⁷⁴.

³⁷² Countering Malign Kremlin Influence Development Framework // USAID. June 27, 2019. URL: <https://www.usaid.gov/documents/1863/countering-malign-kremlin-influence-development-framework> (дата обращения: 11.11.2020)

³⁷³ Putin's Asymmetric Assault on Democracy in Russia and Europe: Implications for U.S. National Security. A minority staff report prepared for the use of the committee on foreign relations united states senate. January 10, 2018. URL: <https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf> (дата обращения: 11.11.2020)

³⁷⁴ Joint US - UK statement on malicious cyber activity carried out by Russian government. 15 April 2018. URL: <https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government> (дата обращения: 11.11.2020); США и Британия выпустили предупреждение о российской киберугрозе // Ліга.Новости. 17.04.2018. URL: <https://news.liga.net/world/news/ssha-i-britaniya-vypustili-preduprezhdenie-o-rossiyskoy-kiberugroze> (дата обращения: 11.11.2020)

При этом некоторые американские военные эксперты продвигали идею о необходимости максимального привлечения союзников к борьбе с «российской информационной угрозой» не только на двустороннем, но и на многостороннем уровнях. 11 октября 2018 г. появилась статья бывшего командующего силами НАТО в Европе генерала Дж. Ставридиса о необходимости глобального альянса против российской киберугрозы, в которой выдвигались следующие предложения: максимально раскрыть масштабы российской деятельности, согласованно с союзниками публично потребовать от лица различных организаций от НАТО до ООН прекратить хакерские и другие действия российских неправительственных групп, продемонстрировав в ответ свой наступательный киберпотенциал и наложив санкции, выделить больше ресурсов для организации киберзащиты. Статья заканчивается пафосным воззванием: *«США и их союзникам понадобится более жёсткий подход в борьбе с новой волной российских кибератак»*³⁷⁵.

Однако наиболее активная деятельность по разоблачению и противодействию «российской информационной угрозе» в США в поствыборный период развернулась в отношении социальных сетей, на администрации которых оказывалось политическое и юридическое давление с целью заставить их самостоятельно регулировать и ограничивать *«спонсируемую Кремлём пропаганду и дезинформацию»*.

Этот процесс имел нарастающую динамику, обусловленную постепенным смещением фокуса внимания американских СМИ с хакерских атак на попытки России подорвать веру в демократические выборы в США путем распространения новостей в социальных сетях³⁷⁶. На начальном этапе к администрациям соцсетей предъявляли требование провести расследование

³⁷⁵ Stavridis J. U.S. Needs a Global Alliance Against Russia's Cyberattacks. Washington can coordinate with Europe, the UN, Interpol and nongovernmental groups / J. Stavridis / Bloomberg. 11 октября 2018. URL: <https://www.bloomberg.com/opinion/articles/2018-10-11/u-s-needs-a-global-alliance-against-russia-s-cyberattacks> (дата обращения: 11.11.2020)

³⁷⁶ Самкова М.А. Дезинформация как средство информационно-психологической войны против России (на материале медиатекстов о хакерских атаках) / М.А. Самкова // Экология языка и коммуникативная практика. 2018. № 3. С. 96–115 / С. 100.

относительно их использования для манипулирования избирательными настроениями и общественным мнением США. Фактически, речь шла о том, чтобы соцсети сами предъявили доказательства российского вмешательства в американские выборы и признали часть своей ответственности за создание возможностей для такого вмешательства. После этого от них требовалось принять меры для ликвидации этих возможностей с регулярными публичными отчётами о масштабе и эффективности подобных мер. Материалы этих отчётов ложились в основу новых разоблачительных докладов различных официальных и неофициальных структур, которые, таким образом, не только поддерживали тематику российского вмешательства в американской политической повестке дня, но и выдвигали новые инициативы и требования по пресечению подобного вмешательства в дальнейшем, в том числе путём принятия новых законодательных ограничений. Так, накануне любых последующих выборов в органы власти США различных уровней американскими официальными лицами озвучивались опасения о возможном вмешательстве России, а после выборов – проводились расследования «фактов вмешательства». Кроме того, многие внутривнутриполитические события в США, особенно кризисного характера, сопровождались сообщениями о якобы связанной с ними активизации «российских троллей» в соцсетях. Эти сообщения документировались как факты доказанного российского вмешательства, для чего некоторые американские «мозговые центры» запустили ряд специальных проектов и структур с собственными информационными ресурсами³⁷⁷.

Администрации ведущих социальных сетей реагировали на подобное давление неоднозначно, постепенно выполняя выдвигаемые требования, когда они подкреплялись значительным политическим резонансом. Наиболее показательной стала реакция социальных сетей *Facebook*, *Twitter* и поисковой системы *Google*.

³⁷⁷ Царик В.С. Деятельность западных негосударственных организаций и аналитических институтов в сфере борьбы с «российской дезинформацией» / В.С. Царик // Вестник Международного юридического института. – 2019. – № 4 (71). – С. 152-165.

6 сентября 2017 г. начальник безопасности «Фейсбука» опубликовал обновления к апрельскому релизу об информационных операциях в «Фейсбуке». Сообщив, что компания продолжает расследования о возможном использовании Россией социальной сети в политических целях, он привёл данные о появлении на ресурсе политически ориентированной рекламы, как-либо связанной с Россией. Выяснилось, что большая часть сомнительной рекламы на общую сумму 100 000 долларов действовала с учётных записей, вероятно созданных за пределами России, и не привязывалась к конкретным кандидатам или выборам Президента США, но эта реклама и эти учётные записи *«фокусировались на усилении разногласий в социальной и политической сфере по всему идеологическому спектру – затрагивая темы от вопросов ЛГБТ до проблем борьбы с иммиграцией к права на оружие»*, и это разобщающее провоцирующее поведение соответствовало методам, раскрытом в апрельском релизе «Фейсбука». Какую-либо связь с Россией по *«широкому поиску, включая, например, рекламу, купленную со счетов с американскими IP-адресами, но с русским языком, даже если они не обязательно нарушали какие-либо правила или законы»*, удалось обнаружить в *«потенциально политически связанных рекламных расходах примерно на 2200 объявлений на сумму примерно 50 000 долларов США»*³⁷⁸.

21 ноября 2017 г. Эрик Шмидт, исполнительный директор компании *Alphabet*, являющейся материнской компанией *Google*, заявил, что компания приступает к «ранжированию» (отодвиганию на неприоритетное место в результатах поиска) сообщений российских компаний *Russia Today* и *Sputnik*³⁷⁹, а 23 ноября администрация сети *Facebook* сообщила, что до конца года создаст портал, на котором пользователи смогут проверить, связаны ли публикации или

³⁷⁸ Stamos A. An Update On Information Operations On Facebook / A. Stamos. – Facebook. September 6, 2017. URL: <https://newsroom.fb.com/news/2017/09/information-operations-update/> (дата обращения: 11.11.2020)

³⁷⁹ Демидова О. Google намерен фильтровать российскую пропаганду. Интернет-гигант Google работает над техническим решением, с помощью которого будет понижаться ранжирование сайтов RT и Sputnik / О. Демидова // DW. 21.11.2017. URL: <https://www.dw.com/ru/google-намерен-фильтровать-российскую-пропаганду/a-41461675> (дата обращения: 11.11.2020)

аккаунты, с которыми они сталкиваются, с Агентством Интернет-исследований в Санкт-Петербурге³⁸⁰.

10 мая 2018 г. член Комитета Палаты представителей по разведке Адам Шифф выступил в Конгрессе с докладом о деятельности «российских троллей». В очень эмоциональной речи он заявил, что целью «фабрики троллей» было посеять рознь внутри американской нации, используя любые возможные линии раскола, с целью *«использовать вполне реальные разочарования американцев и гнев по чувствительным политическим вопросам, чтобы влиять на американское мышление, голосование и поведение»*³⁸¹. При этом никакого конкретного результата этого «влияния» он не назвал. А 18 июня 2018 г. демократические члены Комитета по разведке Палаты представителей опубликовала около 1100 имен учетных записей в Твиттере, связанных с Агентством Интернет-исследований, затем этот список был расширен до 3800 учетных записей³⁸².

Однако конкретные шаги администраций соцсетей по ограничению доступа к выявленным вредоносным материалам последовали не ранее второй половины августа 2018 г. 21 августа Президент компании Майкрософт Брэд Смит воспроизвёл заявление об атаках русских хакеров против представителей всего политического спектра США, как до этого против всех кандидатов на президентских выборах во Франции³⁸³. 22 августа компания Фейсбук удалила в

³⁸⁰ Венкина Е. Facebook создаст сайт для отслеживания российской пропаганды / Е. Венкина // DW. 23.11.2017. URL: <https://www.dw.com/ru/facebook-создаст-сайт-для-отслеживания-российской-пропаганды/a-41493405> (дата обращения: 11.11.2020)

³⁸¹ Schiff Statement on Release of Facebook Advertisements // Permnet Select Committee of Intelligence. Washington, May 10, 2018. URL: <https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=379> (дата обращения: 11.11.2020)

³⁸² Hanlon B. Twitter Release Reveals the Kremlin's News Impersonation Game / B. Hanlon // Alliance for Securing Democracy. June 21, 2018. URL: <https://securingdemocracy.gmfus.org/twitter-release-reveals-the-kremlins-news-impersonation-game/> (дата обращения: 11.11.2020); В США обнаружили новую лазейку для российских троллей // Lenta.ru. 20 октября 2018. URL: <https://lenta.ru/news/2018/10/20/startup/> (дата обращения: 11.11.2020)

³⁸³ Microsoft: русские хакеры атакуют весь политический спектр // Газета.ru. 21.08.2018. URL: https://www.gazeta.ru/tech/news/2018/08/21/n_11933191.shtml (дата обращения: 11.11.2020); Microsoft: под прицелом русских хакеров были все кандидаты на выборах во Франции // Газета.ru. 21.08.2018. URL: https://www.gazeta.ru/tech/news/2018/08/21/n_11933131.shtml (дата обращения: 11.11.2020)

сетях *Facebook* и *Instagram* ряд страниц, групп и аккаунтов, связанных с Россией и Ираном, «за согласованные недостоверные сведения»³⁸⁴.

Тем самым, вопреки ранее обещанной, в том числе в выступлении Адама Шиффа, линии на раскрытие сведений, касающихся предполагаемой деятельности «русских троллей» в американских соцсетях с этого момента начинает преобладать вариант удаления неких данных из Интернета без предоставления третьей стороне возможности проверить, действительно ли там содержалась дезинформация, о которой было заявлено американскими властями и компаниями.

К концу 2018 г. к раскрутке тематики «русской информационной угрозы» в соцсетях, помимо экспертных и аналитических структур, начинают подключать компании IT-сектора, специализирующиеся на пакетном анализе больших массивов информации. Так, 7 декабря 2018 г. IT-компания *New Knowledge* (позднее *Yonder*) подготовила на основе «данных, предоставленных Комитету по разведке Сената США» собственный «независимый отчёт» о действиях и тактике Агентства Интернет-исследований, на деле представлявший собой упаковку заданных сообщений с диаграммами и другими доходчивыми иллюстрациями³⁸⁵. В отчёте говорилось об особой нацеленности «русских троллей» на афроамериканскую аудиторию и её вербовку, использовании таких тактик подавления воли избирателей-демократов, как дезинформация о правилах голосования и агитация за неучастие в голосовании под предлогом невозможности повлиять на результат, переключение избирателей Хиллари Клинтон на других кандидатов, поддержку Трампа, поощрение сепаратистских настроений в США. Руководители Фейсбука критиковались за недостаточное освещение активности Агентства Интернет-исследований в *Instagram*.

А уже 17 декабря был опубликован и сам доклад сенатского Комитета по разведке, опиравшийся на выводы *New Knowledge* в качестве «независимого

³⁸⁴ Facebook удалил связанные с Россией и Ираном страницы // Газета.ru/ 22.08.2018/ URL: https://www.gazeta.ru/tech/news/2018/08/22/n_11933911.shtml (дата обращения: 11.11.2020)

³⁸⁵ The Disinformation Report on Foreign Interference in the 2016 Election // Yonder. Dec 17, 2018. URL: <https://www.yonder-ai.com/resources/the-disinformation-report/> (дата обращения: 11.11.2020)

источника», а также на доклад Оксфордского университета и компании *Graphika*³⁸⁶, текст которой был передан газете *The Washington Post*. Второй доклад во многом совпадал с выводами первого и добавлял устрашающие цифры о том, что контент, размещённый Агентством Интернет-исследований, был доступен десяткам миллионов пользователей в США и удостоился репостов 30 миллионов пользователей, что «русские тролли» способствовали радикализации и конфронтационному поведению крайне правых избирателей, их деятельность касалась «*расширяющегося круга вопросов государственной политики, вопросов национальной безопасности и вопросов, касающихся более молодых избирателей*», а пики их активности приходятся на важные даты политической жизни США (например, накануне и сразу после выборов 2016 г., во время ракетного удара США в Сирии). Таким образом, сенатский Комитет заключил, что дезинформационная деятельность Агентства Интернет-исследований на платформах *Facebook*, *Twitter*, *Instagram* не прекратилась после его разоблачения и является более сложной, чем представлялось ранее³⁸⁷.

Помимо давления на администрации соцсетей, в Конгрессе в этот период был выдвинут ряд новых антироссийских законодательных инициатив, призванных усилить диффамацию России и расширить арсенал политических и практических мер по противодействию её информационному влиянию. Наиболее далекоидущей из них стал законопроект одиозного республиканца Линдси Грэхема «О защите американской безопасности от агрессии Кремля (*Defending American Security from Kremlin Aggression Act of 2018, DASKAA*)³⁸⁸,

³⁸⁶ The IRA, Social Media and Political Polarization in the United States, 2012-2018 / Ph. N. Howard et al. // Computational Propaganda Research Project. University of Oxford. 46 p. URL: <https://www.documentcloud.org/documents/5631936-IRA-Report-17-Dec.html> (дата обращения: 11.11.2020)

³⁸⁷ O'Sullivan D. Russians sought to recruit 'assets' through social media, Senate told / D. O'Sullivan // CNN. Business. December 17, 2018. URL: <https://edition.cnn.com/2018/12/17/tech/russia-2016-election-social-media-report/index.html> (дата обращения: 11.11.2020); Sheth S. A new report found that Russia's disinformation operation in the US picked up speed even after it was caught by Mueller / S. Sheth // Business Insider. Dec 17, 2018. URL: <https://www.businessinsider.com/new-knowledge-oxford-reports-russia-disinformation-campaign-senate-intelligence-committee-2018-12> (дата обращения: 11.11.2020); The IRA, Social Media and Political Polarization in the United States, 2012-2018 / Ph. N. Howard et al. – Computational Propaganda Research Project. University of Oxford. – 46 p. URL: <https://www.documentcloud.org/documents/5631936-IRA-Report-17-Dec.html> (дата обращения: 11.11.2020)

³⁸⁸ Defending American Security from Kremlin Aggression Act of 2018. S. 3336. A Bill // 115th Congress. URL: <https://www.govinfo.gov/content/pkg/BILLS-115s3336is/pdf/BILLS-115s3336is.pdf> (дата обращения: 11.11.2020) URL: <https://www.govinfo.gov/content/pkg/BILLS-115s3336is/pdf/BILLS-115s3336is.pdf> (дата обращения: 11.11.2020)

представленный 1 августа 2018 г. В нём, среди прочего, предлагается создать Национальный координационный центр по отражению гибридных угроз, объединяющий должностных лиц из двадцати профильных ведомств и занимающийся, главным образом, отражением «гибридных угроз», исходящих от Правительства Российской Федерации. В числе подобных угроз упоминаются: 1) осуществление дезинформационных и пропагандистских кампаний с помощью традиционных СМИ и социальных сетей; 2) формирование, инфильтрация или манипуляция культурными, религиозными, образовательными и политическими организациями или партиями; 3) скрытая передача средств для спонсирования коррупции, преступной и подрывной деятельности, в том числе посредством политических партий и заинтересованных групп; 4) тактики принуждения, включая использование парамилитарных и параполицейских сил; 5) кибер- и другие нетрадиционные угрозы общественной инфраструктуре, органам власти или политическим организациям; 6) использование энергетических ресурсов для оказания влияния или ограничения действий государств. В целях отражения данных угроз создаваемому центру вменяется в обязанности осуществлять постоянный мониторинг публичного пространства, включая социальные сети, для своевременного выявления деструктивной информации и каналов её распространения, и регулярно докладывать о результатах этого мониторинга администрации Президента и Конгрессу (раздел 704). Кроме того, в законопроекте предлагается установить ответственность технологических компаний, в особенности социальных сетей, за гарантирование отсутствия на их платформах дезинформации, спонсируемой Правительством РФ и других иностранных государств (раздел 710).

В конце декабря 2019 г. законопроект Л. Грэхема успешно прошёл слушания в комитете Сената, однако далее его продвижение не пошло, что не исключает возможности его полного или частичного принятия в будущем. Практика последних лет показывает, что большинство выдвинутых в Конгрессе антироссийских инициатив на том или ином этапе принимаются, когда на фоне

очередной волны медийного резонанса создаётся такой политический контекст, который требует немедленного и осязаемого «наказания России». В подобных случаях заранее сформулированные и уже некоторое время обсуждаемые в СМИ проекты решений превращаются в наиболее логичные и доступные шаги, возражать против принятия которых становится политически невыгодно.

Таким образом, вопрос предполагаемого вмешательства России в ход избирательной кампании 2016 г. стал поводом для актуализации тематики «российской информационной угрозы» непосредственно в приложении к национальной безопасности США и других западных государств. Следствием этого стало законодательное закрепление возможности введения американской администрацией санкций за любые действия, направленные на донесение российского нарратива до западной аудитории, либо приписанные России действия неизвестной атрибуции, предположительно направленные на подрыв западной информационной сферы. Однако конкретные меры на этом направлении последовали лишь в середине 2018 г. и сводились к давлению на ряд российских СМИ, компаний, ассоциируемых в западной прессе с Евгением Пригожиным, обвинению нескольких десятков частных лиц и, предположительно, сотрудников российских спецслужб, без прямых обвинений в адрес российских органов власти или силовых структур.

Политико-дипломатические институциональные механизмы реагирования на «российскую информационную угрозу» в США формировались медленно, под влиянием медийной и политической конъюнктуры. Пик наибольшей активности на данном направлении пришёлся на середину 2018 г. и наблюдался на фоне медийного резонанса от «дела Скрипалей». Активизация специального созданного для противодействия иностранной пропаганде Центра глобального взаимодействия в рамках Госдепартамента произошла только в конце 2018 – начале 2019 гг. и существенно отставала от аналогичных механизмов в Европейском союзе. Наряду с этим, информационная сфера подверглась значительной милитаризации на доктринальном и институциональном уровнях, будучи интегрирована в компетенцию военного ведомства в рамках его

полномочий в области кибербезопасности и отражения киберугроз. На законодательном уровне были прописаны широкие полномочия и обязанности Пентагона в отношении проведения военных информационных операций, в том числе превентивных, скрытых и не достигающих порога прямых боевых действий. Причём были сняты действовавшие ранее ограничения, связанные с необходимостью межведомственной координации таких операций, а сами они были юридически приравнены к традиционным военным действиям, не требующим особых процедур согласования на уровне политического руководства страны. При этом в утверждённых в 2018 г. киберстратегиях были сформулированы расширительные трактовки объекта вероятных киберугроз и круга инструментов, которые могут быть применены для их нейтрализации.

Но если формальные государственные механизмы противодействия РФ в информационной сфере в США развивались постепенно и носили преимущественно рамочный характер, то на уровне негосударственных организаций и медиасреды довольно быстро была сформирована целая инфраструктура исследования, отслеживания, мониторинга и отражения «российских информационных угроз». Она включает в себя экспертные, академические, медийные, сетевые, технические организации и проекты, позволяющие не только поддерживать данную тематику в политической повестке дня независимо от позиции действующей администрации, но и постоянно развивать её, выявляя новые формы и методы распространения «кремлёвской пропаганды и фейков» и требуя от государства своевременной их нейтрализации. Причём организации и проекты подобного толка существуют как при Демократической партии (основная структура – Германский фонд Маршалла), так и при Республиканской (основная структура – Атлантический совет)³⁸⁹, что подтверждает надпартийный характер кампании по

³⁸⁹ Царик В.С. Деятельность западных негосударственных организаций и аналитических институтов в сфере борьбы с «российской дезинформацией» / В.С. Царик // Вестник Международного юридического института. – 2019. – № 4 (71). – С. 152-165.

конструированию «российской информационной угрозы» в США, не являющейся сугубо продуктом внутривнутриполитических противоречий.

3.2. Выстраивание и укрепление институциональной инфраструктуры противодействия «российской информационной угрозе» в европейских государствах

Резонанс тематики «российской информационной угрозы» после избрания Д. Трампа сказался, в том числе, и на развитии системы информационного противодействия на уровне национальных государств Европы. Данный процесс развивался неравномерно: страны-инициаторы антироссийской кампании, уже сформировавшие соответствующие внутренние механизмы на предыдущем этапе, продолжали расширять ограничительные практики, тогда как для остальных западноевропейских государств распространение утверждений о вмешательстве Кремля в их политическую жизнь и его попытки повлиять на результаты выборов с помощью информационного воздействия стали толчком для формирования подобных механизмов.

Великобритания

Отличительной чертой Великобритании в процессе конструирования западной системы противодействия «российской информационной угрозе» являлось то, что выступая активным генератором дискурса об опасности «кремлёвской пропаганды», инициатором и активным участником всех международных органов по борьбе с такой пропагандой в рамках НАТО и Евросоюза, официальный Лондон при этом не спешил с формализацией и институционализацией данного направления своей политики в структуре национального управленческого аппарата. Гласные официальные практические меры противодействия российскому информационному влиянию ограничились доктринальным выделением «российской дезинформации» как особо опасного вида угрозы и созданием двух специальных команд, одна из которых была

ориентирована на работу с гражданами-потребителями информации, а другая – на представителей СМИ, запустивших регулярные практики по недопущению российского влияния.

Интерес к тематике информационного влияния России в Британии усилился на фоне неожиданного исхода президентской кампании 2016 г. в США в свете возможного вмешательства России в британский референдум по выходу из ЕС 2016 г. Ещё 21 февраля 2017 г. Комитет по внешним сношениям Палаты общин выпустил отчёт о британско-российских отношениях, некоторые пункты которого (149-й, 152-й и 155-й) непосредственно касались информационной войны. Говорилось о финансировании российским Правительством каналов *RT* и *Sputnik News*, о якобы нарушении ими беспристрастности (таковым примером считалось утверждение телеканала *RT* о фальсификации компанией *BBC* части отчёта о химической атаке в Гуте), о необходимости «творческого подхода» к противодействию российской информационной кампании в русскоязычных регионах Украины и Прибалтики: расширении вещания *BBC*, а за рамками этого вещания – «расширения поддержки независимых СМИ»³⁹⁰. 3 марта 2017 г. Правительство Великобритании ответило на документ парламентского Комитета, полностью согласившись с его тезисами и даже расширив формулировки, а также ответив на вопрос о планах противодействия российскому нарративу через русскоязычное вещание³⁹¹.

Однако большую часть 2017 г. становление британских структур информационной войны с Россией шло не слишком активно, поскольку работа по обоснованию их необходимости ещё не была закончена, и практических шагов по формированию особых структур информационного противодействия России предпринято не было. И только ближе к концу года деятельность в этом направлении резко активизировалась.

³⁹⁰ The United Kingdom's relations with Russia. Seventh Report of Session 2016–17 // House of Commons. Foreign Affairs Committee. URL: <https://publications.parliament.uk/pa/cm201617/cmselect/cmfaaff/120/120.pdf> (дата обращения: 11.11.2020)

³⁹¹ The United Kingdom's relations with Russia: Government Response to the Foreign Committee's Seventh Report of Session 2016–17, published on 2 March 2017. URL: <https://publications.parliament.uk/pa/cm201719/cmselect/cmfaaff/332/33202.htm> (дата обращения: 11.11.2020)

13 ноября 2017 г. Премьер-министр Тереза Мэй в ежегодной речи на банкете лорда-мэра заявила о дезинформационной кампании России, направленной на внесение раздора и подрыв демократических институтов, однако позднее в ответе на вопрос парламентария в палате общин отрицала возможность России повлиять на британские выборы и референдум.

23 ноября 2017 г. парламентский Комитет по разведке и безопасности провёл первое заседание, посвящённое расследованию действий России против Великобритании³⁹². В ежегодном отчёте комитета за 2016-2017 гг., опубликованном в декабре 2017 г., рассматривались, среди прочего, уязвимости в киберсфере, и на основании опыта «вмешательства» в президентские выборы в США делался вывод о том, что *«государственные акторы обладают высокой способностью осуществлять передовые кибератаки»*, однако использование этих методов ограничено ответными мерами, *«которые последуют в случае обнаружения такой деятельности. Недавняя российская киберактивность, похоже, указывает на то, что это перестало быть сдерживающим фактором»*³⁹³. Целями возможных кибератак против страны, по мнению авторов доклада, могли быть подрыв нормального порядка функционирования политических процессов в Великобритании, подрыв конкретных выборов или референдума с выгодой для предпочитаемой стороны враждебного актора, нанесение вреда общественному дискурсу по чувствительным политическим вопросам и выявление людей, которые могут быть открыты для подрывной деятельности или политического экстремизма в интересах враждебного актора³⁹⁴. А уже 21 декабря Тереза Мэй заявила о запуске совместного польско-

³⁹² Garraway A. Russian interference in UK politics and society / A. Garraway, B. Smith. – Research Briefing. House of Commons Library. 19 December, 2017. URL: <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CDP-2017-0255> (дата обращения: 11.11.2020)

³⁹³ Annual report 2016–2017, Intelligence and Security Committee of Parliament, 2018. p. 31. URL: <https://www.gov.uk/government/publications/intelligence-and-security-committee-annual-report-2016-2017> (дата обращения: 11.11.2020). Цит. по: Попов П.В. Возможности демократических государств по реагированию и противодействию гибридным угрозам / П.В. Попов // Via in tempore. История. Политология, 2020. Vol. 47, No 1. P. 187-193.

³⁹⁴ Там же, pp. 32-33.

британского проекта по борьбе с «российской пропагандой», на которую каждая из сторон должна была выделить по пять миллионов фунтов стерлингов³⁹⁵.

23 января 2018 г., на следующий день после шокирующего заявления начальника Генерального штаба Великобритании Николаса Картера о том, что Россия хотела бы начать новую мировую войну, пока Запад не получил над ней дополнительное технологическое преимущество, Совет национальной безопасности решил создать в Великобритании новое национальное подразделение для противодействия дезинформации от иностранных государств, включая Россию. В заявлении пресс-секретаря Терезы Мэй говорилось: *«Мы живём в эпоху фейковых новостей и конкурирующих нарративов. Правительство будет реагировать всё активнее и эффективнее»*³⁹⁶.

Повод для активного повышения эффективности представился после предположительного отравления в Солсбери Сергея Скрипаля 4 марта 2018 г. и обвинений РФ в многочисленных актах дезинформации касательно этого события. Уже в конце месяца Совет национальной безопасности выпустил Обзор возможностей национальной безопасности³⁹⁷, центральная часть которой представляла т. н. «Доктрину слияния» (*Fusion Doctrine*), предполагавшая соединение (слияние) возможностей национальной обороны, экономики, дипломатии, коммуникационной политики для достижения «национальных задач». Тем самым, роль коммуникаций повышалась по значимости до финансовых и военных вопросов, в частности, Премьер-министр Тереза Мэй объявила, что выявлением искажающих и дезинформирующих соцсетей займутся разведывательные службы, которые будут использовать социальные сети, чтобы подорвать дезинформацию из Москвы. Как поясняла газета *The Telegraph*, британские эксперты по безопасности объясняли это необходимостью

³⁹⁵ Захаров Р. Польша и Великобритания объединятся в борьбе с «российской пропагандой» / Звезда, 21.12.2017. URL: https://tvzvezda.ru/news/vstrane_i_mire/content/201712211613-j3uu.htm (дата обращения: 11.11.2020)

³⁹⁶ British army to create a unit against Russian propaganda // Voltaire Network. 6 February 2018. URL: <https://www.voltairenet.org/article199602.html> (дата обращения: 11.11.2020)

³⁹⁷ National Security Capability Review (NSCR) // Cabinet Office. 28 March 2018. URL: <https://www.gov.uk/government/publications/national-security-capability-review-nscr> (дата обращения: 11.11.2020)

нейтрализовать более 20 различных нарративов, придуманных «Правительством Президента Путина», чтобы объяснить нападение в Солсбери и запутать картину происходящего для экспертов. Частью новой линии фронта должны были стать британские «мягкие силы» и способность противостоять пропаганде в Интернете. Также в Обзоре отмечалось, что важную роль в защите будут играть коммуникации, а противодействие дезинформации станет важным оружием в арсенале³⁹⁸.

Действия Правительства по институционализации мер информационного противодействия разветвились по двум направлениям.

В апреле 2018 г. Правительство объявило, что оно «значительно расширит» Команду национальной безопасности по коммуникациям (NSCT), которая должна заниматься устранением в коммуникациях элементов, составляющих угрозу национальной безопасности, включая (но не только) дезинформацию³⁹⁹. В числе инициатив этой команды, собранной из правительственных специалистов по СМИ, была запущенная кампания «Не кормите зверя», в рамках которой общественность побуждалась к обнаружению дезинформации по чувствительным вопросам (вакцинация, массовые беспорядки, мистификации) до того, как она будет распространена. Был предложен контрольный список действий гражданина для самостоятельной проверки информации в Интернете перед тем, как поделиться ею в соцсети: проверка источника, соответствия заголовка содержанию, фактов, фотографий, подлинности URL-адресов; наконец, обращение внимания на орфографию⁴⁰⁰.

Также в апреле 2018 г. Кабинет министров создал в рамках Государственной службы связи при Правительстве Группу быстрого

³⁹⁸ Mccann K. Britain to launch counter-propaganda war against Russia as Theresa May unveils 'Fusion Doctrine' defence plan / K. Mccann / The Telegraph. 28 March 2018. URL <https://www.telegraph.co.uk/politics/2018/03/27/britain-launch-counter-propaganda-war-against-russia-theresa/> (дата обращения: 11.11.2020)

³⁹⁹ Owen J. Government boosts national security comms capability to combat international threats / J. Owen // PRWeek. May 23, 2018. URL: <https://www.prweek.com/article/1465497/government-boosts-national-security-comms-capability-combat-international-threats> (дата обращения: 11.11.2020)

⁴⁰⁰ Government Responses to Disinformation on Social Media Platforms: United Kingdom // Library of Congress, Legal Reports. URL: <https://www.loc.gov/law/help/social-media-disinformation/uk.php> (дата обращения: 11.11.2020)

реагирования⁴⁰¹ из «специалистов, включая аналитиков-редакторов, специалистов по обработке данных, специалистов по СМИ и цифровых экспертов»⁴⁰² с задачей «отслеживать ... новости и информацию, которые распространяются и используются в Интернете, чтобы выявлять возникающие проблемы быстро, точно и с целостностью»⁴⁰³. Результаты этого мониторинга должны были «помочь Правительству понять текущие СМИ... и оценить эффективность их общественных коммуникаций»⁴⁰⁴. В отличие от Команды национальной безопасности, в задачу Группы быстрого реагирования входило не создание алгоритмов для нераспространения отдельных «фейковых новостей», а отслеживание тенденций в информационном пространстве, в основном, по запросам в поисковых системах, чтобы своевременно корректировать результаты поиска и информационную политику правительства. Кроме того, Подразделение было ориентировано на работу с представителями СМИ и корректировку их редакционной политики, в частности, разработало для них модель с аббревиатурой *FACT* с алгоритмом «быстрого реагирования на неточности», а также продвигало «общественные дебаты, основанные на фактах»⁴⁰⁵.

В течение весны 2018 г. было озвучено ещё несколько обвинений по адресу России. 17 апреля 2018 г. ФБР, Министерство внутренней безопасности (МВБ) США и Национальный центр кибербезопасности Великобритании опубликовали техническое предупреждение о «злонамеренной киберактивности российского Правительства», а 20 апреля 2018 г. в британском Парламенте была создана

⁴⁰¹ Alex Aiken introduces the Rapid Response Unit // Government Communication Service. 19 July 2018. URL: <https://webarchive.nationalarchives.gov.uk/20200203104056/https://gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/> (дата обращения: 11.11.2020); Robinson M. Beyond Integrity Initiative: The Scale of UKGOV Counter Disinformation / M. Robinson // UKCOLUMN. 7th February 2019. URL: <https://www.ukcolumn.org/article/beyond-integrity-initiative-scale-ukgov-counter-disinformation> (дата обращения: 11.11.2020)

⁴⁰² Alex Aiken introduces the Rapid Response Unit // Government Communication Service. 19 July 2018. URL: <https://webarchive.nationalarchives.gov.uk/20200203104056/https://gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/> (дата обращения: 11.11.2020)

⁴⁰³ Там же.

⁴⁰⁴ 5 Trends in Leading-Edge Communications // Government Communication Service. 7 Oct. 2018. URL: <https://gcs.civilservice.gov.uk/publications/five-trends-in-leading-edge-communications/> (дата обращения: 11.11.2020)

⁴⁰⁵ Cabinet Office, Rapid Response Unit: Written Question – 226754 // Parliament.UK. Mar. 4, 2019. URL: <https://perma.cc/KL7K-MBTL> (дата обращения: 11.11.2020)

специальная координационная группа, которая должна была сосредоточиться на разборе российского вмешательства в выборы и распространении дезинформации⁴⁰⁶. 18 апреля 2018 г. британский телекоммуникационный регулятор Ofcom инициировал семь расследований о «необъективности» при освещении дела об отравлении Сергея Скрипаля и его дочери Юлии в Солсбери телеканалом *RT*. По итогам расследования предполагалось назначение штрафа или лишение лицензии⁴⁰⁷. 21 мая 2018 г. были открыты ещё три подобных расследования⁴⁰⁸.

27 июня 2018 г., в рамках противостояния «российской дезинформации», Великобритания выделила 5 миллионов евро Украине на *«поддержку украинской общественной телерадиовещательной компании, проект помощи украинским школам по созданию устойчивости против дезинформации, финансирование сети НПО в Европе для развенчивания недостоверных новостных сюжетов»*⁴⁰⁹.

В течение лета и осени относительно малозначимые практические шаги продолжали сочетаться с дискурсивным нагнетанием информационного противостояния. 28 июля 2018 г. Комитет по цифровой культуре, медиа и спорту Палаты общин выпустил промежуточный отчёт «Дезинформация и фейковые новости», в котором дал подробные пояснения по феномену и проблематике дезинформации и кибербезопасности, а также посвятил большой раздел российскому влиянию на политические процессы в Великобритании⁴¹⁰. 5

⁴⁰⁶ Медведева Н. В Британии депутаты создали спецгруппу для борьбы с влиянием РФ / Н. Медведева // Ліга.Новости. 20.04.2018. URL: <https://news.liga.net/world/news/v-britanii-deputaty-sozdali-spetsgruppu-dlya-borby-s-vliyaniem-rf> (дата обращения: 11.11.2020)

⁴⁰⁷ Великобритания начала семь расследований против RT за необъективное освещение «дела Скрипаля» // Новая газета. 18 апреля 2018. URL: <https://www.novayagazeta.ru/news/2018/04/18/141080-velikobritaniya-nachala-sem-rassledovaniy-protiv-rt-za-neobektivnoe-osveschenie-dela-skripalya> (дата обращения: 11.11.2020)

⁴⁰⁸ В Британии начали три новых расследования против RT // Газета.ру. 21.05.2018. URL: https://www.gazeta.ru/tech/news/2018/05/21/n_11559871.shtml (дата обращения: 11.11.2020); Великобритания открыла три расследования против RT из-за нарушения принципа объективности // Новая газета. 21 мая 2018. URL: <https://www.novayagazeta.ru/news/2018/05/21/141845-velikobritaniya-otkryla-tri-rassledovaniya-protiv-rt-iz-zanarusheniya-printsipa-obektivnosti> (дата обращения: 11.11.2020)

⁴⁰⁹ Скрыпач И. Британия пришла на украинский рынок «борьбы с российской пропагандой» ради «слабеющего» Порошенко / И. Скрыпач // Экономика сегодня. 27 Июня 2018. URL: <https://rueconomics.ru/334749-britaniya-prishla-na-ukrainskii-rynok-borby-s-rossiiskoi-propagandoi-radi-slabeyushhego-poroshenko> (дата обращения: 11.11.2020)

⁴¹⁰ Disinformation and 'fake news': Interim Report. 29 July 2018 URL: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcmds/363/36302.htm> (дата обращения: 11.11.2020)

сентября 2018 г. Тереза Мэй заявила о необходимости введения нового механизма санкций ЕС за использование химического оружия, кибератаки и нарушения прав человека⁴¹¹. 21 сентября 2018 г. было сообщено о намерении британских властей выделить не менее 250 млн. фунтов стерлингов на увеличение численности «наступательных» кибервойск почти в четыре раза, до 2 тысяч специалистов, чтобы «сдерживать» страны, желающие нанести ущерб Великобритании⁴¹².

4 октября 2018 г. МИД Великобритании обвинил российское ГРУ в кибератаках в отношении самых разных объектов по всему миру: серверов Демократической партии США, организации WADA, транспортных систем на Украине, демократий разных стран и бизне-структур. Министр иностранных дел Джереми Хант заявил по этому поводу: *«Наша идея ясна: вместе с нашими союзниками мы разоблачим и ответим на попытки ГРУ подорвать международную стабильность»*. Кроме того, в заявлении британского МИД были приведены хакерские объединения, которые, по оценке Национального центра кибербезопасности Великобритании, управлялись ГРУ⁴¹³.

Поворот к ещё более жёсткому ограничению информационного пространства Великобритании от попыток коммуникации со стороны России наметился к концу 2018 г. и завершился в начале 2019 г. 23 октября 2018 г. британское Правительство опубликовало ответ⁴¹⁴ на июльский промежуточный отчёт парламентского Комитета, в котором выдвинуло целый ряд рекомендаций, как то более широкое понимание дезинформации, установление стандартов новостного контента телекоммуникационным регулятором Ofcom, расширение

⁴¹¹ Кулькова О. Как Британия собирается «наказать» Россию? / О. Кулькова // РСМД. 1 октября 2018. URL: http://russiancouncil.ru/analytics-and-comments/analytics/kak-britaniya-sobiraetsya-nakazat-rossiyu/?sphrase_id=20895665 (дата обращения: 11.11.2020)

⁴¹² Sky News: Британия собирает наступательные кибервойска для противодействия России // Газета.ru. 21.09.2018. URL: https://www.gazeta.ru/tech/news/2018/09/21/n_12065293.shtml (дата обращения: 11.11.2020)

⁴¹³ Британский МИД обвинил ГРУ в «неизбирательных и безрассудных» кибератаках // РБК. 04 окт 2018. URL: <https://www.rbc.ru/politics/04/10/2018/5bb568109a79475eb1173794?from=main> (дата обращения: 11.11.2020); Reckless campaign of cyber attacks by Russian military intelligence service exposed // National Cyber security Centre. 3 October 2018. URL: <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> (дата обращения: 11.11.2020)

⁴¹⁴ 5th Special Report - Disinformation and 'fake news': Interim Report: Government Response to the Committee's Fifth Report. 9 October 2018. URL: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1630/163002.htm> (дата обращения: 11.11.2020)

прав Информационного уполномоченного, принуждение *Facebook* и других социальных сетей к выполнению своей части работы, установление «цифровой Атлантической хартии», созыв межпарламентского собрания Атлантического совета для обсуждения информационных рисков и российского вмешательства и т. д.

Ноябрь и декабрь 2018 г. ознаменовались наслоением двух тенденций. С одной стороны, были опубликованы разоблачения о британском проекте *Integrity Initiative*⁴¹⁵, курируемом Институтом построения государства (Institute for Statecraft), который, в свою очередь, получал бюджетное финансирование от британского МИДа⁴¹⁶. Эта информация продемонстрировала дирижируемый британскими манипуляторами характер видимой, публичной части общеевропейского «общественного негодования» по поводу «российского вмешательства», академических и псевдоакадемических исследований «российской гибридной войны», неправительственных инициатив по «сопротивлению российской агрессии»⁴¹⁷. К сожалению, сенсационный характер подачи материала (сосредоточение на шокирующих подробностях, таких как предложение директора института Кристофера Донелли заминировать Севастопольскую бухту⁴¹⁸), помешал адекватной интерпретации этих данных в контексте проблемы конструирования «российской угрозы» (в т. ч. информационной) и, шире, всей тематики «гибридной войны». Простое

⁴¹⁵ Integrity Initiative. Начало // Окологремля. 23.11.2018. URL: <https://okolokremlya.ru/content/5133> (дата обращения: 11.11.2020)

⁴¹⁶ Foreign and Commonwealth Office: Integrity Initiative. Question for Foreign and Commonwealth Office. UIN 196177, tabled on 27 November 2018. URL: <https://questions-statements.parliament.uk/written-questions/detail/2018-11-27/196177> (дата обращения: 11.11.2020)

⁴¹⁷ Британские спецслужбы активизировали крупнейшую агентурную сеть под легендой "борьбы с российской дезинформацией" // Окологремля. 22.11.2018 URL: <https://okolokremlya.ru/content/5130> (дата обращения: 11.11.2020); Операция «Монклоа» // Colonelcassad. 22.11.2018 URL: <https://colonelcassad.livejournal.com/4596438.html> (дата обращения: 11.11.2020), Операция Integrity Initiative. // Colonelcassad. 30.11.2018. URL: <https://colonelcassad.livejournal.com/4612495.html> (дата обращения: 11.11.2020); Устаревшие (удалённые) ссылки: <https://archive.cyberguerrilla.org/a/2018/operation-integrity-initiative-british-informational-war-against-all/>, <https://archive.cyberguerrilla.org/a/2018/operation-integrity-initiative-british-informational-war-against-all-part-2/>, <https://archive.cyberguerrilla.org/a/2018/operation-integrity-initiative-british-informational-war-against-all-part-3/>, <https://www.cyberguerrilla.org/blog/operation-integrity-initiative-british-informational-war-against-all-part-4/> (дата обращения: 7.07.2020).

⁴¹⁸ Фахрутдинов Р. «Заминируем Севастополь»: что придумали британские чиновники. Хакеры Anonymous выложили новые данные по Integrity Initiative / Р. Фахрутдинов // Газета.ру. 15.12.2018. URL: https://www.gazeta.ru/tech/2018/12/15_a_12095869.shtml?updated (дата обращения: 11.11.2020)

хронологическое отслеживание процесса оставляет впечатление о тревоге обеспокоенной общественности западных стран, бескорыстных инициативников из НГО и искателей истины среди академических исследователей по поводу «российской агрессии», которые смогли достучаться до прессы и парламентариев своих стран либо ЕС; последние инициировали расследования и, обнаружив масштабы проблемы, принудили правительства своих стран и Еврокомиссию усилить на правительственном уровне борьбу с «российской угрозой», подключая к «сопротивлению российской агрессии» масс-медиа, социальные сети, спецслужбы, правоохранные органы. Но информация о проекте *Integrity Initiative* переставляет причинно-следственные связи. Выясняется, что на первом месте стояла организация и финансирование полусекретными структурами в европейских странах скоординированных *кластеров*⁴¹⁹ из представителей общественности, инициативников НГО и экспертов, публицистов и руководителей СМИ, политических представителей, блогеров и ботов в соцсетях, которые изображали искреннее беспокойство по поводу «российской агрессии» и запускали в своих странах конструирование российской угрозы. Иными словами, речь идёт об имитации демократических процедур для получения изначально запрограммированного результата. (Во время слушаний 12 декабря 2018 г. в Палате общин замминистра иностранных дел подтвердил, что министерство выделяло Институту госуправления, которому подчинялись некоторые кластеры *Integrity Initiative*, 2 млн. фунтов стерлингов, но только на заграничную деятельность, а не для влияния внутри Великобритании⁴²⁰, то есть управляемая имитация демократического процесса в других странах даже не рассматривалась как незаконная.)

С другой стороны, несмотря на разоблачения, конструирование «российской угрозы» продолжало идти по намеченному пути. Так, 5 ноября

⁴¹⁹ Антироссийскую сеть планировалось создать на базе университета в Брюсселе // РИА. 24.11.2018. URL: <https://ria.ru/20181124/1533417894.html> (дата обращения: 11.11.2020)

⁴²⁰ Institute for Statecraft: Integrity Initiative // House of Commons Hansard. 12 December 2018. URL: <https://hansard.parliament.uk/Commons/2018-12-12/debates/298F9A3C-307A-40ED-9CB1-3B2A98F14165/InstituteForStatecraftIntegrityInitiative> (дата обращения: 11.11.2020)

2018 г. общество Генри Джексона выпустило доклад «Путин всё видит и слышит всё: как агенты российской разведки угрожают Соединённому Королевству»⁴²¹. 24 ноября 2018 г. начальник Генштаба армии Великобритании заявил, что угроза от РФ превосходит таковую от ИГИЛ, и пояснил, что, помимо конвенциональной военной угрозы, русские постоянно пытаются подорвать Запад через развитие новых возможностей в кибернетической сфере и в космосе⁴²². 27 ноября 2018 г. в Палате общин заслушали показания Ричарда Алена, вице-президента «Фейсбука», по вопросу о противодействии его компании дезинформации и фейковым новостям⁴²³. 20 февраля 2019 г. Комитет по цифровым технологиям, культуре, СМИ и спорту парламента Великобритании опубликовал свой окончательный отчет о дезинформации и «фейковых новостях», в котором подтвердил выводы июльского промежуточного отчёта и, кроме того, потребовал более активного преследования национальным регулятором компаний-распространителей вредоносного контента, а также более активной борьбы компаний-владельцев соцсетей против дезинформации⁴²⁴.

Ещё до публикации отчёта большим практическим шагом в рамках правового давления на источники российского нарратива стало завершение 20 декабря 2018 г. расследований, начатых ещё в апреле британским медиарегулятором *Ofcom* против телеканала *RT*. Регулятор пришёл к выводу о нарушении каналом принципов объективности при освещении дела Скрипалей и конфликта в Сирии, решение о санкциях (штрафе или отзыве лицензии) было отложено на более поздний срок. А 23 декабря 2018 г., в рамках давления на

⁴²¹ Foxall A. Putin Sees and Hears it all: How Russia's Intelligence Agencies Menace The UK / A. Foxall. – Henry Jackson Society Report. 5th November 2018. URL: <https://henryjacksonsociety.org/publications/as-many-as-200-russian-case-officers-in-london-handling-up-to-500-agents-and-75000-informants-report-finds/> (дата обращения: 11.11.2020)

⁴²² Coughlin C. Russia poses greater threat to Britain than Isil, says new Army chief / C. Coughlin // The Telegraph. 23 November 2018. URL: <https://www.telegraph.co.uk/news/2018/11/23/russia-poses-greater-threat-britain-isil-says-new-army-chief/> (дата обращения: 11.11.2020)

⁴²³ Oral evidence: Disinformation and 'fake news', HC 363. – Digital, Culture, Media and Sport International Grand Committee // House of Commons. 27 November 2018. URL: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/92923.pdf> (дата обращения: 11.11.2020)

⁴²⁴ Disinformation and 'fake news': Final Report published. The Digital, Culture, Media and Sport Committee has published its final report on Disinformation and 'fake news' // House of Commons. 18 February 2019. URL: <https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/> (дата обращения: 11.11.2020)

канал *Sputnik*, британская газета «Таймс» опубликовала имена и фотографии восьми сотрудников агентства, которые первыми опубликовали данные о проекте *Integrity Initiative*⁴²⁵.

Франция

После президентских выборов 2017 г. Франция начала перемещаться из относительно нейтральных стран, идущих в последних рядах антироссийских инициатив, в их более заметного проводника, хотя и не слишком активного на официальном уровне.

В западных СМИ считается, что российским фаворитом на выборах была кандидатура Марин Ле Пен, а победа над ней Макрона во втором туре голосования чуть было не сорвалась из-за взлома его почты хакерами: только установленный французским законодательством «день тишины» накануне голосования помешал широкому освещению содержания этой почты и подрыву позиций Макрона. Предполагаемая заинтересованность РФ в победе Марин Ле Пен позволила привязать Россию к откровенно противозаконной деятельности хакеров, а заодно криминализировать политические контакты французских политиков с Россией, выражение симпатии к французской оппозиции российскими СМИ и т. п. Уже 7 мая 2017 г. в *Wikileaks* заявили о российском следе во взломе почте Макрона⁴²⁶, а 29 мая после двусторонних переговоров с Президентом РФ В.В. Путиным новоизбранный Президент Франции, оправдывая недопуск журналистов *RT* и *Sputnik* в свой предвыборный штаб, заявил: «*Russia Today* и *Sputnik* во время этой [избирательной] кампании были органами иностранной пропаганды, которые неоднократно распространяли неправду обо мне и моей кампании. <...> *Russia Today* и *Sputnik* вели себя не как

⁴²⁵ Минеева Ю. Сбитый *Sputnik*. Россия и Британия продолжают медийную гибридную войну / Ю. Минеева // Новая газета. 29 декабря 2018. URL: <https://www.novayagazeta.ru/articles/2018/12/29/79098-sbityy-sputnik> (дата обращения: 11.11.2020)

⁴²⁶ В *Wikileaks* заявили о российском следе во взломанной почте Макрона // INTERFAX.RU. 7 мая 2017. URL: <https://www.interfax.ru/world/561431> (дата обращения: 11.11.2020)

*органы прессы и не как журналисты, но как органы влияния, пропаганды и лживой пропаганды...»*⁴²⁷.

Однако 1 июня 2017 г. Управление по информационной безопасности Правительства Франции заявило об отсутствии свидетельств о причастности группы российских хакеров к атаке на предвыборную кампанию Эммануэля Макрона⁴²⁸. Следующие полгода антироссийская повестка продвигалась больше на неофициальном уровне. Так, в декабре 2017 г. французские власти позволили открыть франкоязычную версию телеканала *RT*.

Несмотря на это, уже 3 января 2018 г. Э. Макрон рассказал о планах противодействия «фейковым СМИ» и иностранных «органов дезинформации» и заявил, что планирует дать контролирующим органам дополнительные полномочия для отзыва журналистских лицензий либо отказа в них, а также для наказаний за нарушения⁴²⁹. Началось подчёркнутое третирование представителей российских СМИ, например, 15 января 2018 г. корреспондента *RT France* не пустили на брифинг пресс-секретаря французского Президента⁴³⁰.

Для лучшего понимания выстраиваемой в этот период системы борьбы с российским информационным влиянием следует учитывать, что французское государство обладало инструментами преодоления (настоящей) дезинформации задолго до ухудшения отношений с Россией. Французское законодательство, в отличие от немецкого, содержало довольно детальное регулирование деятельности СМИ и проявлений свободы слова⁴³¹. Так, недобросовестная

⁴²⁷ Ерёмина Д. Макрон назвал *RT* и *Sputnik* инструментами влияния и пропаганды / Д. Ерёмина // DW. 29.05.2017. URL: <https://www.dw.com/ru/макрон-назвал-rt-и-sputnik-инструментами-влияния-и-пропаганды/a-39035271> (дата обращения: 11.11.2020), Сафронов Ю. 50 оттенков подрывной деятельности. Франция собирается бороться с российской пропагандой, Москва обвиняет ее в цензуре / Ю. Сафронов // Новая газета. 06 сентября 2018. URL: <https://www.novayagazeta.ru/articles/2018/09/06/77731-50-ottenkov-podryvnoy-deyatelnosti> (дата обращения: 11.11.2020)

⁴²⁸ Французские власти не нашли следов атаки хакеров из РФ на штаб Макрона // INTERFAX.RU. 1 июня 2017. URL: <https://www.interfax.ru/world/564892> (дата обращения: 11.11.2020)

⁴²⁹ Сафронов Ю. Макрон примет закон против иностранной пропаганды / Ю. Сафронов // Новая газета. 4 января 2018. URL: <https://www.novayagazeta.ru/articles/2018/01/04/75074-makron-primet-zakon-protiv-inostrannoy-propagandy> (дата обращения: 11.11.2020)

⁴³⁰ Фахрутдинов Р. «Макрон вместо свободы слова защищает багет». Корреспондента *RT France* не пустили в Елисейский дворец / Газета.ru // Р. Фахрутдинов. 15.01.2018. URL: <https://www.gazeta.ru/social/2018/01/15/11614082.shtml> (дата обращения: 11.11.2020)

⁴³¹ Здесь и далее в этом подразделе изложение особенностей законодательного регулирования информационного пространства Франции опирается на Boring N. France / N. Boring // Government Responses to Disinformation on

«публикация, распространение или воспроизведение любыми средствами фальшивых новостей [и] материалов, которые были сфабрикованы, сфальсифицированы или неправдиво приписаны третьим лицам», когда такие действия могут вызвать беспокойство у общественности, наказываются штрафом в размере 45 000 евро, крупные штрафы положены за клевету и публичные оскорбления. Законодательство также регулировало политическую рекламу в обычных и «аудиовизуальных» СМИ, закон 2011 г. распространил ограничения на Интернет. За нарушение норм тоже были предусмотрены штрафы. Таким образом, существовавшие нормы не носили характера, направленного против влияния иностранных государств, тем более адресного, но распространяли на Интернет и СМИ правила здоровых взаимоотношений в обществе. Примером активной регулирующей деятельности правительственных органов по защите информационного пространства Франции на указанной правовой основе стала «просьба» Национальной комиссии по контролю избирательной кампании к СМИ не публиковать письма из штаба Макрона, полученные накануне выборов в результате утечки, поскольку такая публикация нарушала бы «день тишины»⁴³².

7 июня 2018 г. депутаты президентской фракции «Вперёд, республика!» вынесли на рассмотрение законопроект о борьбе с манипуляцией в СМИ, который должен был действовать в течение 3 месяцев перед любыми выборами. В законопроекте любому кандидату предоставлялась возможность в 48-часовой срок получить судебное решение о приостановке распространения ложной информации, для органов регулирования упрощалось решение вопроса об отзыве лицензий для СМИ, используемых *«для посягательства на основополагающие национальные интересы и для участия в действиях по дестабилизации государственных институтов, в частности, путем*

Social Media Platforms. Report for Congress. September 2019. P. 73-81. URL: <https://www.loc.gov/law/help/social-media-disinformation/social-media-disinformation.pdf> (дата обращения: 11.11.2020).

⁴³² Conley H.A. Successfully Countering Russian Electoral Interference 2 / H.A. Conley, J.-B. Jeangène Vilmer. – CSIS Briefs. June 2018. URL: <https://www.csis.org/analysis/successfully-countering-russian-electoral-interference> (дата обращения: 11.11.2020)

распространения ложных сведений», социальным сетям вменялось повышение прозрачности в вопросах финансирования рекламных объявлений. Этот половинчатый законопроект, полный размытых формулировок, подвергся критике с разных сторон и был отправлен на доработку⁴³³.

Доработанный законопроект, в котором вместо понятия «фейковых новостей» использовалось более широкое определение «манипулирование информацией», был принят французским парламентом в ноябре 2018 г. и утверждён Конституционным судом в декабре⁴³⁴. Под наименованием Закона о борьбе с распространением ложной информации он был подписан Эммануэлем Макроном 22 декабря 2018 г. и наложил дополнительные обязательства на администрацию соцсетей и других Интернет-источников⁴³⁵. Онлайн-платформам вменялось создание «легкодоступного и видимого» метода отметки фейковых новостей пользователями, продвижение контента агентств печати, радио и телевидения, борьба с аккаунтами, массово распространяющими фальшивую информацию, информирование пользователей о личностях, купивших платный контент по политически значимым вопросам, медиа-просвещение людей о средствах массовой информации и информации, предоставление статистики характера доступа пользователей. Они должны были предоставлять Национальному совету по аудиовизуальным средствам (*Conseil supérieur de l'audiovisuel, CSA*) ежегодные отчёты о своей борьбе с фейковыми новостями, а агентство – публиковать регулярные отчёты о деятельности онлайн-платформ в этом вопросе. Несоблюдение требований массово посещаемыми онлайн-платформами карается тюремным заключением на срок до одного года и штрафом. В предвыборный и выборный период суды уполномочены принимать по ходатайству прокурора, кандидата, политической

⁴³³ Парламент Франции рассмотрел меры по борьбе с «манипулированием информацией» // RFI. 07/06/2018. URL: <http://www.rfi.fr/ru/frantsiya/20180607-parlament-frantsii-rassmotrel-mery-po-borbe-s-manipulirovaniem-informatsiei> (дата обращения: 11.11.2020)

⁴³⁴ Funke D. A guide to anti-misinformation actions around the world / D. Funke, D. Flamini. – Poynter. 2018. URL: <https://www.poynter.org/ifcn/anti-misinformation-actions/#france> (дата обращения: 11.11.2020)

⁴³⁵ Loi relative à la lutte contre la manipulation de l'information : DOSSIER LEGISLATIF // Senat.fr. URL: <https://www.senat.fr/dossier-legislatif/ppl17-623.html> (дата обращения: 11.11.2020)

партии, отдельных лиц *«любую пропорциональную и необходимую меру»*, чтобы остановить *«преднамеренное, искусственное или автоматическое и массовое»* распространение фальшивой или вводящей в заблуждение информации онлайн.

Кроме того, CSA может приостановить действие лицензии на вещание оператора, контролируемого иностранным государством или находящегося под его влиянием, если в период выборов он передает ложную информацию, которая может повлиять на результаты выборов, после первого предупреждения отозвать лицензию на вещание у оператора радио или телевидения, контролируемого или находящегося под влиянием иностранного государства, если он передает контент, который наносит ущерб *«фундаментальным интересам нации»*. В положении поясняется, что распространение ложной информации, препятствующей нормальному функционированию институтов, должно рассматриваться как наносящее ущерб фундаментальным национальным интересам.

На фоне доработки и принятия закона предпринимались практические действия, направленные против информационного влияния России: 27 июня 2018 г. французский Высший совет по аудиовизуальным средствам (CSA) вынес предписание о «несоблюдение (норм) честности, точности подачи информации и разнообразия точек зрения» во время эфира 13 апреля 2018 г., в которой говорилось об инсценировке группировкой «Джейш-аль-Ислам» химической атаки в Восточной Гуте, ответственность за которую Запад возложил на официальный Дамаск⁴³⁶. Звучали и новые обвинения: в декабре 2018 г. Франция начала расследование возможного вмешательства России в организацию движения «жёлтых жилетов» и обнаружила, что сотни аккаунтов в соцсетях, связанные с РФ, стремились усилить уличные протесты⁴³⁷.

⁴³⁶ Маргарита Симоньян сообщила о начале расследования в отношении RT полицией Австралии // Новая газета. 17 июля 2018. URL: <https://www.novayagazeta.ru/news/2018/07/17/143396-margarita-simonyan-soobschila-o-nachale-rassledovaniya-v-otnoshenii-rt-politsiy-avstralii> (дата обращения: 11.11.2020), Сафронов Ю. «Несоблюдение норм честности»: за что телеканалу RT вынесли предписание во Франции / Ю. Сафронов // Новая газета. 29 июня 2018. URL: <https://www.novayagazeta.ru/news/2018/06/29/142900-nesoblyudenie-norm-chestnosti-za-chto-telekanalu-rt-vynесли-predpisanie-vo-frantsii> (дата обращения: 11.11.2020)

⁴³⁷ Blakely R. Russian accounts fuel French outrage online / R. Blakely / The Times. December 08, 2018. URL: <https://www.thetimes.co.uk/article/russian-accounts-fuel-protesters-outrage-online-xx2f2g8th> (дата обращения: 11.11.2020), Matlack C. France to Probe Possible Russian Influence on Yellow Vest Riots / C. Matlack, R. Williams //

Со временем более отчётливой становилась и личная роль Э. Макрона в становлении системы противодействия «российской информационной угрозе». Так, в марте 2019 г. он опубликовал программный документ о будущем Европы⁴³⁸, в котором, среди прочего, предложил создать общеевропейское агентство для защиты европейской демократии и борьбы с фейковыми новостями⁴³⁹.

Германия

Германия значительно отстаёт от своих соседей в институционализации системы информационного противостояния России, отчасти это происходит из-за изначального отставания в государственном регулировании информационной политики. Деятельность немецких средств массовой информации и социальных сетей основывается на конституционном положении о свободе слова, предусматривающем свободное выражение оценочных суждений и сообщения положенных в их основу фактов, если они являются правдивыми. При этом вплоть до 2017 г. реальные правовые ограничения на свободу слова накладывались только общими законами, как то уголовным преследованием за клевету, за оскорбление или распространение идей, унижающих человеческое достоинство. Специфический Закон о СМИ, обязывающий их представителей соблюдать журналистские стандарты и проверять публикуемые данные, не предусматривал никаких санкций за нарушение этих обязанностей, кроме публичных выговоров Совета по прессе. Хост-провайдеры, как правило, не несли ответственности за ложную информацию, опубликованную третьими сторонами на их платформах, если они не знают о нарушении прав, и они были обязаны немедленно удалить контент сразу по получении уведомления о его

Bloomberg. 8 декабря 2018. URL: <https://www.bloomberg.com/news/articles/2018-12-08/pro-russia-social-media-takes-aim-at-macron-as-yellow-vests-rage> (дата обращения: 11.11.2020)

⁴³⁸ Macron E. For European renewal / E. Macron // Elisee.fr. 4 March 2019. URL: <https://www.elysee.fr/emmanuel-macron/2019/03/04/for-european-renewal.en> (дата обращения: 11.11.2020)

⁴³⁹ Macron issues plea for Europe ahead of EU elections // DW. 04.03.2019. URL: <https://www.dw.com/en/macron-issues-plea-for-europe-ahead-of-eu-elections/a-47769832-0> (дата обращения: 11.11.2020)

незаконности, однако на практике регулярно игнорировали уведомления, в то время как санкций за это не было предусмотрено⁴⁴⁰.

Положение дел изменилось после публикации в декабре 2016 г. отчёта Службы парламентских исследований Бундестага о борьбе с распространением дезинформации («фейковыми новостями»)⁴⁴¹, совпавшего по времени с обсуждением распространения дезинформации во время предвыборной кампании США в 2016 г. в «Фейсбуке» и других социальных сетях.

В 2017 г. в Германии был принят Закон о защите сети, принявший во внимание недостаточность добровольных обязательств соцсетей по борьбе с разжиганием ненависти и фальшивыми новостями в социальных сетях⁴⁴². Закон обязывает указанные социальные сети удалять «явно незаконный» контент в течение двадцати четырех часов после получения жалобы пользователя. Если незаконность содержания неочевидна, у социальной сети есть семь дней на дополнительное изучение случая, а в особых случаях (недостаточность фактов для проверки информации, наём стороннего агентства для выполнения проверки) срок может быть и дольше. Для определения незаконности действия Закон отсылается на Уголовный кодекс, в частности, на положения о распространении пропагандистских материалов или использовании символов неконституционных организаций, о поощрении совершения серьёзного насильственного преступления, создающего угрозу государству, о разжигании ненависти и клеветы, среди прочего. Кроме того, платформы соцсетей обязаны предлагать пользователям простой и прозрачный механизм подачи жалоб и

⁴⁴⁰ Здесь и далее изложение особенностей законодательного регулирования информационного пространства Германии опирается на Gesley J. Government Responses to Disinformation on Social Media Platforms: Germany / J. Gesley // Government Responses to Disinformation on Social Media Platforms. Report for Congress. September 2019. P. 82-91. URL: <https://www.loc.gov/law/help/social-media-disinformation/social-media-disinformation.pdf> (дата обращения: 11.11.2020)

⁴⁴¹ Der Umgang mit Fake-News. Rechtslage und Reformansatz. // Deutscher Bundestag. Wissenschaftliche Dienste. Report No. WD 10 - 3000 - 067/16 (Dec. 20, 2016). URL: <https://www.bundestag.de/resource/blob/494418/4321d229204080dce488ebd0356b5db2/wd-10-067-16-pdf-data.pdf> (дата обращения: 11.11.2020)

⁴⁴² Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerkdurchsetzungsgesetz] // Bundesgesetzblatt. Teil I Nr. 61. Sept. 1, 2017. URL: https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&toctf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F%5B%40node_id%3D%27634128%27%5D&skin=pdf&tlevel=-2&nohist=1 (дата обращения: 11.11.2020)

получения ответа и раз в полгода публиковать на немецком языке двухгодичные отчёты определённого формата о рассмотрении жалоб, если их число превышает 100 в течение календарного года. Социальная сеть, которая намеренно или по неосторожности нарушает некоторые из вышеупомянутых обязательств, может быть оштрафована Федеральным управлением юстиции Германии на сумму до 50 миллионов евро. Если Федеральное управление юстиции хочет оштрафовать компанию за то, что оно считает контент, который не был удален, незаконным, оно должно сначала получить решение суда на этот счет. Таким образом, Закон о защите прав в сети не создаёт принципиально новых обязанностей по удалению контента по сравнению с ранее существовавшими добровольными обязанностями, но конкретизирует порядок их выполнения и налагает штрафы, если компании, работающие в социальных сетях, не соблюдают существующие обязанности.

В числе прочих мер следует отметить несколько кампаний⁴⁴³, запущенных и профинансированных Федеральным Правительством Германии для повышения медиакомпетентности в немецком обществе в целях борьбы с разжиганием ненависти, кибермоббингом и дезинформацией, а также планируемый в настоящее время пересмотр Межземельного договора о радиовещании, который введёт обязанность медиа-посредников, таких как платформы социальных сетей, выявлять социальных ботов, которые публикуют информацию в Интернете, с целью повышения прозрачности, а также обяжет электронные СМИ чётко идентифицировать человека, который публикует политическую, идеологическую или религиозную рекламу.

Резюмируя путь, пройденный Германией в рассматриваемом вопросе, можно сделать вывод, что конструирование системы противодействия «российской информационной угрозе» ещё не завершено, а созданные в стране

⁴⁴³ Подробнее см. Gesley J. Government Responses to Disinformation on Social Media Platforms: Germany / J. Gesley // Government Responses to Disinformation on Social Media Platforms. Report for Congress. September 2019. P. 82-91. URL: <https://www.loc.gov/law/help/social-media-disinformation/social-media-disinformation.pdf> (дата обращения: 11.11.2020)

правовые рамки контроля за состоянием информационного пространства, по крайней мере, на формальном уровне сохраняют элементы объективности.

Малые и средние страны Европы

В республиках *Балтии* уже сформированные механизмы информационной борьбы дополнялись некоторыми новыми инструментами в соответствии с текущей политической повесткой дня. При этом поддерживался необходимый информационный фон якобы постоянно продолжающихся информационных атак со стороны России и огромной угрозы, исходящей от них. Например, 6 октября 2018 г. латвийское агентство сообщило, что латвийская социальная сеть *Draugiem.lv* подверглась кибератаке в день выборов в Парламент страны⁴⁴⁴. 5 февраля 2019 г. в Литве опубликовали доклад спецслужб, согласно которому Москва пытается «повлиять на выборы», а также задействует против Литвы «самые продвинутые киберинструменты, которые нельзя выявить с помощью обычных систем кибербезопасности»⁴⁴⁵. Похожий доклад 14 марта 2019 г. подготовили эстонские спецслужбы, сделавшие упор на задействование Россией неправительственных участников в преступной киберактивности и на сборе ФСБ информации об иностранных гражданах⁴⁴⁶.

С другой стороны, предпринимались практические меры по подавлению нарративов, отличных от западного мейнстрима. Так, 21 декабря 2018 г. компания *Facebook* объявила о намерении открыть в латвийской столице отделение, которое будет заниматься модерацией публикаций пользователей социальной сети, на языках стран Балтии, а также на русском языке⁴⁴⁷.

31 августа 2017 г. Министры обороны *Дании* и *Швеции* выпустили совместное заявление о готовности совместно вести сопротивление российской

⁴⁴⁴ Латвийская соцсеть подверглась кибератаке в день выборов в парламент страны // ТАСС. 6 октября 2018. URL: <https://tass.ru/mezhdunarodnaya-panorama/5645523> (дата обращения: 11.11.2020)

⁴⁴⁵ Россия – "главная угроза": в Литве опубликовали доклад спецслужб // Sputnik. 2 февраля 2019. URL: <https://lt.sputniknews.ru/politics/20190205/8264040/Rossiia--glavnaya-ugroza-v-Litve-opublikovali-doklad-spetssluzhb.html> (дата обращения: 11.11.2020)

⁴⁴⁶ International Security and Estonia 2019 // Estonian Foreign Intelligence Service Report. Tallinn, 2019. 72 p. URL: <https://www.valisluureamet.ee/pdf/raport-2019-ENG-web.pdf> (дата обращения: 11.11.2020)

⁴⁴⁷ Facebook открывает офис в Риге, где модераторы будут искать язык ненависти на русском // Страна.ua. 21 декабря 2018. URL: <https://strana.ua/news/177824-facebook-otkryvaet-ofis-v-rihe-hde-moderatory-budut-iskat-jazyk-nenavisti-na-russkom.html> (дата обращения: 11.11.2020)

«гибридной войне», в частности, борьбу с «фейковыми новостями», которые якобы представляли опасность для обеих стран⁴⁴⁸. В феврале 2018 г. шведский Премьер-министр заявил, что его страна не потерпит российского вмешательства в сентябрьские выборы⁴⁴⁹. Соответственно, к сентябрю Швеция разработала стратегию сопротивления возможному российскому вмешательству⁴⁵⁰, включавшую, помимо укрепления киберсил, создание Межведомственного координационного форума для планирования, подготовки и защиты выборов, подготовку участников выборов к противостоянию информационному влиянию, сотрудничество основных СМИ в борьбе с фейковыми новостями, обучение студентов и журналистов работе с источниками информации, развития умений по проверке фактов⁴⁵¹.

7 декабря 2017 г. **Польша** собрала экспертов из четырёх стран Вышеградской группы (V4) на конференцию под названием «Борьба с дезинформацией в V4» с задачей подключить к информационной войне, помимо государственных учреждений, гражданское общество: имелось в виду активное вовлечение НКО и журналистов в пропагандистскую деятельность под видом «борьбы с дезинформацией».⁴⁵² Отмечался положительный опыт **Чехии**, создавшей при своём МВД первое подразделение, занимающееся борьбой с

⁴⁴⁸ Chalfant M. Denmark, Sweden team up to counter Russian 'fake news' / M. Chalfant // The Hill. 31 August 2017. URL: <https://thehill.com/policy/cybersecurity/348693-denmark-sweden-team-up-to-counter-russian-fake-news> (дата обращения: 11.11.2020); Denmark And Sweden: "Russian Fake News Is A Danger To Our Countries" // EUvsDisInfo. 1 September 2017. URL: <https://euvsdisinfo.eu/denmark-and-sweden-russian-fake-news-is-a-danger-to-our-countries/> (дата обращения: 11.11.2020)

⁴⁴⁹ Birnbaum M. Sweden is taking on Russian meddling ahead of fall elections. The White House might take note / M. Birnbaum // The Washington Post. 22 February 2018. URL: https://www.washingtonpost.com/world/europe/sweden-looks-at-russias-electoral-interference-in-the-us-and-takes-steps-not-to-be-another-victim/2018/02/21/9e58ee48-0768-11e8-aa61-f3391373867e_story.html (дата обращения: 11.11.2020)

⁴⁵⁰ Cederberg G. Catching Swedish Phish How Sweden is Protecting its 2018 Elections / G. Cederberg // Belfer Center for Science and International Affairs Report. August 2018. URL: <https://www.belfercenter.org/publication/catching-swedish-phish-how-sweden-protecting-its-2018-elections> (дата обращения: 11.11.2020)

⁴⁵¹ Taylor M. L. Combating disinformation and foreign interference in democracies: Lessons from Europe / M. L. Taylor // Brookings Cybersecurity and Election Interference Series. 31 July 2019. URL: <https://www.brookings.edu/blog/techtank/2019/07/31/combating-disinformation-and-foreign-interference-in-democracies-lessons-from-europe/> (дата обращения: 11.11.2020)

⁴⁵² Вендик Ю. Польша: всем странам ЕС нужно бороться с российской пропагандой / Ю. Вендик // BBC News. Русская служба. 12 декабря 2017. URL: <https://www.bbc.com/russian/features-42316849> (дата обращения: 11.11.2020); Крылов А. В борьбе с «российской пропагандой» Европа становится жертвой собственных СМИ / А. Крылов // Взгляд. 13 декабря 2017. URL: <https://vz.ru/politics/2017/12/13/899464.html> (дата обращения: 11.11.2020)

дезинформацией⁴⁵³. Развивая свою передовую роль, 13 декабря 2018 г. Чехия обвинила российские спецслужбы в причастности к двум кибератакам на МИД страны⁴⁵⁴.

4 октября 2018 г. свой вклад в борьбу с «российскими шпионами» и «российской киберпреступностью» внесли *Нидерланды*. Они заявили, что в апреле депортировали четверых сотрудников ГРУ, заподозренных в организации кибератаки на штаб-квартиру ОЗХО 13 апреля 2018 г.: последние якобы установили начинённый электронной шпионской аппаратурой автомобиль и пытались получить доступ к беспроводной сети ОЗХО в тот момент, когда там анализировались образцы яда, которым были предположительно отравлены Сергей и Юлия Скрипали, а также образцы химического оружия, якобы применённого в сирийской Думе. В связи с этим Премьер-министр Нидерландов Марк Рютте сделал совместное заявление с британским лидером Терезой Мэй с решительным осуждением действий ГРУ⁴⁵⁵. И уже 14 октября Министр обороны Нидерландов Анк Бейлевельд заявила, что её страна ведёт кибервойну с Россией⁴⁵⁶. Аналогичные процессы происходили в *Швейцарии*, в которой 24 октября 2018 г. задержали двух граждан РФ по подозрению в планировании хакерской атаки на лабораторию Всемирного антидопингового агентства (WADA) в Лозанне⁴⁵⁷.

Украина начала полномасштабную информационную войну весной 2014 г., заблокировав российские телеканалы и запустив антироссийскую пропаганду, которую вела по всем возможным каналам (включая соцсети), а с 1 мая 2017 г. заблокировала на своей территории ещё ряд российских соцсетей и сайтов. Тем

⁴⁵³ Centre Against Terrorism and Hybrid Threats // Czech Republic Ministry of Interior Affairs. URL: <https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx> (дата обращения: 11.11.2020)

⁴⁵⁴ Чехия обвинила Россию в кибератаках на МИД // Коммерсант. 3.12.2018. URL: <https://www.kommersant.ru/doc/3819587> (дата обращения: 11.11.2020)

⁴⁵⁵ Joint statement from Prime Minister May and Prime Minister Rutte // UK Government. 4 October 2018. URL: <https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte> (дата обращения: 11.11.2020)

⁴⁵⁶ Министр обороны Нидерландов заявила о кибервойне с Россией // Газета.ру. 14 октября 2018. URL: <https://www.gazeta.ru/army/news/2018/10/14/12167533.shtml> (дата обращения: 11.11.2020)

⁴⁵⁷ В Швейцарии задержали двух российских хакеров за попытку атаки на лабораторию WADA // Страна.ua. 24 октября 2018. URL: <https://strana.ua/news/167771-v-shveitsarii-zaderzhali-dvukh-hrazhdan-rf-po-podozreniju-v-planirovanii-khakerskoj-ataki-na-laboratoriju-wada.html> (дата обращения: 11.11.2020)

самым, к середине 2017 г. Украина задействовала, наверное, весь спектр государственных инструментов информационной войны своими силами, и дальнейшие внутривластные инициативы касались, скорее, юридического оформления фактического положения: в частности, вносились законопроекты о противодействии «государству-агрессору в информационном пространстве»⁴⁵⁸, изменялись правила блокировки сайтов и др. Накопленный опыт активно предлагался для использования другими странами. Например, Украина инициировала обсуждение российской пропаганды и «фейковых новостей» 9 мая 2018 г. в штаб-квартире ООН в Нью-Йорке. К обсуждению привлекались участники украинских НГО *StopFake.org* и *VoxUkraine*. Лейтмотивом собрания было утверждение, что *«пропаганда и фейки – это элементы гибридной войны России против Украины и других стран мира»*, в противостоянии «агрессии» Украина *«накопила немалый опыт и разработала инструменты для борьбы с российской пропагандой и фейковыми новостями»*⁴⁵⁹, поэтому её пример должны учитывать остальные страны. В этом же ряду стоит выступление украинского представителя Олега Николенко в Четвёртом комитете Генеральной Ассамблеи ООН по вопросам, связанным с информационной безопасностью, состоявшееся 10 октября 2018 г. В нём описывалась *«начатая Россией массированная пропагандистская кампания, разжигающая ненависть к Украине и украинцам»*⁴⁶⁰, и якобы преследования Россией журналистов; дипломат призвал активнее противостоять России.

Таким образом, главным итогом данного периода стало формирование первичных национальных механизмов борьбы с «российской информационной угрозой» крупными государствами Западной Европы, которые до этого ограничивались лишь дискурсивной поддержкой мер, предпринимаемых на

⁴⁵⁸ В Раду внесли законопроект о противодействии "государству-агрессору в информпространстве" // Страна.ua. 7 сентября 2018. URL: <https://strana.ua/news/160019-v-rade-zarehistrovan-zakonoproekt-o-protivodejstviu-hosudarstvu-ahressoru-na-tv-.html> (дата обращения: 11.11.2020)

⁴⁵⁹ ООН призывают усерднее бороться с кремлевской пропагандой // Ліга.Новости. 10.05.2018. URL: <https://news.liga.net/politics/news/oon-prizvali-prilozit-usiliya-k-borbe-s-rossiyskoy-propagandoy> (дата обращения: 11.11.2020)

⁴⁶⁰ Делегаты Генеральной Ассамблеи: развивая цифровые медиа, не надо забывать о традиционных СМИ // Новости ООН. 20 октября 2018. URL: <https://news.un.org/ru/story/2018/10/1341102> (дата обращения: 11.11.2020)

уровне международных организаций. Однако и на этом этапе предпринятые европейскими государствами шаги существенно отличались: если в Великобритании резонанс от «дела Скрипалей» дал повод Правительству перейти к созданию специальных гражданских и военных структур для противодействия «российской дезинформации», то во Франции и Германии данный процесс свёлся пока что только к принятию законодательных актов по ужесточению контроля над информационной сферой и соцсетями со стороны национальных регуляторов.

3.3. Эволюция институциональных механизмов информационного противодействия России на уровне западных межгосударственных объединений

НАТО

Деятельность структур НАТО в рамках системы противодействия «российской информационной угрозе» в указанный период продолжила траекторию, заложенную в 2014-2016 гг., и развивалась преимущественно в русле формирования и совершенствования инфраструктуры по отражению «гибридных угроз». Этот процесс происходил на нескольких направлениях: создания новых органов по борьбе с «гибридными угрозами» на военном и политическом уровнях, дальнейшей формализации союзнических обязательств в этой области, инкорпорации «гибридных угроз» в доктринальный аппарат и разрабатываемые кризисные сценарии, отработки отражения «гибридных угроз» в ходе проводимых Альянсом военных учений, проведения исследований и регулярного издания публикаций с разбором отдельных, в том числе информационных, аспектов «гибридных войн».

В институциональном отношении интегрирование сферы «гибридных угроз» в военную и политическую структуры НАТО происходило путём формирования небольших самостоятельных подразделений, призванных выработать холистическое видение текущего стратегического ландшафта и объединить в единой картине традиционные и «гибридные» угрозы. Так, в июле

2017 г. в Объединенном управлении разведки и безопасности НАТО был создан отдел гибридного анализа (Hybrid Analysis Branch), которому поручено анализировать весь спектр гибридных действий на основе военных, гражданских, закрытых и открытых источников⁴⁶¹. 8 ноября 2017 г. Генеральный секретарь НАТО Й. Столтенберг провёл брифинг по итогам встречи Министров обороны членов Альянса, в котором сообщил, что НАТО создаёт новый Центр киберопераций в рамках адаптации структуры командования НАТО, киберпланирование и операции НАТО будут интегрированы на всех уровнях, как и потенциал союзников в этой сфере. В то же время, командование киберсилами, предоставляемыми союзниками, предполагалось оставить в руках предоставивших их государств⁴⁶².

На Брюссельском саммите НАТО 11-12 июля 2018 г. значительное внимание было уделено вопросу совершенствования механизмов защиты союзников от «гибридных угроз». В итоговой декларации саммита содержались положения об усилении обязательств как в сфере киберобороны (п. 20):

«Киберзащита является частью основной задачи НАТО по обеспечению коллективной обороны. Мы должны уметь действовать в кибернетическом пространстве так же эффективно, как и в воздухе, на суше и на море, чтобы укрепить потенциал сдерживания и обороны Североатлантического союза. В связи с этим, мы продолжаем преобразование кибернетического пространства в сферу операций. Мы согласовали, каким образом интегрировать внутренние действия государств, осуществляемые странами НАТО в киберпространстве, на

⁴⁶¹ фон Лорингховен А. Ф. Адаптация разведки Североатлантического союза в поддержку «Единой НАТО» / А. Ф. фон Лорингховен // NATO Review. 8 сентября 2017. URL: <https://www.nato.int/docu/review/ru/articles/2017/09/08/adaptatsiya-razvedki-severoatlanticheskogo-soyuza-v-podderyoku-edinoj-nato/index.html> (дата обращения: 11.11.2020)

⁴⁶² Moore D. Why We Are Unconvinced NATO's Cyber Policy Is More Aggressive, and That's a Good Thing / D. Moore // Council on Foreign Relations Blog. 6 February 2018. URL: <https://www.cfr.org/blog/why-we-are-unconvinced-natos-cyber-policy-more-aggressive-and-thats-good-thing> (дата обращения: 11.11.2020) ; Ricks Th. NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons / Th. Ricks // Foreign Policy. 7 December 2017. URL: <https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/> (дата обращения: 11.11.2020); O'Neill P. H. NATO will establish new cyber command centers / P. H. O'Neill // Cyberscoop. 9 November 2017. URL: <https://www.cyberscoop.com/nato-cyber-command-centers/> (дата обращения: 11.11.2020)

добровольной основе, в контекст операций и миссий Североатлантического союза в рамках строгого политического надзора. Подтверждая оборонительный мандат НАТО, мы полны решимости использовать весь свой потенциал, в том числе в кибернетической сфере, чтобы обеспечивать сдерживание и оборону и противодействовать всему спектру кибернетических угроз, в частности осуществляемых в рамках гибридной кампании».

так и в сфере борьбы с «гибридными угрозами» (п. 21):

«Наши страны сталкиваются со всё более серьёзными вызовами со стороны как государственных, так и негосударственных субъектов, которые используют гибридные действия, порождающие неопределённость и стирающие грани между миром, кризисом и конфликтом. Хотя основная обязанность по реагированию на гибридные угрозы возложена на подвергшееся им государство, НАТО готова, по решению Совета, оказать содействие любому государству НАТО на любом этапе гибридной кампании. В случае гибридной войны Североатлантический совет мог бы принять решение о приведении в действие статьи 5 Вашингтонского договора, как и в случае вооружённого нападения. Мы укрепляем свою устойчивость, улучшаем осведомленность об обстановке и усиливаем наше построение сдерживания и обороны. Мы также расширяем набор располагаемых нами инструментов по противодействию враждебным гибридным действиям. Мы объявляем о создании групп поддержки по борьбе с гибридными действиями, которые предоставляют адресную, целевую поддержку государствам НАТО, по их запросу, в обеспечении готовности и реагировании на гибридные действия»⁴⁶³.

⁴⁶³ Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года // НАТО. 11 июля 2018. URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 11.11.2020)

Концепция групп поддержки по борьбе с гибридными действиями как элемента помощи Альянсу государствам, подвергшимся «гибридным вызовам», предусматривала формирование небольших команд преимущественно гражданских экспертов в области стратегических коммуникаций, контрразведки, защиты критической инфраструктуры и т. п., способных оказать помощь национальным оборонным структурам в условиях кризиса. Подобный механизм позволяет формально выполнить союзнические обязательства, не задействуя весь аппарат интегрированного командования НАТО, как в случае полноценной активации гарантий ст. 5 Вашингтонского договора⁴⁶⁴.

Также с 2018 г. антикризисные учения НАТО стали включать отработку ответов на гибридные сценарии, включая дезинформационные кампании, угрозы критической инфраструктуре и пограничные ситуации кризисов низкой интенсивности⁴⁶⁵. Для обсуждения всего комплекса проблем безопасности в условиях «гибридных конфликтов» эта тематика была вынесена на политический уровень путём инициирования специальных форматов в рамках Североатлантического совета. Так, в мае 2019 г. прошла первая неформальная встреча на уровне советников по национальной безопасности и высших военных экспертов стран Альянса, где рассматривалась необходимость выработки всеобъемлющего подхода к отражению «гибридных вызовов»⁴⁶⁶.

Параллельно шла работа по укреплению взаимодействия НАТО с Европейским союзом в сфере противодействия «гибридным угрозам». Институциональный аспект этого взаимодействия обеспечивался не только благодаря сотрудничеству соответствующих подразделений обеих организаций, но и благодаря учреждению в апреле 2017 г. Европейского центра передового опыта по противодействию гибридным угрозам в Финляндии (*Hybrid CoE*),

⁴⁶⁴ Rühle M. NATO's Response to Hybrid Threats / M. Rühle // National Institute for Public Policy Information Series. 4 November 2019. Issue No. 448. P. 4. URL: <https://www.nipp.org/wp-content/uploads/2019/11/IS-448.pdf> (дата обращения: 11.11.2020)

⁴⁶⁵ Bajarūnas E. Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond / E. Bajarūnas // European View. 2020. Vol. 9 (1). P. 62-70. (66)

⁴⁶⁶ Rühle M. NATO's Response to Hybrid Threats / M. Rühle // National Institute for Public Policy Information Series. 4 November 2019. Issue No. 448. P. 4. URL: <https://www.nipp.org/wp-content/uploads/2019/11/IS-448.pdf> (дата обращения: 11.11.2020)

созданного, подобного рижскому и таллиннскому центрам, по решению девяти государств и наделённого постфактум соответствующими функциями в качестве «узлового» органа, организующего взаимодействие между НАТО, ЕС, национальными государствами и структурами гражданского общества в области отражения «гибридных угроз».

Каждые полгода Альянс выпускает отчёт о прогрессе в выполнении перечня совместных задач в сфере нейтрализации «гибридных угроз», утверждённого в декабре 2016 г., включая обмен разведданными, согласование планов наращивания потенциала, разработку сценариев и алгоритмов совместного реагирования на «гибридные угрозы», проведение так называемых Параллельных скоординированных учений (“PACЕ”) и регулярный формальный и неформальный диалог между политическими и военными органами НАТО и ЕС по данным вопросам⁴⁶⁷.

Значительно активизировалась публикационная и презентационная деятельность органов НАТО. Так, в феврале 2017 г. в издательстве *Cambridge University Press* вышло «Таллиннское руководство 2.0 по международному праву, применимому к кибероперациям»⁴⁶⁸, расширяющее аналогичное издание 2013 г. и содержащее, по сути, произвольные западные интерпретации правового регулирования киберпространства, представляемые как общепринятые и базовые для всего мирового сообщества. В 2017 г. рижский Центр стратегических коммуникаций запускает серию регулярных обзоров деятельности якобы связанных с РФ автоматизированных аккаунтов в соцсетях (так называемых ботов) “*Robotrolling*”. В первых же обзорах ботами были объявлены 60% русскоязычных аккаунтов в *Twitter* – это куда выше процента автоматизированных аккаунтов в англоязычном сегменте – 39%. Они якобы

⁴⁶⁷ Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 16 June 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf (дата обращения: 11.11.2020)

⁴⁶⁸ Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M. N. Schmitt (ed.). 2nd ed. Cambridge: Cambridge University Press, 2017. 598 p.

создали примерно 70% всех сообщений о НАТО в Прибалтике и Польше⁴⁶⁹. А в 2018 г. Центр начинает издавать академический журнал «Оборонительные стратегические коммуникации»⁴⁷⁰, придавая, тем самым, размещаемым на его сайте материалам статус академических работ. Знаковой также стала вышедшая в ноябре 2018 г. публикация Центра о противодействии правительствам злонамеренному использованию социальных сетей с рекомендациями, которые в обычной ситуации показались бы недемократическими: фактическая цензура, принуждение журналистов к публикации стандартного контента, инвестирование в оборону и безопасность, криминализация автоматического генерирования сообщений⁴⁷¹.

Ещё одним пунктом обвинения России в применении подрывных мер в отношении союзников и партнёров НАТО стали озвученные публично подозрения в создании электронных помех во время учений Альянса. Так, 10 ноября 2018 г. Финляндия заявила, что подозревает Россию в создании помех для сигнала GPS во время совместных с НАТО учений *Trident Juncture 2018* 6 ноября⁴⁷², а 13 ноября 2018 г. Минобороны Норвегии дополнило, что эти помехи были созданы российскими войсками⁴⁷³. Примечательно, что в авангард борьбы с российскими «гибридными угрозами» выводились такие нейтральные и не входящие в НАТО страны, как Финляндия и Швеция.

Немалую лепту в поддержание публичного резонанса вокруг тематики «российской информационной угрозы» в 2018 г. внесла Парламентская Ассамблея НАТО. 27 марта 2018 г. в комитете Гражданской безопасности Парламентской Ассамблеи НАТО был представлен доклад лорда Джоплинга

⁴⁶⁹ Robotrolling 2017/1. Report prepared by the NATO Strategic Communications Centre of Excellence. Riga, 2017. 6 p. URL: <https://www.stratcomcoe.org/robotrolling-20171> (дата обращения: 11.11.2020)

⁴⁷⁰ Academic journal “Defence Strategic Communications” // NATO Stratcom Centre of Excellence. URL: <https://www.stratcomcoe.org/academic-journal-defence-strategic-communications> (дата обращения: 11.11.2020)

⁴⁷¹ Bradshaw S. Government Responses to Malicious Use of Social Media / S. Bradshaw, L.-M. Neudert, Ph. N. Howard // NATO Stratcom CoE. Riga, November 2018. 20 p. URL: <https://www.stratcomcoe.org/government-responses-malicious-use-social-media> (дата обращения: 11.11.2020)

⁴⁷² Россию заподозрили в создании помех НАТО // Lenta.ru. 9 ноября 2018. URL: https://lenta.ru/news/2018/11/09/trident_juncture/ (дата обращения: 11.11.2020)

⁴⁷³ Россию официально обвинили во взломе системы GPS во время учений НАТО // Lenta.ru 13 ноября 2018. URL: https://lenta.ru/news/2018/11/13/gps_nato/ (дата обращения: 11.11.2020)

“Countering Russia’s Hybrid Threats: an Update”⁴⁷⁴, коротко повторяющий всю теорию «российской гибридной войны» и устрашающих перспектив натовского бездействия перед лицом нависшей угрозы. Ссылаясь на результаты американских исследователей, Джоплинг говорил, что русское вмешательство на американских выборах и российских наёмников в Сирии однозначно выдаёт единое дирижирование от приближённого к Президенту РФ В.В. Путину олигарха Е.В. Пригожина. В то же время, оценить результативность всего русского вмешательства на западную политику трудно: в большинстве случаев вмешательство России даже не может спровоцировать новые расколы в обществе или государствах, а только усиливают существующие. И даже если речь идёт о финансировании из российского банка или о кибератаках хакерских групп, базирующихся в России, сложно установить существование прямой связи их акций с Кремлём. 18 ноября 2018 г. в Парламентской ассамблее НАТО был заслушан доклад Сьюзан Девис⁴⁷⁵ о российском вмешательстве в выборы и референдумы на территории Альянса, а 19 ноября была принята Резолюция⁴⁷⁶ комитета Парламентской ассамблеи о новых ответах российским гибридным тактикам.

Европейский союз

Итоги президентских выборов в США и резонанс вокруг якобы имевшего место российского вмешательства придали новый, довольно мощный импульс развитию инфраструктуры борьбы с «российской информационной угрозой» в Европейском союзе. Оно происходило как по пути совершенствования уже сформированных к тому моменту форматов и механизмов, так и посредством инициирования новых. Приближение избирательных кампаний во многих

⁴⁷⁴ Lord Jopling. Countering Russia’s Hybrid Threats: an Update / Lord Jopling // Special report for the Committee on the Civil Dimension of Security NATO Parliamentary Assembly. 27 March 2018. URL: <https://www.nato-pa.int/document/2018-countering-russias-hybrid-threats-jopling-report-166-cds-18-e> (дата обращения: 11.11.2020)

⁴⁷⁵ Davis S. Russian Meddling in Elections and Referenda in the Alliance / S. Davis // Special report for Science and Technology Committee NATO Parliamentary Assembly. 18 November 2018. URL: <https://www.nato-pa.int/document/2018-russian-meddling-elections-and-referenda-alliance-davis-report-181-stc-18-e-fin> (дата обращения: 11.11.2020)

⁴⁷⁶ Resolution 445 - Updating the Responses to Russia’s Hybrid Tactics – CDS // NATO Parliamentary Assembly. 19 November 2018. URL: <https://www.nato-pa.int/document/resolution-445-updating-responses-russias-hybrid-tactics> (дата обращения: 11.11.2020)

европейских государствах и грядущие в 2019 г. выборы в Европарламент позволили антироссийским силам в ЕС вновь апеллировать к коммунитарным органам с призывами обеспечить защиту демократических институтов от «кремлёвской пропаганды» и ради этого конкретизировать выработанные доктринальные принципы борьбы с ней, переведя их в ранг прямых политических обязательств, и усилить нацеленные на эту борьбу механизмы.

На рассматриваемом этапе в структуре европейского компонента системы информационного противодействия России выделяются три ключевых самостоятельных направления: 1) предупреждение и нейтрализация вызовов в киберпространстве, 2) отражение «гибридных угроз» и борьба с дезинформацией и «фейковыми новостями», в рамках которой отдельное значение придаётся 3) регулированию социальных сетей. На каждом из этих направлений формировались самостоятельные политические рамки и практические механизмы регулирования, позволяющие ЕС и его органам осуществлять контроль за информационной сферой в автономном режиме, вне зависимости от позиции государств-членов ЕС. Благодаря этому степень коммунитаризации европейского информационного пространства и контроля над ним со стороны евроинтеграционных структур значительно возросла.

Кибербезопасность

В течение 2017 г. основные процессы в построении системы информационного противодействия ЕС разворачивались в отношении киберпространства, на которое Евросоюз, вслед за НАТО, постепенно распространял действие своих механизмов и гарантий безопасности.

В марте 2017 г. ЕСВД совместно с Еврокомиссией представила проект документа «Дипломатический ответ ЕС на зловредные кибердействия», который после обсуждения в Комитете по вопросам политики и безопасности ЕС был утверждён в июне того же года⁴⁷⁷. В нём было зафиксировано, что, отвечая на

⁴⁷⁷ Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") // General Secretariat of the Council. 7 June 2017. URL: <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> (дата обращения: 11.11.2020)

зловредные кибердействия, Евросоюз будет использовать весь комплекс средств в рамках Общей внешней политики и политики безопасности, включая, при необходимости, ограничительные меры, и давалось поручение ЕСВД и Еврокомиссии подготовить комплекс шагов по реализации данного положения, создать для этого необходимый потенциал и отработать оперативные практики. Для этих целей был запущен формат экспертного обсуждения дальнейших шагов на данном направлении: Европейский институт исследований безопасности (EUISS) в партнёрстве с Еврокомиссией учредил Целевую группу по созданию киберпотенциала из пяти экспертов⁴⁷⁸. В развитие данной инициативы 13 сентября 2017 г. Еврокомиссия подготовила сообщение для Европарламента и Совета ЕС «Соппротивление, сдерживание и защита: строительство сильной кибербезопасности ЕС»⁴⁷⁹, а 24 октября 2017 г. выступила с рядом инициатив в направлении укрепления кибербезопасности: оказать поддержку в поиске и преследовании киберпреступников за пределами Евросоюза, усилить санкции против третьих стран, позволяющих хакерам атаковать со своей территории, проще раскрывать данные о владельцах сайтов⁴⁸⁰.

11 октября 2017 г. Комитет по вопросам политики и безопасности утвердил подробное Руководство по имплементации июньского документа⁴⁸¹. В нём содержится перечень мер, которые могут быть использованы для предотвращения или реагирования на зловредные кибердействия, в том числе такие, которые не дотягивают до уровня нарушений международного права, но расцениваются как недружественные акты, независимо от того, исходят ли они от государства или негосударственного актора. В особо серьёзных случаях такие действия могут приравниваться к использованию силы или вооружённой атаке в

⁴⁷⁸ Cyber Capacity Building Task Force // EU ISS. 26 March 2018. URL: <https://www.iss.europa.eu/content/cyber-capacity-building-task-force-0> (дата обращения: 11.11.2020)

⁴⁷⁹ Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Joint Communication to the European Parliament and the Council // European Commission. 13 September 2017. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=en> (дата обращения: 11.11.2020)

⁴⁸⁰ Stupp C. EU plans aid to prosecute hackers and support member states / C. Stupp // EurActiv. 24 October 2017. URL: <https://www.euractiv.com/section/cybersecurity/news/eu-plans-aid-to-prosecute-hackers-and-support-member-states/> (дата обращения: 11.11.2020)

⁴⁸¹ Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities // General Secretariat of the Council. 9 October 2017. URL: <https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf> (дата обращения: 11.11.2020)

том смысле, в каком это подразумевается в Уставе ООН, и, соответственно, давать основания для государств-членов ЕС использовать своё право на индивидуальную и коллективную самооборону, включая задействования статьи 42 (7) Договора о Европейском союзе. Меры дипломатического реагирования ЕС, согласно данному Руководству, подразделяются на превентивные, кооперативные, стабилизационные, ограничительные и меры поддержки государств-членов со стороны ЕС. В Руководстве приведено подробное описание каждой группы мер, в том числе возможных решений коммунитарных органов и делегаций ЕС в третьих странах. Среди ограничительных мер упомянуты запрет на поездки для физических лиц, запрет на продажу оружия, заморозка счетов или иных экономических активов. Причём не все приведённые меры требуют однозначного установления источника кибератак.

В 2018 г. Европейский совет трижды в своих выводах касался вопросов кибербезопасности, в том числе, дав в октябре поручение подготовить список конкретных шагов по усилению потенциала ЕС в области киберобороны для выполнения положений документов, принятых в 2017 г. Это вылилось в принятие в мае 2019 г. юридически обязывающего решения Совета относительно ограничительных мер в случае кибератак, несущих угрозу Евросоюзу или его членам⁴⁸². В нём крайне чётко выписаны правовые рамки и процедуры реагирования на внешние кибератаки против государств-членов или Евросоюза в целом, причём среди критериев для квалификации подобных атак упомянут, среди прочего, ущерб критическим государственным функциям, в частности, в области обороны управления и функционирования институтов, включая публичные выборы и процесс голосования. Кроме того, допускается использование ответных мер в случае кибератаки против государства, не являющегося членом ЕС, или против другой международной организации. Согласно ст. 5 и 6 данного Решения, Европейский совет по представлению

⁴⁸² Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member State // Council of the European Union. 14 May 2019. URL: <https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf> (дата обращения: 11.11.2020)

Высокого представителя или государства-члена ЕС единогласно утверждает список лиц, ответственных за осуществлённые или планируемые кибератаки, вовлечённых в их организацию, оказывающих им сознательное содействие или ассоциируемых с ними, и замораживает все их активы. Для максимизации эффекта от подобных мер ЕС будет привлекать третьи страны к их принятию.

Нетрудно заметить, что описанный механизм во многом повторяет аналогичные санкционные механизмы американского законодательства, в частности, положения санкционного закона 2 августа 2017 г., и, фактически, предоставляет ЕС и его членам право произвольно накладывать экономические санкции на лица, причастные не только к реальным, но и предполагаемым кибератакам. Хотя требование единогласного принятия решений и отсутствие прямых санкций в отношении причастных к кибератакам государств несколько ограничивает возможности для использования данного механизма отдельными государства или институтами ЕС в политических целях, общая тенденция к выходу за рамки международного права и установлению собственных норм и инструментов регулирования киберпространства подтверждается на примере ЕС не в меньшей мере, чем на примере США.

«Гибридные угрозы»

В 2017 г. продвижение работы по выстраиванию механизма сдерживания и отражения «гибридных угроз» в Евросоюзе происходило в русле закрепления и наполнения содержанием уже принятых форматов, включая созданный в апреле Европейский центр передового опыта по противодействию гибридным угрозам (Hybrid CoE) в Хельсинки, а также развития концептуальных положений, прописанных в Глобальной стратегии 2016 г.

7 июня 2017 г. Еврокомиссия и Высокий представитель по внешней политике и политике безопасности направили Совместное сообщение Европарламенту и Совету «Стратегический подход к устойчивости во внешних

действиях»⁴⁸³, уточняющий ключевое для Глобальной стратегии понятие устойчивости (*resilience*) во внешней политике ЕС. В данном документе провозглашалась необходимость усилить устойчивость ЕС, в том числе, в сфере энергетической безопасности, отражения «гибридных угроз» и стратегических коммуникаций. Также говорилось, что внутренняя устойчивость ЕС является залогом успешной политики в отношении России с опорой на утверждённые в марте 2016 г. пять руководящих принципов и что обеспечение устойчивости требует широкого вовлечения в дела восточного соседства вплоть до Центральной Азии для гарантирования того, что и Евросоюз, и его партнёры свободны в своём политическом, дипломатическом и экономическом выборе, а степень внешнего воздействия или принуждения сведена к минимуму.

Утверждалось, что в рамках согласованных ЕС и НАТО мер по повышению устойчивости к «гибридным угрозам» ЕС продолжит работу по нескольким направлениям, в частности:

- в рамках противодействия «гибридным угрозам» усилит *«защиту критически важной инфраструктуры при одновременной диверсификации источников и поставщиков энергии и укреплении обороноспособности»* в рамках оперативного сотрудничества стран-членов с привлечением участников из разных секторов;

- в рамках обеспечения кибербезопасности реализует нормативную и оперативную повестку дня, включая продвижение своего видения в ООН;

- в рамках стратегической коммуникации ЕС примет меры *«по повышению устойчивости граждан к враждебной дезинформации... за счет повышения осведомлённости, поддержки большего плюрализма и профессионализма СМИ, а также распространения позитивных нарративов и сообщений, основанных на фактах. ЕС должен усилить ресурсы Оперативной группы East Stratcom и активизировать свое сотрудничество с институтами ЕС, государствами-*

⁴⁸³ A Strategic Approach to Resilience in the EU's external action. Joint Communication to the European Parliament and the Council // European Commission. 7 June 2017. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0021&from=en> (дата обращения: 11.11.2020)

членами и партнёрами-единомышленниками. Долгосрочный стратегический подход и охват стран Восточного партнёрства будут и далее развиваться с упором на обмены между людьми и на работу с существующими сетями гражданского общества, которые уже представляют собой источник устойчивости на уровне сообществ». Аналогичный подход предполагается распространить на Балканы, Турцию, а затем и страны арабского мира.

Таким образом, противодействие России в восточном соседстве, в том числе в плане нейтрализации «гибридных угроз», провозглашалось одним из ключевых условий обеспечения внешнеполитической устойчивости ЕС. Это усилило антироссийский уклон доктринальных и позиционных документов ЕС, чего удалось избежать в Глобальной стратегии 2016 г.

19 июля 2017 г. Еврокомиссия совместно с Высоким представителем выпустила отчёт о прогрессе в выполнении Общей рамочной программы противодействия «гибридным угрозам» 2016 г. В нём подчёркивались, среди прочего, такие достижения в данной сфере, как создание при Европейском совете группы экспертов «Друзья председательства», чьей задачей является выработка к концу общей схемы выявления и оценки «гибридных угроз» в странах-членах ЕС, образование Центра анализа гибридных угроз и издание им периодического «Гибридного бюллетеня» с анализом актуальных на данный момент «гибридных угроз» и вызовов, а также проведение Европейским оборонным агентством за указанный период трёх учений для отработки процедур реагирования в кризисных ситуациях по «гибридным» сценариям совместно с Еврокомиссией ЕСВД и государствами-членами, что позволило внести соответствующие коррективы в регулярный План развития оборонного потенциала ЕС.

В конце 2017 г. тематика дезинформации и «гибридных угроз» получила новый импульс благодаря эстонскому председательству в Совете ЕС и лоббистским усилиям ряда других государств-членов. Так, 2 октября 2017 г. Европейский институт исследований безопасности (EUISS) совместно с председательствующей Эстонией провели конференцию «Гибридные угрозы и

ЕС: состояние дел и прогноз на будущее»⁴⁸⁴, ориентированную на информационный аспект – кибербезопасность, стратегические коммуникации, борьбу с дезинформацией, радикализацией и экстремизмом.

Резонанс вокруг «дела Скрипалей» весной 2018 г. дал толчок новому витку обсуждения тематики «гибридных угроз» и необходимости усиления механизмов их нейтрализации в Евросоюзе. В выводах Европейского совета от 22 марта 2018 г. было сказано, что ЕС должен усилить свою устойчивость в отношении рисков использования биологического, радиологического и химического оружия, и с этой целью Евросоюз и его члены должны продолжать укреплять свой потенциал в отношении «гибридных угроз», в том числе в области кибербезопасности, стратегических коммуникаций и контрразведки. Европейский совет призвал Еврокомиссию и Высокого представителя активизировать работу на этом направлении и представить отчёт о прогрессе на июньском саммите⁴⁸⁵.

На выполнение этого поручения 13 июня 2018 г. Еврокомиссия совместно с Высоким представителем обнародовали два новых документа по данной тематике – новый годовой отчёт о прогрессе Общей рамочной программы⁴⁸⁶ и сообщение «Повышение устойчивости и укрепление потенциала для борьбы с гибридными угрозами»⁴⁸⁷, призванное дополнить программу.

В отчёте отмечалось, что группа «Друзей председательства» запустила в конце 2017 г. опрос среди государств-членов по выработанной ею общей схеме для определения текущих уязвимостей к «гибридным угрозам». На основании полученных данных председательствующая в Совете страна представит сводный

⁴⁸⁴ Hybrid threats and the EU. State of play and future progress // EU ISS Conference Report. 2-3 October 2017. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/EE_hybrid_event_report.pdf (дата обращения: 11.11.2020)

⁴⁸⁵ European Council meeting (22 March 2018) – Conclusions // General Secretariat of the Council. 23 March 2018. URL: <https://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf> (дата обращения: 11.11.2020)

⁴⁸⁶ Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018 // European Commission. 13 June 2018. URL: https://eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf (дата обращения: 11.11.2020)

⁴⁸⁷ Increasing resilience and bolstering capabilities to address hybrid threats. Joint Communication to the European Parliament, the European Council and the Council // European Commission. 13 June 2018. URL: https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf (дата обращения: 11.11.2020)

доклад. Также предлагалось продлить истекающий в 2018 г. мандат данной группы до 2020 г. с учётом стоящих перед ЕС масштабных задач в данной сфере. Особых успехов достиг, согласно отчёту, Центр анализа гибридных угроз, установивший связь с 26 национальными контактными пунктами, созданными государствами-членами для координации усилий в области отражения «гибридных угроз». Кроме того, данная сеть была дополнена налаживанием регулярных обменов между Еврокомиссией и ЕСВД, которые ежемесячно проводят встречи для обсуждения конкретных тематических вопросов в рамках проблематики «гибридных угроз». Таким образом, в Евросоюзе по указанию отдельных коммунитарных органов, императивным путём была создана система органов по борьбе с «гибридными угрозами» на национальном уровне, систематически контролируемая и направляемая соответствующими структурами Евросоюза.

Отдельное внимание в отчёте уделено вопросу применения закреплённых в ЕС механизмов солидарности и взаимопомощи к «гибридным» сценариям и возможному взаимодействию в этом вопросе с гарантиями коллективной обороны в рамках НАТО. Проработка этой темы на уровне исследований и обсуждений между государствами-участниками поручена Европейскому центру передового опыта в Хельсинки. Также в консультации с хельсинкским Центром проводится работа по определению возможного военного вклада ЕС в противодействие «гибридным угрозам» в рамках Общей внешней политики и политики обороны. По сути, Евросоюз шёл параллельными путями с НАТО, постепенно вводя «гибридные угрозы» в диапазон потенциальных объектов применения существующих гарантий безопасности и военных инструментов.

В сообщении «Повышение устойчивости...» кратко повторялась общая проблематика «гибридных угроз» и излагались задачи по их отражению на кратко- и среднесрочную перспективу. В нём не содержалось принципиально новых положений. По сравнению с предыдущими документами, в данном сообщении было уделено особое внимание возможным рискам использования биологического, радиологического и химического оружия, для их изучения

предлагалось создать специализированные аналитические ячейки в Центре анализа гибридных угроз, а Комиссии и Высокому представителю поручалось финализировать работу над оценкой масштаба «гибридных угроз» в различных секторах общественной жизни. Кроме того, ЕСВД и Еврокомиссии было предписано разработать и внедрить практические меры для укрепления способности ЕС и его членов противостоять враждебной активности иностранных спецслужб, в особенности направленной против демократических институтов. С этой целью предлагалось также ввести в состав Центра анализа гибридных угроз экспертов по контрразведывательной работе для отслеживания и информирования о специфике вероятной враждебной деятельности спецслужб в отношении физических лиц и институтов ЕС.

Очевидно, что данный документ лишь отвечал на сформированный в СМИ конъюнктурный политический запрос и представлял дополнение к Общей рамочной программе противодействия «гибридным угрозам».

Приближение выборов в Европарламент стало поводом для формулирования нового перечня мер для сдерживания потенциальных угроз избирательному процессу. Так, 12 сентября 2018 г. главой Еврокомиссии Жан-Клодом Юнкером были сформулированы рекомендации по обеспечению *«свободных и справедливых европейских выборов»*. Например, государствам-членам рекомендовалось *«создать национальную сеть сотрудничества в области выборов с соответствующими органами, такими как избирательные органы, кибербезопасность, защита данных и правоохранные органы, и назначить контактный пункт для участия в сети сотрудничества по выборам европейского уровня»*, предлагалось *«раскрывать информацию о том, какая партия или группа политической поддержки стоит за политической рекламой в Интернете»*, активнее применять законы о защите данных в свете скандала с компанией *Cambridge Analytica*, защищать сети и информационные системы от угроз кибербезопасности в согласовании с Агентством по кибербезопасности ЕС

и Еврокомиссией, ужесточить правила финансирования европейских политических партий⁴⁸⁸.

В мае 2019 г. был обнародован очередной годовой отчёт о прогрессе в выполнении Общей рамочной программы и сообщения «Повышение устойчивости...»⁴⁸⁹ с довольно обширной систематизацией предпринятых за прошедший период шагов. Главным из них является завершение процесса оценки существующих уязвимостей и представление соответствующего доклада болгарским председательством в начале 2019 г. По итогам данного отчёта в июле было принято решение придать группе «Друзей председательства» постоянный статус, утвердив её в качестве Постоянной рабочей группы по усилению устойчивости и противодействию «гибридным угрозам» при Европейском совете⁴⁹⁰.

Одним из результатов её работы стало принятие в декабре 2019 г. специальных выводов о Дополнительных усилиях в сфере усиления устойчивости и противодействия «гибридным угрозам»⁴⁹¹, в которых идёт речь о необходимости выработки всеобъемлющего подхода к данной проблематике, охватывающего все области правительственной политики. В содержательном отношении выводы не представляют особой оригинальности, перечисляя преимущественно уже прописанные в более ранних документах меры, однако примечательно, что благодаря институционализации подобной структуры при высшем политическом органе ЕС внимание к тематике «гибридных угроз» привлекается значительно активнее, без потребности в предварительном лоббировании со стороны заинтересованных антироссийских акторов.

⁴⁸⁸ State of the Union 2018: European Commission proposes measures for securing free and fair European elections // European Commission. 12 September 2018. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5681 (дата обращения: 11.11.2020)

⁴⁸⁹ Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats // European Commission. 28 May 2019. URL: https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilience.pdf (дата обращения: 11.11.2020)

⁴⁹⁰ Bajarūnas E. Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond / E. Bajarūnas // European View. 2020. Vol. 9 (1). P. 65.

⁴⁹¹ Complementary efforts to enhance resilience and counter hybrid threats - Council Conclusions (10 December 2019) // General Secretariat of the Council. 10 December 2019. URL: <https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf> (дата обращения: 11.11.2020)

Дезинформация

В течение двух с половиной лет после своего образования основную часть работы по противодействию дезинформации в Евросоюзе выполняла Оперативная рабочая группа по стратегическим коммуникациям *East Stratcom*. Она обеспечивала регулярную и весьма впечатляющую статистику выявленных фактов «российской дезинформации», которая фиксировалась в отчётах и выступлениях высших европейских чиновников. К примеру, выступая на организованной эстонским председательством конференции по гибридным угрозам в октябре 2017 г. Федерика Могерини выступила с заявлением о промежуточных результатах работы группы *East StratCom*:

*«Нам важно анализировать, прогнозировать и реагировать на дезинформацию. По этой причине мы создали в рамках Европейской службы внешних действий первую оперативную рабочую группу по стратегическим коммуникациям, сосредоточив внимание на восточных партнерах и русскоязычных общинах. За последние два года группа East StratCom выявила более 3000 случаев дезинформации»*⁴⁹².

12 сентября 2017 г. группа *East StratCom* запустила новый проект – трёхязычный (английский, русский, немецкий) сайт «Евросоюз против дезинформации» www.euvsdisinfo.eu, направленный «на решение проблемы прокремлевской дезинформации»⁴⁹³. На сайте были представлены как оригинальные материалы, так и перепечатки экспертных и публицистических работ представителей других организаций, что придавало им видимость поддержки со стороны ключевого европейского органа по противодействию дезинформации⁴⁹⁴. Некоторые работы были опубликованы непосредственно от имени Оперативной группы. Например, в январе 2017 г. вышла заметка с

⁴⁹² Контрпропагандистская группа ЕС выявила за два года свыше 3 тыс. случаев дезинформации от русскоязычных СМИ – Могерини // Интерфакс-Украина. 2 октября 2017. URL: <https://interfax.com.ua/news/general/452361.html> (дата обращения: 11.11.2020)

⁴⁹³ Гальперович Д. Европа создала новый веб-сервис по разоблачению российской пропаганды / Д. Гальперович // Голос Америки. 14 сентября 2017. URL: <https://www.golos-ameriki.ru/a/eu-fights-disinformation-from-russia/4027827.html> (дата обращения: 11.11.2020)

⁴⁹⁴ Подробнее о наполнении сайта EUvsDisInfo см. нашу статью Царик В.С. Борьба с "российской дезинформацией" в публичном позиционировании западных институтов: анализ официальных сайтов НАТО и европейского союза // Среднерусский вестник общественных наук. 2019. Том 14, Номер 6. С. 109-125.

описанием общего контекста работы группы⁴⁹⁵, воспроизводившая широко растиражированные на тот момент штампы и подававшая их как объективные факты, а именно что российская информационная стратегия, направленная на то, чтобы «ослабить и дестабилизировать Запад», использует не только крупные СМИ вроде *RT* и *Sputnik*, но также маргинальные ресурсы – блоги и соцсети. Доказательством эффективности «российской дезинформации» авторы посчитали такие факты, как поддержка третью немцев ослабления антироссийских санкций, признание половиной французов вины Киева в конфликте на Донбассе, недоверие к США и НАТО, проявившееся в ходе опроса в Чехии, Словакии и Венгрии. Таким образом, гипотеза о независимом формировании общественного недоверия к официальной линии в странах Запада авторами доклада даже не проверялась.

Именно с расширением работы *East StratCom* и распространением её опыта на другие сопредельные регионы (Западные Балканы и Ближний Восток) долгое время связывались дальнейшие планы по усилению борьбы с дезинформацией в Евросоюзе. 26 ноября 2017 г. ЕС принял решение выделить группе *East StratCom* финансирование в размере 1,1 млн. евро в год непосредственно из бюджета Евросоюза. Глава Европейского совета Дональд Туск при этом заявил, что для противодействия «кибератакам, фейковым новостям, гибридной войне» в ЕС должны «сохранять осторожность и бдительность и быть честными. Если мы хотим защитить себя, если мы хотим помочь нашим партнёрам, мы должны чётко осознавать присутствие угрозы внутри ЕС»⁴⁹⁶.

Однако для наиболее активных сторонников жёстких мер противодействия «кремлёвской пропаганде» этих усилий было явно недостаточно. С разных сторон в адрес коммунитарных органов направлялись инициативы, призывающие к расширению инфраструктуры борьбы с дезинформацией и

⁴⁹⁵ Commentary: Means, Goals and Consequences of the Pro-Kremlin Disinformation Campaign // EUvsDisInfo. 19 January 2017. URL: <https://euvsdisinfo.eu/commentary-means-goals-and-consequences-of-the-pro-kremlin-disinformation-campaign/> (дата обращения: 11.11.2020)

⁴⁹⁶ Пудовкин Е. Евросоюз борется с "российским влиянием". Британский министр поднимет тему пропаганды социальных сетей в ходе визита в Москву / Е. Пудовкин // Независимая газета. 27 ноября 2017. URL: http://www.ng.ru/world/2017-11-27/6_7123_eurosouz.html (дата обращения: 11.11.2020)

подключению к ней ресурсов Еврокомиссии. Так, 30 марта 2017 г. Европейская народная партия на своём съезде на Мальте приняла резолюцию «Русская дезинформация, подрывающая западную демократию»⁴⁹⁷. А в октябре 2017 г. Министры иностранных дел Хорватии, Чехии, Латвии, Литвы, Польши, Румынии, Швеции и Великобритании в письме к Могерини выразили озабоченность якобы *«более изощрённым и интенсивным, чем когда-либо»* распространением дезинформации со стороны «внешних субъектов», призванным *«вызвать недоверие и недовольство демократическим порядком и дискредитировать ЕС, партнёров по ЕС, а также ослабить европейское единство»*⁴⁹⁸, и предложили дальнейшее усиление стратегической коммуникации ЕС, в том числе, в направлении Западных Балкан.

В ответ на подобные воззвания Еврокомиссия запустила процесс более тщательного экспертного изучения данной проблематики с целью выработать новые меры контроля на этом направлении, не ограниченные сугубо мониторингом и документацией фактов дезинформации, а способные эффективно противостоять их распространению.

15 января 2018 г. впервые собралась группа экспертов высокого уровня по поддельным новостям и онлайн-дезинформации из 39 назначенных Еврокомиссией экспертов по фейкам. Ей была поставлена задача описать феномен и предоставить Еврокомиссии рекомендации по обращению с ним⁴⁹⁹.

17 января 2018 г. член этой комиссии, Еврокомиссар по союзу безопасности сэр Джулиан Кинг выступил на слушаниях в Европарламенте по поводу влияния пропаганды РФ на страны ЕС. Он воспроизвёл тезис об опаснейшей дезинформационной стратегии Кремля, состоящей в распространении одних и тех же дезинформационных мессиджей сразу по многим каналам и на многих

⁴⁹⁷ Russian disinformation undermining Western democracy // Resolution adopted at the European People's Party Congress, St. Julian's (Malta), 29 – 30 March 2017. URL: <https://www.epp.eu/papers/russian-disinformation-undermining-western-democracy/> (дата обращения: 11.11.2020)

⁴⁹⁸ Maksimovic M. EU officials warn of 'underestimating' Russian propaganda in Balkans / M. Maksimovic // Deutsche Welle. 14 November 2017. URL: <https://www.dw.com/en/eu-officials-warn-of-underestimating-russian-propaganda-in-balkans/a-41371020> (дата обращения: 11.11.2020)

⁴⁹⁹ Candau M. MEPs bare teeth in debate over Russian propaganda / M. Candau // EurActiv. 23 January 2018. URL: <https://www.euractiv.com/section/justice-home-affairs/news/meps-bear-teeth-in-debate-over-russian-propaganda/> (дата обращения: 11.11.2020)

языках (всего комиссия выявила 3500 примеров *«прокремлёвской дезинформации, противоречащей общедоступным фактам»*), в результате, согласно опросам общественного мнения, слишком много людей верят прокремлёвскому нарративу. В его выступлении присутствовало утверждение, перекочевавшее из западной интерпретации несуществующей «доктрины Герасимова»: *«В официальной военной доктрине России, а также в заявлениях ведущих российских генералов они описывают использование ложных данных и дестабилизирующую пропаганду в качестве законных инструментов, а информацию – в качестве другого типа вооружённых сил»*. Кинг отчитался об огромной работе по анализу и опровержению контента российских СМИ, «повышению медиаграмотности» и подготовке журналистов, продвижению «качественных СМИ».

Всего два месяца спустя 12 марта 2018 г. был представлен заключительный отчёт собранной в марте группы экспертов по фейкам. Группа дала самое широкое определение дезинформации как любой формы ложной, неточной или вводящей в заблуждение информации, предназначенной, представленной и продвигаемой для преднамеренного причинения общественного вреда или получения прибыли, но не включили в неё те виды нелегального контента (как то клевета, подстрекательство к насилию), которые и так регулируются законодательством ЕС или регламентируются на национальном уровне. Такое определение позволяет отнести к дезинформации любую немейнстримную точку зрения, поэтому применить определение к «российской пропаганде» уже не составляло труда. Для «борьбы с дезинформацией» группа тоже предложила стандартный подход, облечённый в эвфемистические формулировки:

1. *«повысить прозрачность онлайн-новостей, включая адекватный и конфиденциальный обмен данными о системах, которые обеспечивают их распространение в Интернете;*

2. *продвигать медиа- и информационную грамотность, чтобы противостоять дезинформации и помогать пользователям ориентироваться в среде цифровых медиа;*

3. разработать инструменты, позволяющие пользователям и журналистам бороться с дезинформацией и содействовать позитивному взаимодействию с быстро развивающимися информационными технологиями;

4. сохранять разнообразие и устойчивость европейской экосистемы новостных СМИ, и

5. содействовать постоянным исследованиям влияния дезинформации в Европе, чтобы оценить меры, принимаемые различными участниками, и постоянно корректировать необходимые ответные меры»⁵⁰⁰.

Нетрудно понять, что за этим списком кроется отслеживание российской пропаганды и российских информационных сетей, их разоблачение и приоритезация собственной пропаганды и своих информационных сетей, «правильные» фабрики контента, склонение журналистов и блогеров на свою сторону, сохранение подконтрольности европейских СМИ, принуждение европейской системы к конфронтации с российским нарративом.

На основе доклада группы экспертов и широких консультаций с общественностью было разработано Сообщение Еврокомиссии «Борьба с онлайн-дезинформацией: европейский подход», размещённое на её сайте 26 апреля 2018 г.⁵⁰¹.

Подготовленные Еврокомиссией документы были одобрены Европейским советом в заключении от 26 июня 2018 г., где, в частности, содержалось предложение «Высокому представителю и Комиссии представить в сотрудничестве с государствами-членами и в соответствии с выводами Европейского совета в марте 2015 года план действий к декабрю 2018 года с конкретными предложениями по скоординированному реагированию ЕС на проблему дезинформации, включая соответствующие мандаты и достаточные

⁵⁰⁰ Final report of the High Level Expert Group on Fake News and Online Disinformation // European Commission. 12 March 2018. URL: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation> (дата обращения: 11.11.2020)

⁵⁰¹ Tackling online disinformation: a European Approach. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions // EUR-Lex. 26 April 2018. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236> (дата обращения: 11.11.2020)

ресурсы для соответствующих команд ЕСВД по стратегическим коммуникациям». В заявлении также было уделено внимание проблеме предупреждения и атрибуции кибератак, углублению сотрудничества ЕС и НАТО на ниве информационной войны, а также высказана поддержка «намерению Еврокомиссии представить законодательное предложение по улучшению обнаружения и удаления контента, разжигающего ненависть»⁵⁰².

26 сентября 2018 г. на сайте Еврокомиссии был опубликован Кодекс практических правил по дезинформации⁵⁰³, выработанный представителями онлайн-платформ, ведущих социальных сетей, рекламодателей и рекламной индустрии для самостоятельной борьбы с распространением онлайн-дезинформации и поддельных новостей. 18 октября 2018 г. Европейский совет поддержал рекомендации Еврокомиссии в своём заключении: «Переговоры по предложению о механизме гражданской защиты ЕС должны быть завершены к концу года»⁵⁰⁴.

Очередной план действий⁵⁰⁵ в этом направлении был подготовлен рядом комиссаров ЕС, включая сэра Джулиана Кинга, к 5 декабря 2018 г. он включал «улучшенное обнаружение» дезинформации специально созданными целевыми группами, финансирование которых предполагалось увеличить, постоянную координацию между общеевропейским и национальным уровнями, чёткое соблюдение принятого в сентябре 2018 г. Кодекса практических правил по дезинформации, наблюдение за результатами работы системы и её корректировку.

⁵⁰² European Council meeting (28 June 2018) – Conclusions // European Council. 28 June 2018. URL: <https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final/> (дата обращения: 11.11.2020)

⁵⁰³ EU Code of Practice on Disinformation // European Commission. 28 September 2018. URL: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> (дата обращения: 11.11.2020)

⁵⁰⁴ European Council meeting (18 October 2018) – Conclusions // General Secretariat of the Council. 18 October 2018. URL: <https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conclusions/> (дата обращения: 11.11.2020)

⁵⁰⁵ Action Plan against Disinformation. Joint Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions // European Commission. 5 December 2018. URL: https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf (дата обращения: 11.11.2020)

План Дж. Кинга был рассмотрен и одобрен на саммите Европейского совета 13-14 декабря 2018 г. В выводах саммита говорилось, что распространение намеренной, масштабной и систематической дезинформации как составляющей «гибридной войны» является острым вызовом для европейских демократий, требующим немедленного ответа при полном уважении фундаментальных прав человека. Вследствие этого Совет подчёркивает необходимость дать слаженный ответ на этот вызов, объединяющий внутреннее и внешнее измерение, и для этого скорейшим образом выполнить положения плана Кинга, в том числе, путём подключения частного сектора и экспертизы⁵⁰⁶.

Тут же началось привлечение к полноценной информационной войне на стороне ЕС американских соцсетей. 28 декабря 2018 г. Еврокомиссия обвинила *Facebook*, *Twitter* и *Google* в бездействии по сопротивлению фейкам, в невыполнении «добровольного» Кодекса практических правил, подписанного в сентябре. Так, эти компании несвоевременно размещали данные об использовании своих рекламных мощностей, недостаточно активно удаляли «фейковые» учётные записи и др. После этих заявлений председатель либеральной группы Европарламента Ги Верхофстадт выступил с новым заявлением об угрозе «нормальному порядку предстоящих европейских выборов» из-за недостаточного регулирования соцсетей, а сэр Джулиан Кинг пояснил, что усиление регулирования возможно, а пока Еврокомиссия даёт американским платформам шанс «проявить себя»⁵⁰⁷.

Официальное заявление с требованием к «Фейсбуку» и «Твиттеру» «усилить меры по борьбе с дезинформацией» Еврокомиссия сделала 28 января 2019 г. Отметив прогресс в закрытии фейковых аккаунтов, Еврокомиссия потребовала полного раскрытия данных обо всех политических объявлениях («прозрачности политической рекламы»). Еврокомиссия пригрозила наложить

⁵⁰⁶ European Council meeting (13 and 14 December 2018) – Conclusions // General Secretariat of the Council. 14 December 2018. URL: <https://www.consilium.europa.eu/media/37535/14-euco-final-conclusions-en.pdf> (дата обращения: 11.11.2020)

⁵⁰⁷ Stolton S. EU raps Facebook, Twitter and Google for inaction on fake news / S. Stolton // EurActiv. 1 March 2019. URL: <https://www.euractiv.com/section/digital/news/eu-wraps-facebook-twitter-and-google-for-inaction-on-fake-news/> (дата обращения: 11.11.2020)

более серьёзное регулирование на онлайн-платформы, если по итогам комплексной оценки результаты их самостоятельных усилий к сентябрю 2019 г. окажутся неудовлетворительными⁵⁰⁸.

14 июня 2019 г. Еврокомиссия подготовила для Европарламента и Европейского совета Отчёт о выполнении Плана действий против дезинформации. Отметив немалый прогресс в выполнении плана, особенно со стороны социальных сетей, составители доклада отметили их недостаточную активность в объяснении своим пользователям, что удаление аккаунтов способствует укреплению демократии, а также поставили новые задачи:

«Несмотря на достижения, предстоит ещё многое сделать: все онлайн-платформы должны предоставлять более подробную информацию, позволяющую выявлять злостных субъектов и целевые государства-члены. Им также следует активизировать сотрудничество с проверщиками фактов и предоставить пользователям возможность лучше обнаруживать дезинформацию. Наконец, платформы должны предоставлять исследовательскому сообществу осмысленный доступ к данным в соответствии с правилами защиты личных данных. В связи с этим недавняя инициатива Twitter, направленная на выпуск соответствующих наборов данных для исследовательских целей, открывает возможности для проведения независимых исследований по предпринятым злоумышленниками операциям дезинформации. Кроме того, Комиссия призывает платформы применять свою политику прозрачности политической рекламы к предстоящим национальным выборам»⁵⁰⁹.

Кодекс правил и соответствующий План действий сформировали новый механизм контроля за дезинформацией, дополнивший действующий формат

⁵⁰⁸ Code of Practice against disinformation: Commission calls on signatories to intensify their efforts. Presse release // European Commission. 29 January 2019. URL: http://europa.eu/rapid/press-release_IP-19-746_en.htm (дата обращения: 11.11.2020); Stolton S. EU Commission hits out at Facebook's disinformation report / S. Stolton // EurActiv. 30 January 2019. URL: <https://www.euractiv.com/section/data-protection/news/facebook-singled-out-in-eu-disinformation-report/> (дата обращения: 11.11.2020)

⁵⁰⁹ Report on the implementation of the Action Plan Against Disinformation. Joint Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions // EUR-Lex. 14 June 2019. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:JOIN_2019_0012_FIN (дата обращения: 11.11.2020)

East StratCom и основанный на так называемом адаптивном подходе с приоритетом самостоятельного регулирования и удаления нежелательного контента средствами массовой информации и администрациями социальных сетей, повышения сознательности и медиаграмотности общества, его готовности самостоятельно отсекают ложную и деструктивную информацию. Этот подход противопоставляется так называемому патерналистскому подходу, предполагающему императивное ограничение распространения нежелательной информации государственными органами⁵¹⁰. Российские исследователи полагают⁵¹¹, что Еврокомиссия воплощает в своей работе первый подход, тогда как Оперативная группа *East StratCom* – второй. Однако на практике оба подхода применялись в работе *East StratCom* и других международных структур параллельно. Повышение медиаграмотности и общественной сознательности в вопросе выявления дезинформации фигурировало в качестве приоритета работы на данном направлении начиная с 2014 г. На каждой стадии развития системы противодействия российскому информационному влиянию маркировка нежелательной информации и её источников запускала процесс её ограничения либо путём императивного запрета, либо путём оказания давления на публичные площадки, требуя от них самостоятельно ограничивать подобную информацию под угрозой прямых или косвенных санкций. Новаторство механизма, сформированного Еврокомиссией в 2018 г., заключалось в формулировании чётких политических обязательств в этой сфере, обозначении критериев их выполнения и формировании инструментов контроля за «добровольным» удалением нежелательного контента администрациями соцсетей. В этом плане данный механизм является на текущий момент наиболее формализованным, что даёт основания говорить о ведущей роли Европейского союза в практическом измерении системы информационного противодействия России.

⁵¹⁰ Романова Т. А. Дезинформация (фейковые новости, пропаганда) как угроза стрессоустойчивости: подходы на уровне Евросоюза и Литвы как его члена / Т.А. Романова, Н. И. Соколов, Ю. Ю. Колотаев // Балтийский регион. 2020. Т. 12, № 1. С. 53—67.

⁵¹¹ Там же.

Тем не менее, лоббистские усилия антироссийских сил этим механизмом не ограничились. Любой резонансный медиаповод, независимо от степени достоверности и доказанности, используется для педалирования необходимости усилить борьбу с подрывными действиями России и её агентов в информационной среде. Так, 4 октября 2018 г. Премьер-министр Нидерландов Марк Рютте заявил о возможных санкциях в отношении России из-за скандала с якобы попыткой российских разведчиков осуществить кибератаку на штаб-квартиру ОЗХО⁵¹².

Для придания нового импульса этому процессу к нему вновь после двухлетнего перерыва, подключили Европарламент. 13 марта 2019 г. им была принята очередная резолюция, где РФ названа главным источником дезинформации в Европе наряду с Китаем, Ираном и Северной Кореей, *«которые стремятся подорвать основы и принципы европейских демократий, а также суверенитет всех стран Восточного партнёрства»*. Европарламент призвал преобразовать группу *East Stratcom Task Force* в полноценную структуру в рамках ЕСВД, отрегулировать деятельность соцсетей, курьерских служб и поставщиков соцсетей законодательством (а не просто добровольным Кодексом), установить привлечение к ответственности компаний, которые не могут быстро удалять фейковые новости, предоставить властям возможность выявлять авторов и спонсоров представленного политического контента⁵¹³.

Таким образом, в период 2017-2019 гг. европейский компонент западной системы противодействия «российской информационной угрозе» значительно укрепился за счёт усиления существующих органов в структуре ЕСВД – Оперативной группы *East Stratcom* и Центра анализа гибридных угроз – и создания новых – Европейского центра передового опыта по противодействию «гибридным угрозам» и Постоянной рабочей группы по усилению устойчивости

⁵¹² В ЕС задумались о новых санкциях из-за российских кибератак // Lenta.ru. 5 октября 2018. URL: <https://lenta.ru/news/2018/10/05/hacker/> (дата обращения: 11.11.2020)

⁵¹³ Follow up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties // European Parliament. 13 March 2019. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0187_EN.pdf?redirect (дата обращения: 11.11.2020)

и противодействию «гибридным угрозам» при Европейском совете, а также благодаря значительной активизации участия Еврокомиссии в процессе формализации механизма контроля за распространением дезинформации, во многом усилиями Еврокомиссара по союзу безопасности сэра Джулиана Кинга. Формирование подобных структур и механизмов позволило регуляризировать дискурсивные и практические меры по противодействию «российской пропаганде», сделав их неотъемлемым элементом политической и стратегической повестки дня Евросоюза.

Выводы по главе 3

1. Итог президентских выборов в США 2016 г. и резонанс вокруг предполагаемого российского вмешательства дали новый толчок процессу выстраивания инфраструктуры подавления «российской информационной угрозы», позволив представить эту угрозу как направленную против безопасности и стабильности Запада в целом, а не только русскоязычного пространства или стран Восточной Европы. Вследствие этих событий информационная составляющая концепта «гибридной войны» в рассматриваемый период была выведена на первый план как несущая наибольшую опасность западным государствам и институтам и требующая немедленных масштабных мер для её нейтрализации. Это создало основания для инициирования и утверждения на международном и национальном уровнях комплекса более жёстких мер по информационному противодействию России, включая введение адресных санкций за организацию кибератак и попытки вмешательства в избирательный процесс. В 2017 г. подобные меры были формализованы и закреплены на нормативно-правовом уровне, а в 2018 г., на фоне нового всплеска резонанса вокруг данной тематики под влиянием «дела Скрипалей», начинается их активное применение наряду с усилением контроля за информационной сферой и социальными сетями.

2. В США главными движущими силами кампании стали отдельные разведывательные, силовые и правоохранительные структуры, присоединившиеся к уже сформированному симбиозу антироссийски настроенных представителей законодательной власти, экспертной среды и СМИ. Они провели публичное расследование «российского вмешательства» и вынесли на повестку дня вопрос о необходимости «наказания» России за него, прежде всего, через санкционные механизмы в информационной сфере и законодательное закрепление наложенных на Россию санкций без возможности их снятия решением Президента.

Политико-дипломатические институциональные механизмы реагирования на «российскую информационную угрозу» в США формировались медленно, под влиянием медийной и политической конъюнктуры. Пик наибольшей активности на данном направлении пришёлся на середину 2018 г. и наблюдался на фоне медийного резонанса от «дела Скрипалей». Активизация специального созданного для противодействия иностранной пропаганде Центра глобального взаимодействия в рамках Госдепартамента произошла только в конце 2018 – начале 2019 гг. и существенно отставала от аналогичных механизмов в Европейском союзе. Наряду с этим, информационная сфера подверглась значительной милитаризации на доктринальном и институциональном уровнях, будучи интегрирована в компетенцию военного ведомства в рамках его полномочий в области кибербезопасности и отражения киберугроз. На законодательном уровне были прописаны широкие полномочия и обязанности Пентагона в отношении проведения военных информационных операций, в том числе превентивных, скрытых и не достигающих порога прямых боевых действий. Причём были сняты действовавшие ранее ограничения, связанные с необходимостью межведомственной координации таких операций, а сами они были юридически приравнены к традиционным военным действиям, не требующим особых процедур согласования на уровне политического руководства страны. При этом в утверждённых в 2018 г. киберстратегиях

были сформулированы расширительные трактовки объекта вероятных киберугроз и круга инструментов, которые могут быть применены для их нейтрализации.

3. В становлении инфраструктуры борьбы с «российской информационной угрозой» в рассматриваемый период особую роль играла Великобритания. Несмотря на то, что в британском государственном аппарате степень институционализации функций, связанных с информационным противодействием России, оставалась не самой высокой, официальный Лондон выступил в роли активного генератора дискурса об исходящих от России «гибридных угрозах» на международной арене, принял наиболее жёсткие ограничительные меры в отношении российских СМИ, а его представители участвовали и осуществляли руководство многими международными структурами, созданными для борьбы с «российской пропагандой». Кроме того, заметная часть работы по насаждению антироссийских нарративов и лоббированию антироссийских инициатив в Европе осуществлялась через проекты *Integrity Initiative* – якобы независимой сети кластеров «гражданского общества», курируемой британскими службами и финансируемой структурами британского МИД.
4. Ключевой тенденцией в развитии системы подавления «российской информационной угрозы» на уровне национальных государств в данный период стало законодательное оформление нормативной базы контроля за информационным пространством, СМИ и социальными сетями с обязательствами последних удалять нежелательные материалы, квалифицированные как дезинформация, и возможностями государственного контроля за их удалением.
5. Североатлантический альянс, как и прежде, выступал основой структуры, задающей доктринальный вектор развития системы информационного противодействия России, продвигаясь в данный период по пути дальнейшей милитаризации информационной сферы и инкорпорации «гибридных угроз» в свой военно-стратегический аппарат. Для подкрепления политических

обязательств о возможности задействования гарантий безопасности НАТО для отражения «гибридных атак» в структуре Альянса были образованы уже не просто аффилированные центры, а стационарные подразделения, осуществляющие мониторинг, планирование операций и подготовку потенциала для задействования в случае «гибридных сценариев» конфликтов.

Также Альянс продолжил играть направляющую роль в формировании повестки дня в области «гибридных угроз» для Европейского союза, в том числе с помощью образованного для этих целей Европейского центра передового опыта в Финляндии.

6. На рассматриваемом этапе в структуре европейского компонента системы информационного противодействия России выделяются три ключевых самостоятельных направления: 1) предупреждение и нейтрализация вызовов в киберпространстве, 2) отражение «гибридных угроз» и 3) борьба с дезинформацией и «фейковыми новостями», в рамках которой отдельное значение придаётся регулированию социальных сетей. В сфере кибербезопасности в Евросоюзе постепенно оформляется инструментарий реагирования на реальные или планируемые кибератаки извне с возможностью применения ограничительных мер, включая адресные экономические санкции против причастных лиц, по американскому примеру. В области отражения «гибридных угроз» продолжилась работа по закреплению данной сферы в политико-стратегическом и доктринальном аппарате ЕС и формированию институциональной инфраструктуры её обеспечения на коммунитарном и национальном уровнях. Основным её результатом стало составление подробного перечня «гибридных угроз» и уязвимостей государств-членов и анализ необходимого для их устранения потенциала. Вслед за НАТО, Евросоюз также пошёл по пути распространения на сферу «гибридных угроз» своих гарантий безопасности и имеющихся военно-политических средств их обеспечения. В области борьбы с «дезинформацией» вследствие активного подключения

Еврокомиссии был достигнут значительный прогресс в виде формирования отдельного механизма регулирования «дезинформации» со специально прописанными критериями и принципами, а также ответственностью СМИ и соцсетей за удаление нежелательного «пропагандистского» контента.

Благодаря подобным мерам были сформированы политические рамки и практические механизмы регулирования, позволяющие Евросоюзу и его органам осуществлять контроль за информационной сферой в автономном режиме, вне зависимости от позиции государств-членов ЕС. Ввиду этого, можно констатировать, что Европейский союз с его разветвлённой сетью бюрократических процедур и инструментов взял на себя ведущую роль в осуществлении практической работы по информационному противодействию России на регулярной основе.

Заключение

В результате проведённого исследования диссертантом были сформулированы следующие выводы:

1. После окончания «холодной войны» потенциал России в области так называемой «мягкой силы» и невоенных средств влияния оценивался на Западе как незначительный, однако волна «цветных революций» на постсоветском пространстве в середине 2000-х годов заставила руководство РФ активизировать усилия по укреплению авторитета и поддержки со стороны общественности сопредельных стран. Эти усилия выставлялись антироссийски настроенными политическими силами на Западе в качестве вызова демократическим преобразованиям и государственности соседних стран, что дало толчок процессу формирования представления о «российской информационной угрозе».

В период 2007-2013 гг. на Западе с опорой на предвзятую интерпретацию инцидентов вокруг Эстонии и Грузии были сформированы основные контуры представления о «российской информационной угрозе» как целенаправленного использования российским руководством кибератак, пропаганды, симпатий русских общин за рубежом и других информационных средств влияния для достижения политических и военно-стратегических целей в ущерб интересам и безопасности западных государств. Это дало толчок дискуссиям о необходимости выработки механизмов защиты от подобных вызовов, в том числе, на уровне НАТО. Однако до 2014 г. данной угрозе придавалось весьма ограниченное, преимущественно тактическое значение как возможного дополнительного средства воздействия России в ходе конфликтов и кризисов на постсоветском пространстве, а не как ключевого вызова всему либеральному миропорядку. Причём эффективность этого средства оценивалась западными исследователями, в целом, довольно объективно, с признанием того, что даже эстонский и грузинский инциденты принесли российскому руководству довольно сомнительные политические результаты.

2. Концептуальной основой системы противодействия «российской информационной угрозе» после украинского кризиса стал дискурс о «гибридной войне» России против Запада. Он был сформулирован весной 2014 г. рядом военных экспертов и представителей аналитических структур стран Балтии, Польши, Великобритании, Украины для консолидации западного сообщества вокруг идеи помощи новому украинскому руководству в противостоянии с Россией, а главной движущей силой его продвижения выступили структуры НАТО. Данный дискурс основывался на ряде искусственно сконструированных (или откровенно сфабрикованных) представлений о внешней политике России, якобы доказывающих наличие у её руководства агрессивных замыслов в отношении Запада и планов по его дестабилизации задолго до украинского кризиса. В новом политическом контексте концепт «гибридной войны» был использован для объединения в единое целое конвенциональных, иррегулярных, экономических и информационных средств ведения войны и международной конкуренции и для приписывания России роли инициатора в использовании подобных средств для реализации военно-политических целей. Он прочно вошёл в западный академический и политический лексикон и выполняет в нём ряд важных функций по конструированию и поддержанию политической конфронтации с Россией, криминализации реальных или предполагаемых действий РФ на международной арене и обоснованию права Запада на жёсткую реакцию в ответ на любые действия, трактуемые как проявления «гибридной войны». Кроме того, концепт «гибридной войны» позволяет придать текущей конфронтации характер, не ограниченный традиционным межгосударственным военно-политическим противостоянием, охватывающий практически все сферы общественной жизни и предполагающий задействование широкого круга средств и акторов, не имеющих прямой связи с российским государством.

3. Одним из центральных компонентов концепта «гибридной войны» является представление о «российской информационной угрозе» как комбинации кибернетических, сетевых, информационно-психологических, пропагандистских, дезинформационных, медийных, коммуникативных и иных

методов воздействия на общественные процессы западных и других стран, способствующее поддержанию гипертрофированного образа России как врага западного сообщества, обладающего превосходством в современных высокотехнологичных и инновационных инструментах противостояния, в которых у Запада якобы сохраняется критическое отставание или уязвимость. В ходе конструирования «российской информационной угрозы» в западной академической и политической среде было сформировано представление о «российской пропаганде» как целостном самостоятельном феномене, к которому отнесён и атрибутирован как сугубо российский по своему происхождению и источникам тиражирования целый класс применяемых западными структурами приёмов, манипуляций и методов деструктивного воздействия на общество, а также ряд возникших и бытующих в западном политическом пространстве месседжей, нарративов и идеологем, противоречащих идеологическому мейнстриму. Конечным итогом конструирования «российской информационной угрозы» является делегитимация внешней и внутренней политики России как полноправного субъекта международных отношений, имеющего право отстаивать собственную позицию и преследовать национальные интересы, в том числе, с помощью возможностей «мягкой силы» и публичной дипломатии. Беспрецедентность и тотальный характер якобы ведущейся Россией «гибридной войны» против Запада и всего либерального порядка оправдывают аналогично тотальные меры по отражению данной «угрозы».

4. Период 2014-2016 гг. стал начальным этапом построения системы противодействия «российской информационной угрозы» на Западе, в ходе которого генерируемый номинально независимыми экспертами дискурс был довольно быстро поддержан сначала правительствами отдельных европейских государств, а затем и структурами НАТО. Давление со стороны обеих упомянутых групп акторов привело к постепенному подключению Европейского союза к процессу создания институциональной инфраструктуры для борьбы с «российской информационной угрозой». При том, что после украинского кризиса значимость и деструктивный потенциал данной угрозы в восприятии

западного политического класса резко возросли, формирование институциональной инфраструктуры для её нейтрализации происходило в ориентации на её ограниченный масштаб: она воспринималась как непосредственно затрагивающая только русскоязычное пространство и страны с многочисленным русским населением.

При этом институциональное закрепление механизмов противодействия «российской информационной угрозе» со стороны западных межгосударственных объединений имело свои особенности.

Так, выступив в качестве локомотива в дискурсивном признании и утверждении якобы исходящих от России «гибридных угроз» безопасности Запада летом-осенью 2014 г., Североатлантический альянс пошёл по пути частичной институционализации в своей структуре функций, связанных с отражением данных угроз, в том числе в их информационной составляющей. С одной стороны, для противодействия «российской информационной угрозе» были задействованы уже существующие органы – открытый в 2008 г. Центр по сотрудничеству в сфере киберобороны в Таллине и открытый в 2014 г. Центр передового опыта в области стратегических коммуникаций в Риге. Оба центра были созданы по решению отдельных государств-членов НАТО и имеют статус военных органов вне интегрированного командования, утверждённый уже после их создания. Параллельно высшие чиновники НАТО в рассматриваемый период прикладывали основные усилия к тому, чтобы стимулировать Европейский союз взять на себя ведущую ответственность за отражение «гибридных угроз» и, тем самым, вовлечь его в организацию сдерживания и противодействия России в информационной и других невоенных сферах.

При этом Альянс включил киберпространство и «гибридные угрозы» в сферу своей оперативной ответственности с возможностью задействования гарантий статьи 5 Вашингтонского договора в ответ на «гибридные атаки» против его участников.

Включение Евросоюза в систему противодействия «российской информационной угрозе» происходило постепенно, начиная с весны 2015 г., под

влиянием немалого публичного давления со стороны некоторых государств-членов, НАТО и ряда негосударственных аналитических организаций и «мозговых центров». Работа по определению функций ЕС в рамках данной системы и закреплению их в институциональной структуре Евросоюза проводилась на двух направлениях – реагирования на вызов «российской пропаганды и дезинформации» для политики ЕС в восточном соседстве и создания потенциала для отражения «гибридных угроз» в целом. На первом направлении институционализация произошла довольно быстро, путём формирования летом 2015 г. Оперативной рабочей группы по стратегическим коммуникациям *East Stratcom* в рамках Европейской службы внешних действий, однако задачи данной группы формально были ограничены выявлением «российской дезинформации» в русскоязычном информационном пространстве. На втором направлении Евросоюз значительно продвинулся по пути признания актуальности информационных и «гибридных» угроз, однако на уровне базовых позиционных документов, принятых в рассматриваемый период (в первую очередь Глобальной стратегии ЕС 2016 г.), прямая увязка этих угроз с Россией была ослаблена. Тем не менее, эти документы институционализировали механизм информационного противостояния, создавая дополнительные каналы влияния и аргументационную базу для антироссийских сил, заинтересованных в поддержании конфронтации Запада с Россией в информационной сфере.

Из всех коммунитарных органов Европейского союза наиболее активную роль в продвижении дискурса о «российской информационной угрозе» после украинского кризиса сыграл Европарламент, выступавший основной площадкой для вынесения данной тематики на уровень европейского публичного пространства и политической повестки дня ЕС. Наиболее значимый практический эффект в плане доктринального и институционального закрепления данного дискурса на уровне ЕС произвела Европейская служба внешних действий, функционеры которой в сжатые сроки подготовили доклады и планы действий касательно организации работы по противодействию «российской пропаганде» и отражению «гибридных угроз». Наименьшую

активность в деле усиления конфронтации с Россией в информационной сфере на начальном этапе проявила Еврокомиссия.

Борьба с «российской пропагандой и дезинформацией» в НАТО и Европейском союзе, согласно официальным заявлениям их высших функционеров, была организована не вокруг императивных ограничительных мер или ведения ответной контрпропаганды, а вокруг выявления фактов и источников распространения подобной «дезинформации», их своевременного опровержения, повышения «сознательности» самих СМИ и «медиаграмотности» общественности. На практике подобный подход означал регулярную публичную стигматизацию любых фактов и оценок, не вписывающихся в западный нарратив украинского кризиса и последующих событий, в том числе, и официальной позиции российского руководства, как ложных, не заслуживающих внимания, основанных на недостоверной информации и «пропагандистских мифах».

5. На уровне национальных государств на начальном этапе оформления системы противодействия «российской информационной угрозе» можно было наблюдать четыре типа предпринимаемых шагов: а) публичное дискурсивное признание политическими лидерами отдельных стран наличия вызова «кремлёвской пропаганды», б) доктринальное закрепление в позиционных и программных документах общеполитического или, чаще, военно-стратегического характера, в) создание специальных постоянных органов или ситуативных рабочих групп, г) введение ограничительных мер в отношении российских СМИ, общественных организаций или отдельных граждан. Данные шаги, впрочем, носили преимущественно ситуативный, точечный характер и не приобрели повсеместного масштаба. Ограничительные меры были приняты, главным образом, восточноевропейскими странами, тогда как государства Западной Европы только инициировали рассмотрение этого вопроса и в некоторых случаях признавали факт наличия якобы исходящих от России «гибридных угроз» в позиционных и доктринальных документах. Систематические усилия по формированию системы противодействия

«российской информационной угрозе» прилагали Польша, страны Балтии, Великобритания, Нидерланды и скандинавские государства.

На этапе 2014-2016 гг. в США при значительном присутствии дискурса о «российской информационной угрозе» в публичном пространстве на официальном национальном уровне были предприняты лишь ограниченные действия в направлении нейтрализации данной угрозы в виде закрепления на законодательном уровне и на уровне общего военно-стратегического мышления, однако она не стала отдельным поводом для санкций и долгое время не была полноценно институционализирована в системе исполнительной власти страны. Решающую роль в продвижении данной угрозы в американском публичном и политическом пространстве сыграл Конгресс. Наиболее значимой стала инициатива создания в структуре Госдепартамента специального органа для противодействия иностранной пропаганде – Центра глобального взаимодействия, принятая законодательно путём включения в закон о военном бюджете на 2017 г.

6. Результаты президентских выборов в США 2016 г. и резонанс вокруг предполагаемого российского вмешательства дали новый толчок процессу выстраивания инфраструктуры подавления «российской информационной угрозы», позволив представить эту угрозу как направленную против безопасности и стабильности Запада в целом, а не только русскоязычного пространства или стран Восточной Европы. Вследствие этих событий информационная составляющая концепта «гибридной войны» в рассматриваемый период была выведена на первый план как несущая наибольшую опасность западным государствам и институтам и требующая немедленных масштабных мер для её нейтрализации. Это создало основания для инициирования и утверждения на международном и национальном уровнях комплекса более жёстких мер по информационному противодействию России, включая введение адресных санкций за организацию кибератак и попытки вмешательства в избирательный процесс. В 2017 г. подобные меры были формализованы и закреплены на нормативно-правовом уровне, а в 2018 г., на

фоне нового всплеска резонанса вокруг данной тематики под влиянием «дела Скрипалей», начинается их активное применение наряду с усилением контроля за информационной сферой и социальными сетями.

В США главными движущими силами кампании стали отдельные разведывательные, силовые и правоохранительные структуры, присоединившиеся к уже сформированному симбиозу антироссийски настроенных представителей законодательной власти, экспертной среды и СМИ. Они провели публичное расследование «российского вмешательства» и вынесли на повестку дня вопрос о необходимости «наказания» России за него, прежде всего, через санкционные механизмы в информационной сфере и законодательное закрепление наложенных на Россию санкций без возможности их снятия решением президента. Наряду с созданием специально созданного для противодействия иностранной пропаганде Центра глобального взаимодействия в рамках Госдепартамента, были прописаны широкие полномочия и обязанности Пентагона в отношении проведения военных информационных операций, в том числе превентивных, скрытых и не достигающих порога прямых боевых действий. При этом были сняты действовавшие ранее ограничения, связанные с необходимостью межведомственной координации таких операций, а сами они были юридически приравнены к традиционным военным действиям, не требующим особых процедур согласования на уровне политического руководства страны.

7. Ключевой тенденцией в развитии системы подавления «российской информационной угрозы» на уровне национальных европейских государств в данный период стало законодательное оформление нормативной базы контроля за информационным пространством, СМИ и социальными сетями с обязательствами последних удалять нежелательные материалы, квалифицированные как дезинформация, и возможностями государственного контроля за их удалением.

В становлении инфраструктуры борьбы с «российской информационной угрозой» в рассматриваемый период особую роль играла Великобритания.

Несмотря на то, что в британском государственном аппарате степень институционализации функций, связанных с информационным противодействием России, оставалась не самой высокой, официальный Лондон выступил в роли активного генератора дискурса об исходящих от России «гибридных угрозах» на международной арене, принял наиболее жёсткие ограничительные меры в отношении российских СМИ, а его представители участвовали и осуществляли руководство многими международными структурами, созданными для борьбы с «российской пропагандой». Кроме того, заметная часть работы по насаждению антироссийских нарративов и лоббированию антироссийских инициатив в Европе осуществлялась через проекты *Integrity Initiative* – якобы независимой сети кластеров «гражданского общества», курируемой британскими службами и финансируемой структурами британского МИД.

8. Североатлантический альянс, как и прежде, выступал основной структурой, задающей доктринальный вектор развития системы информационного противодействия России, продвигаясь в данный период по пути дальнейшей милитаризации информационной сферы и инкорпорации «гибридных угроз» в свой военно-стратегический аппарат. Для подкрепления политических обязательств о возможности задействования гарантий безопасности НАТО для отражения «гибридных атак» в структуре Альянса были образованы уже не просто аффилированные центры, а стационарные подразделения, осуществляющие мониторинг, планирование операций и подготовку потенциала для задействования в случае «гибридных сценариев» конфликтов. Также Альянс продолжил играть направляющую роль в формировании повестки дня в области «гибридных угроз» для Европейского союза, в том числе с помощью образованного для этих целей Европейского центра передового опыта в Финляндии.

На рассматриваемом этапе в структуре европейского компонента системы информационного противодействия России выделяются три ключевых самостоятельных направления: 1) предупреждение и нейтрализация вызовов в

киберпространстве, 2) отражение «гибридных угроз» и 3) борьба с дезинформацией и «фейковыми новостями», в рамках которой отдельное значение придаётся регулированию социальных сетей. В сфере кибербезопасности в Евросоюзе постепенно оформляется инструментарий реагирования на реальные или планируемые кибератаки извне с возможностью применения ограничительных мер, включая адресные экономические санкции против причастных лиц, по американскому примеру. В области отражения «гибридных угроз» продолжилась работа по закреплению данной сферы в политико-стратегическом и доктринальном аппарате ЕС и формированию институциональной инфраструктуры её обеспечения на коммунитарном и национальном уровнях. Основным её результатом стало составление подробного перечня «гибридных угроз» и уязвимостей государств-членов и анализ необходимого для их устранения потенциала. Вслед за НАТО, Евросоюз также пошёл по пути распространения на сферу «гибридных угроз» своих гарантий безопасности и имеющихся военно-политических средств их обеспечения. В области борьбы с «дезинформацией» благодаря активному подключению Еврокомиссии был достигнут значительный прогресс в виде формирования отдельного механизма регулирования «дезинформации» со специально прописанными критериями и принципами, а также ответственностью СМИ и соцсетей за удаление нежелательного «пропагандистского» контента.

Благодаря подобным мерам были сформированы политические рамки и практические механизмы регулирования, позволяющие Евросоюзу и его органам осуществлять контроль за информационной сферой в автономном режиме, вне зависимости от позиции государств-членов ЕС. Вследствие этого можно констатировать, что Европейский союз с его разветвлённой сетью бюрократических процедур и инструментов взял на себя ведущую роль в осуществлении практической работы по информационному противодействию России на регулярной основе.

Формирование системы противодействия «российской информационной угрозе» на Западе происходило волнообразно, благодаря медийному резонансу от трёх ключевых событий – украинского кризиса 2013-2014 гг., исхода президентских выборов в США в конце 2016 г. и предполагаемой попытки отравления Сергея Скрипаля в 2018 г. Каждое из этих событий становилось поводом для активизации обвинительной риторики в адрес России в западном публичном пространстве и апеллирования к международным и национальным органам управления с требованиями принять меры для отражения якобы крайне актуальной угрозы.

На данном этапе система противодействия «российской информационной угрозе» на Западе представляет собой дисперсную сетевую конструкцию, состоящую из ряда официальных и полуофициальных органов, аффилированных с западными международными организациями или функционирующих непосредственно в их структуре, и опирающуюся на значительный негосударственный компонент в виде различных экспертно-аналитических институтов и волонтерских проектов. Последние регулярно продуцируют материалы, позволяющие поддерживать дискурс о российской «гибридной войне» и «дезинформации» на политической повестке дня западного сообщества. Дисперсный характер данной системы компенсируется её целостной концептуальной основой в виде дискурса о «гибридной войне» и «российской информационной угрозе», разделяемой всеми участниками системы и не являющейся предметом политических дискуссий.

Указанная концептуальная основа сконструирована исходя из базовых представлений о глубинной укоренённости «гибридных» методов в российском стратегическом мышлении и имманентной склонности России к агрессивной внешней политике вне зависимости от конкретных исторических обстоятельств. Изображая подобные свойства нашей страны в качестве политической константы, архитекторы системы борьбы с «российской информационной угрозой» намеренно не заложили в неё критерии и условия, при выполнении которых Россия может опровергнуть обвинения в ведении «гибридной войны»

против Запада. Тем самым, они преодолели доминирующий в течение всего постбиполярного периода нормативный подход к развитию отношений с Россией, где Россия представлялась переходной страной, с которой при выполнении ряда предварительных требований по соответствию «демократическим стандартам» можно пойти на нормализацию отношений и конструктивное партнёрство. Сегодняшняя система борьбы с российской пропагандой и, шире, «российской угрозой» («гибридной» и информационной) изначально выстроена на фундаменте бездоказательных обвинений и произвольных трактовок, которые в любой момент пополняются непредсказуемым образом принципиально новыми обвинениями и трактовками, как только уже известные перестают казаться актуальными. Поэтому, ввиду отсутствия чётко очерченного круга «враждебных» действий России, которые могут подвергнуться криминализации в рамках описанной системы, не существует такой внешнеполитической линии российского государства (в рамках принципиально приемлемого для него), которая не будет охарактеризована как агрессивная и подлежащая наказанию.

При этом данная система, фактически, является частью более обширного комплекса конфронтационного курса Запада в отношении России, включающего меры военно-политического сдерживания, дипломатической изоляции и экономического подавления путём различного рода ограничений и санкций. В рамках этого комплекса система информационного противодействия выполняет ряд важных функций. Во-первых, она закрепляет образ РФ не просто как ситуативного конкурента, а как ценностного антагониста Запада. Благодаря этому формируется репрезентация общей угрозы, в одинаковой степени актуальной для всего западного сообщества. Во-вторых, акцентирует внимание на том, как этот антагонист якобы действует за гранью правил, допустимых в сообществе суверенных государств, чем открывает возможность для Запада не придерживаться этих правил в отношениях с Россией. В-третьих, она поддерживает накал и градус антироссийской напряжённости в западном обществе вне зависимости от реальных действий и заявлений официального

руководства России. Она предоставляет обоснования конфронтационного курса Запада, даже если со стороны Москвы объективно нет признаков готовности к подобной конфронтации. Тем самым искусственно ограничивается субъектность России как ответственного суверенного участника международных отношений, дискредитируется её официальная позиция и подрывается её политическая и правовая легитимность в глазах международной общественности.

Благодаря формированию данной системы мы можем констатировать появление примечательной новации в международных отношениях – возможностей для стигматизации и диффамации государства вне прямой коммуникации и взаимодействия по общепризнанным дипломатическим каналам руками полуофициальных органов невысокого институционального статуса, но имеющих возможность регулярно озвучивать свою позицию в публичном пространстве.

При этом следует отметить, что, хотя основные структурные элементы данной системы уже сформированы, это не исключает возможности их дальнейшего развития, изменения и расширения в будущем. До тех пор, пока Запад будет продолжать свой конфронтационный курс в отношении России, дискурс о «российской информационной угрозе» будет неизменно востребован как для поддержания общей атмосферы конфронтации, так и для нанесения конкретных репутационных ударов по нашей стране, а это означает, что данная система сохранит свою релевантность. Однако на данный момент предпосылок к изменению конфронтационного курса Запада не просматривается – более того, проведённый в настоящей работе анализ показывает, что этот курс, благодаря системному характеру создания конструкта «российской угрозы» и институционального закрепления системы борьбы с ней, приобрёл максимально возможную устойчивость и не будет пересмотрен вплоть до коренной трансформации международно-политического контекста.

Список литературы

Официальные документы

1. Заявление по итогам встречи на высшем уровне в Брюсселе. Обнародовано главами государств и правительств, участвующими в заседании Североатлантического совета в Брюсселе 11-12 июля 2018 года // НАТО. 11 июля 2018. URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=ru (дата обращения: 11.11.2020)
2. Заявление по итогам встречи на высшем уровне в Уэльсе, обнародовано главами государств и правительств, участвующими в заседании Североатлантического союза в Уэльсе – 4-5 сентября 2014 г. URL: https://www.nato.int/cps/en/natohq/official_texts_112964.htm?selectedLocale=ru (дата обращения: 11.11.2020)
3. Недавние события на Украине: угрозы функционированию демократических институтов (неофициальный перевод) // Резолюция Парламентской ассамблеи Совета Европы. 9 апреля 2014 г. № 1988. URL: [https://www.coe.int/T/r/Parliamentary_Assembly/\[Russian_documents\]/\[2014\]/April2014/Res1988_rus.asp](https://www.coe.int/T/r/Parliamentary_Assembly/[Russian_documents]/[2014]/April2014/Res1988_rus.asp) (дата обращения: 11.11.2020)
4. Пересмотр по существенным основаниям ранее утвержденных полномочий российской делегации (неофициальный перевод) // Резолюция Парламентской ассамблеи Совета Европы. 10 апреля 2014 г. № 1990. URL: [https://www.coe.int/T/r/Parliamentary_Assembly/\[Russian_documents\]/\[2014\]/April2014/Res1990_rus.asp](https://www.coe.int/T/r/Parliamentary_Assembly/[Russian_documents]/[2014]/April2014/Res1990_rus.asp) (дата обращения: 11.11.2020)
5. 5 Trends in Leading-Edge Communications // Government Communication Service. 7 Oct. 2018. URL: <https://gcs.civilservice.gov.uk/publications/five-trends-in-leading-edge-communications/> (дата обращения: 11.11.2020)
6. 5th Special Report – Disinformation and 'fake news': Interim Report: Government Response to the Committee's Fifth Report. 9 October 2018. URL:

- <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1630/163002.htm> (дата обращения: 11.11.2020)
7. A Strategic Approach to Resilience in the EU's external action. . Joint Communication to the European Parliament and the Council // European Commission. 7 June 2017. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0021&from=en> (дата обращения: 11.11.2020)
 8. Action Plan against Disinformation. Joint Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions // European Commission. 5 December 2018. URL: https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf (дата обращения: 11.11.2020)
 9. Action Plan on Strategic Communications // European External Action Service. 22 June 2015. URL: <http://archive.eap-csf.eu/assets/files/Action%20PLan.pdf> (дата обращения: 11.11.2020)
 10. Annual report 2016–2017 // Intelligence and Security Committee of Parliament, 2018. pp. 32-33.
 11. Bipartisan Senators question State and Defense Departments on funding delays, inadequate staffing for efforts to counter Russian propaganda and disinformation // Todd Young. March 16, 2018. URL: <https://www.young.senate.gov/newsroom/press-releases/bipartisan-senators-question-state-and-defense-departments-on-funding-delays-inadequate-staffing-for-efforts-to-counter-russian-propaganda-and-disinformation-> (дата обращения: 11.11.2020)
 12. Boring N. France / N.Boring // Government Responses to Disinformation on Social Media Platforms. Report for Congress. September 2019. P. 73-81. URL: <https://www.loc.gov/law/help/social-media-disinformation/social-media-disinformation.pdf> (дата обращения: 11.11.2020)

13. Cabinet Office, Rapid Response Unit: Written Question – 226754 // Parliament.UK. Mar. 4, 2019. URL: <https://perma.cc/KL7K-MBTL>. (дата обращения: 11.11.2020)
14. Code of Practice against disinformation: Commission calls on signatories to intensify their efforts. Presse release // European Commission. 29 January 2019. URL: http://europa.eu/rapid/press-release_IP-19-746_en.htm (дата обращения: 11.11.2020)
15. Complementary efforts to enhance resilience and counter hybrid threats – Council Conclusions (10 December 2019) // General Secretariat of the Council. 10 December 2019. URL: <https://data.consilium.europa.eu/doc/document/ST-14972-2019-INIT/en/pdf> (дата обращения: 11.11.2020)
16. Conclusions on external relations // European Council. 19 March 2015. URL: <https://www.consilium.europa.eu/en/press/press-releases/2015/03/19/conclusions-russia-ukraine-european-council-march-2015/> (дата обращения: 11.11.2020)
17. Confronting Russia's Weaponization of Information. Hearing before the Committee on Foreign Affairs House of Representatives, 15 April 2015 // US House of Representatives. URL: <https://docs.house.gov/meetings/FA/FA00/20150415/103320/HHRG-114-FA00-Transcript-20150415.pdf> (дата обращения: 11.11.2020)
18. Council Conclusions on CSDP // Foreign Affairs Council. 18 May 2015. URL: <https://www.consilium.europa.eu/media/24520/st08971en15.pdf> (дата обращения: 11.11.2020)
19. Council Decision concerning restrictive measures against cyber-attacks threatening the Union or its Member State // Council of the European Union. 14 May 2019. URL: <https://data.consilium.europa.eu/doc/document/ST-7299-2019-INIT/en/pdf> (дата обращения: 11.11.2020)
20. Countering Malign Kremlin Influence Development Framework // USAID. June 27, 2019. URL: <https://www.usaid.gov/documents/1863/countering-malign-kremlin-influence-development-framework> (дата обращения: 11.11.2020)

21. Countering Russian Influence in Europe and Eurasia Act of 2017. S.1221 // 115th Congress (2017-2018). URL: <https://www.congress.gov/bill/115th-congress/senate-bill/1221/text/is?overview=closed&format=txt> (дата обращения: 11.11.2020)
22. Cyber Defence Pledge // NATO. 8 July 2016. URL: http://www.nato.int/cps/en/natohq/official_texts_133177.htm (дата обращения: 11.11.2020)
23. Davis S. Russian Meddling in Elections and Referenda in the Alliance / S. Davis // Special report for Science and Technology Committee NATO Parliamentary Assembly. 18 November 2018. URL: <https://www.nato-pa.int/document/2018-russian-meddling-elections-and-referenda-alliance-davis-report-181-stc-18-e-fin> (дата обращения: 11.11.2020)
24. Defending American Security from Kremlin Aggression Act of 2018. S. 3336. A Bill // 115th Congress. URL: <https://www.govinfo.gov/content/pkg/BILLS-115s3336is/pdf/BILLS-115s3336is.pdf> (дата обращения: 11.11.2020)
25. Delivering on the European Agenda on Security to fight against terrorism and pave the way towards an effective and genuine Security Union // European Commission. 20 April 2016. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52016DC0230&from=EN> (дата обращения: 11.11.2020)
26. Der Umgang mit Fake-News. Rechtslage und Reformansatz. // Deutscher Bundestag. Wissenschaftliche Dienste. Report No. WD 10 – 3000 – 067/16 (Dec. 20, 2016). URL: <https://www.bundestag.de/resource/blob/494418/4321d229204080dce488ebd0356b5db2/wd-10-067-16-pdf-data.pdf> (дата обращения: 11.11.2020)
27. Disinformation and ‘fake news’: Final Report published. The Digital, Culture, Media and Sport Committee has published its final report on Disinformation and ‘fake news’ // House of Commons. 18 February 2019. URL: <https://www.parliament.uk/business/committees/committees-a-z/commons->

- [select/digital-culture-media-and-sport-committee/news/fake-news-report-published-17-19/](#) (дата обращения: 11.11.2020)
28. Disinformation and 'fake news': Interim Report. 29 July 2018 URL: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/36302.htm> (дата обращения: 11.11.2020)
 29. EU Code of Practice on Disinformation // European Commission. 28 September 2018. URL: <https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation> (дата обращения: 11.11.2020)
 30. EU Defence Ministers in Riga call for unity in addressing European security threats. Media Release // Latvian Presidency of the Council of the European Union. 19 February 2015. URL: <https://eu2015.lv/news/media-releases/666-eu-defence-ministers-in-riga-call-for-unity-in-addressing-european-security-threats> (дата обращения: 11.11.2020)
 31. EU strategic communications with a view to countering propaganda // European Parliament Policy Department, Directorate General for External Policies. May 2016. URL: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA\(2016\)578008_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf) (дата обращения: 11.11.2020)
 32. European Council meeting (13 and 14 December 2018) – Conclusions // General Secretariat of the Council. 14 December 2018. URL: <https://www.consilium.europa.eu/media/37535/14-euco-final-conclusions-en.pdf> (дата обращения: 11.11.2020)
 33. European Council meeting (18 October 2018) – Conclusions // General Secretariat of the Council. 18 October 2018. URL: <https://www.consilium.europa.eu/en/press/press-releases/2018/10/18/20181018-european-council-conslusions/> (дата обращения: 11.11.2020)
 34. European Council meeting (22 March 2018) – Conclusions // General Secretariat of the Council. 23 March 2018. URL: <https://www.consilium.europa.eu/media/33457/22-euco-final-conclusions-en.pdf> (дата обращения: 11.11.2020)

35. European Council meeting (28 June 2018) – Conclusions // European Council. 28 June 2018. URL: <https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final/> (дата обращения: 11.11.2020)
36. European Parliament resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties // European Parliament. 23 November 2016. URL: <http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P8-TA-2016-0441&format=XML&language=EN> (дата обращения: 11.11.2020)
37. Executive Order 13694 of April 1, 2015. Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities // US Treasury. URL: https://home.treasury.gov/system/files/126/cyber_eo.pdf (дата обращения: 11.11.2020)
38. Executive Order 13721 of March 14, 2016 Developing an Integrated Global Engagement Center to Support Government-wide Counterterrorism Communications Activities Directed Abroad and Revoking Executive Order 13584 // US Government Information. URL: <https://www.govinfo.gov/content/pkg/CFR-2017-title3-vol1/pdf/CFR-2017-title3-vol1-eo13721.pdf> (дата обращения: 11.11.2020)
39. Executive Order 13757 of December 28, 2016. Taking Additional Steps to Address the National Emergency with Respect to Significant Malicious Cyber-Enabled Activities // US Treasury. URL: https://home.treasury.gov/system/files/126/cyber2_eo.pdf (дата обращения: 11.11.2020)
40. Fifth progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017 // NATO. 16 June 2020. URL: https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200615-progress-report-nr5-EU-NATO-eng.pdf (дата обращения: 11.11.2020)

41. Final report of the High Level Expert Group on Fake News and Online Disinformation // European Commission. 12 March 2018. URL: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation> (дата обращения: 11.11.2020)
42. Follow up taken by the EEAS two years after the EP report on EU strategic communication to counteract propaganda against it by third parties // European Parliament. 13 March 2019. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2019-0187_EN.pdf?redirect (дата обращения: 11.11.2020)
43. Food-for-thought-paper “Countering Hybride Threats” // European External Action Service. 13 May 2015. URL: <http://www.statewatch.org/news/2015/may/eeas-csdp-hybrid-threats-8887-15.pdf> (дата обращения: 11.11.2020)
44. Foreign and Commonwealth Office: Integrity Initiative. Question for Foreign and Commonwealth Office. UIN 196177, tabled on 27 November 2018. URL: <https://questions-statements.parliament.uk/written-questions/detail/2018-11-27/196177> (дата обращения: 11.11.2020)
45. Fotyga A. Draft Report on EU strategic communications to counteract propaganda against it by third parties / A. Fotyga // European Parliament. 2 May 2016. 35 p. URL: [http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA\(2016\)578008_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2016/578008/EXPO_IDA(2016)578008_EN.pdf) (дата обращения: 11.11.2020)
46. Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities ("Cyber Diplomacy Toolbox") // General Secretariat of the Council. 7 June 2017. URL: <https://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf> (дата обращения: 11.11.2020)
47. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken [Netzwerkdurchsetzungsgesetz] // Bundesgesetzblatt. Teil I Nr. 61. Sept. 1, 2017. URL:

- https://www.bgbl.de/xaver/bgbl/text.xav?SID=&tf=xaver.component.Text_0&to cf=&qmf=&hlf=xaver.component.Hitlist_0&bk=bgbl&start=%2F%2F%5B%4 0node_id%3D%27634128%27%5D&skin=pdf&tlevel=-2&nohist=1 (дата обращения: 11.11.2020)
48. Government Responses to Disinformation on Social Media Platforms: United Kingdom // Library of Congress, Legal Reports. URL: <https://www.loc.gov/law/help/social-media-disinformation/uk.php> (дата обращения: 11.11.2020)
49. H.R.4278 – Ukraine Support Act. Draft law introduced by E. Royce on 21 March 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/house-bill/4278> (дата обращения: 11.11.2020)
50. H.R.4490 - United States International Communications Reform Act of 2014. Draft law introduced by E. Royce on 28 April 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/house-bill/4490> (дата обращения: 11.11.2020)
51. H.R.5181 - Countering Foreign Propaganda and Disinformation Act of 2016. Draft law introduced by M. Kinzinger et al. on 10 May 2016 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/house-bill/5181/> (дата обращения: 11.11.2020)
52. H.R.5859 - Ukraine Freedom Support Act of 2014. Public Law No: 113-272. Enacted on 18 December 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/house-bill/5859> (дата обращения: 11.11.2020)
53. H.Res.758 - Strongly condemning the actions of the Russian Federation, under President Vladimir Putin, which has carried out a policy of aggression against neighboring countries aimed at political and economic domination. Resolution introduced by A. Kinzinger on 18 November 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/house-resolution/758/> (дата обращения: 11.11.2020)

54. Hearing before the committee on foreign affairs house of representatives one hundred fifteenth congress first session. March 9, 2017. Serial No. 115–7. URL: <https://docs.house.gov/meetings/FA/FA00/20170309/105674/HHRG-115-FA00-Transcript-20170309.pdf> (дата обращения: 11.11.2020)
55. <https://www.gov.uk/government/publications/intelligence-and-security-committee-annual-report-2016-2017> (дата обращения: 11.11.2020)
56. Implementation Plan on Security and Defence // European External Action Service. 14 November 2016. URL: https://eeas.europa.eu/sites/eeas/files/eugs_implementation_plan_st14392.en160.pdf (дата обращения: 11.11.2020)
57. Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities // General Secretariat of the Council. 9 October 2017. URL: <https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf> (дата обращения: 11.11.2020)
58. Increasing resilience and bolstering capabilities to address hybrid threats. Joint Communication to the European Parliament, the European Council and the Council // European Commission. 13 June 2018. URL: https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf (дата обращения: 11.11.2020)
59. Institute for Statecraft: Integrity Initiative // House of Commons Hansard. 12 December 2018. URL: <https://hansard.parliament.uk/Commons/2018-12-12/debates/298F9A3C-307A-40ED-9CB1-3B2A98F14165/InstituteForStatecraftIntegrityInitiative> (дата обращения: 11.11.2020)
60. International Security and Estonia 2019 // Estonian Foreign Intelligence Service Report. Tallinn, 2019. 72 p. URL: <https://www.välisluureamet.ee/pdf/raport-2019-ENG-web.pdf> (дата обращения: 11.11.2020)
61. John S. McCain National Defense Authorization Act for Fiscal Year 2019. Public law 115–232—AUG. 13, 2018. URL:

- <https://www.congress.gov/115/plaws/publ232/PLAW-115publ232.pdf> (дата обращения: 11.11.2020)
62. Joint Concept for Operating in the Information Environment (JCOIE). 25 July 2018. — 62 p. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/concepts/joint_concepts_jcoie.pdf?ver=2018-08-01-142119-830.pdf (дата обращения: 11.11.2020)
63. Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization // NATO. 8 July 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133163.htm (дата обращения: 11.11.2020)
64. Joint Framework on countering hybrid threats a European Union response. Joint Communication to the European Parliament and the Council // European Commission. 6 April 2016. URL: <https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A52016JC0018> (дата обращения: 11.11.2020)
65. Joint Report to the European Parliament, the European Council and the Council on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018 // European Commission. 13 June 2018. URL: https://eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf (дата обращения: 11.11.2020)
66. Joint statement from Prime Minister May and Prime Minister Rutte // UK Government. 4 October 2018. URL: <https://www.gov.uk/government/news/joint-statement-from-prime-minister-may-and-prime-minister-rutte> (дата обращения: 11.11.2020)
67. Joint Statement from the Department Of Homeland Security and Office of the Director of National Intelligence on Election Security. October 7, 2016. URL: <https://www.dhs.gov/news/2016/10/07/joint-statement-department-homeland-security-and-office-director-national> (дата обращения: 11.11.2020)

68. Joint US - UK statement on malicious cyber activity carried out by Russian government. 15 April 2018. URL: <https://www.ncsc.gov.uk/news/joint-us-uk-statement-malicious-cyber-activity-carried-out-russian-government> (дата обращения: 11.11.2020)
69. Juncker J.-C. Mission Letter / J.-C. Juncker // European Commission. 2 August 2016. URL : https://ec.europa.eu/commission/sites/beta-political/files/king_en.pdf (дата обращения: 11.11.2020)
70. Keynote speech by NATO Secretary General Jens Stoltenberg at the opening of the NATO Transformation Seminar // NATO. 25 March 2015. URL: https://www.nato.int/cps/en/natohq/opinions_118435.htm (дата обращения: 11.11.2020)
71. La vision stratégique pour la Défense (2016-2030) par CPV BEM Renaud FLAMANT Cellule Stratégie // Cabinet de la Défense et de la Fonction Publique. 8 juillet 2016. URL: https://www.cgsp-defense.be/Datas/Documents/Mil/Vision_Strategique_2030.pdf (дата обращения: 11.11.2020)
72. Lidegaatd M. et al. EU Strategic communication responding to propaganda. Non-paper. 8 January 2015. URL: <http://club.bruxelles2.eu/wp-content/uploads/2015/02/Let-StratCommRussie-DkEstLitUk@UK150108.pdf> (дата обращения: 11.11.2020)
73. Loi relative à la lutte contre la manipulation de l'information : DOSSIER LEGISLATIF // Senat.fr. URL: <https://www.senat.fr/dossier-legislatif/ppl17-623.html> (дата обращения: 11.11.2020)
74. Lord Jopling. Countering Russia's Hybrid Threats: an Update / Lord Jopling // Special report for the Committee on the Civil Dimension of Security NATO Parliamentary Assembly. 27 March 2018. URL: <https://www.nato-pa.int/document/2018-countering-russias-hybrid-threats-jopling-report-166-cds-18-e> (дата обращения: 11.11.2020)

75. Macron E. For European renewal / E. Macron // Elisee.fr. 4 March 2019. URL: <https://www.elysee.fr/emmanuel-macron/2019/03/04/for-european-renewal.en> (дата обращения: 11.11.2020)
76. Meeting Conclusions // European Council. 26 June 2015. URL: <https://www.consilium.europa.eu/media/21717/euco-conclusions-25-26-june-2015.pdf> (дата обращения: 11.11.2020)
77. Mueller R. S. Report on the Investigation into Russian Interference in the 2016 Presidential Election / R. S. Mueller // Washington, D.C. March 2019. URL: <https://www.justice.gov/storage/report.pdf> (дата обращения: 11.11.2020)
78. Multinational Capabilities Development Campaign (MCDC) 15-16. COUNTERING HYBRID WARFARE (CHW) // MCDC. 9 November 2015. URL: https://wss.apan.org/public/MCDCpub/MCDC_2015_16/Shared Documents/MCDC 15-16 Project Sheet CHW 09NOV15.pdf (дата обращения: 11.11.2020)
79. Myths about the EU-Ukraine Association Agreement. Setting the facts straight // The European Commission. 22 January 2014. URL: http://trade.ec.europa.eu/doclib/docs/2014/january/tradoc_152074.pdf (дата обращения: 11.11.2020)
80. National cyber strategy of the United States of America // White House. September 2018. URL: https://digital.library.unt.edu/ark:/67531/metadc1259394/m2/1/high_res_d/National-Cyber-Strategy.pdf (дата обращения: 11.11.2020)
81. National Defense Authorization Act for Fiscal Year 2018. Public law 115–91—DEC. 12, 2017 // US Congress. URL: <https://www.congress.gov/115/plaws/publ91/PLAW-115publ91.pdf> (дата обращения: 11.11.2020)
82. National Defense Authorization Act for Fiscal Year 2020. S. 1719. // US Congress. URL: <https://www.govinfo.gov/content/pkg/BILLS-116s1790enr/pdf/BILLS-116s1790enr.pdf> (дата обращения: 11.11.2020)

83. National Security Capability Review (NSCR) // Cabinet Office. 28 March 2018.
URL: <https://www.gov.uk/government/publications/national-security-capability-review-nscr> (дата обращения: 11.11.2020)
84. NATO's response to hybrid threats // NATO. 8 August 2019. URL: https://www.nato.int/cps/en/natohq/topics_156338.htm (дата обращения: 11.11.2020)
85. Ofcom Broadcast Bulletin. Issue number 266 // UK Office of Communications.
10 November 2014. URL: https://www.ofcom.org.uk/_data/assets/pdf_file/0025/47635/obb266.pdf (дата обращения: 11.11.2020)
86. Oral evidence: Disinformation and 'fake news', HC 363. – Digital, Culture, Media and Sport International Grand Committee // House of Commons. 27 November 2018. URL: <http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culture-media-and-sport-committee/disinformation-and-fake-news/oral/92923.pdf> (дата обращения: 11.11.2020)
87. Outcome of the Council Meeting // Council of the European Union. 29 January 2015. URL: <https://www.consilium.europa.eu/media/23243/st05755en15.pdf> (дата обращения: 11.11.2020)
88. Presidential Policy Directive -- United States Cyber Incident Coordination // The White House. 26 July 2016. URL: <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident> (дата обращения: 11.11.2020)
89. Press conference by NATO Secretary General Jens Stoltenberg ahead of Meetings of NATO Defence Ministers // NATO. 25 October 2016. URL: https://www.nato.int/cps/en/natohq/opinions_136414.htm (дата обращения: 11.11.2020)
90. Press statements by the NATO Secretary General Jens Stoltenberg and the EU High Representative for Foreign Affairs and Security Policy, Federica Mogherini // NATO. 1-2 December 2015. URL:

- https://www.nato.int/cps/en/natohq/opinions_125361.htm (дата обращения: 11.11.2020)
91. Putin's asymmetric assault on democracy in Russia and Europe: implications for U.S. national security. A minority staff report prepared for the use of the committee on foreign relations united states senate. January 10, 2018. URL: <https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf> (дата обращения: 11.11.2020)
 92. Putin's Invasion of Ukraine and the Propaganda that Threatens Europe. Hearing before the Subcommittee on Europe and regional security cooperation of the Committee on foreign relations United States Senate, 3 November 2015 // US Senate. URL: https://www.foreign.senate.gov/imo/media/doc/11_03_15_Putin's_Invasion_of_Ukraine_and_the_Propaganda_that_Threatens_Europe.pdf (дата обращения: 11.11.2020)
 93. Reckless campaign of cyber attacks by Russian military intelligence service exposed // National Cyber Security Centre. 3 October 2018. URL: <https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed> (дата обращения: 11.11.2020)
 94. Remarks by President Donald Tusk after the European Council meeting // European Council. 26 June 2015. URL: <https://www.consilium.europa.eu/en/press/press-releases/2015/06/26/tusk-final-remarks-european-council/> (дата обращения: 11.11.2020)
 95. Report for the period from 1 January 2015 to 31 December 2015 // NATO Strategic Communications Centre of Excellence. 31 March 2016. URL: <https://www.stratcomcoe.org/download/file/fid/75507> (дата обращения: 11.11.2020)
 96. Report for the period from 1 January 2016 to 31 December 2016 // NATO Strategic Communications Centre of Excellence. 31 March 2017. URL: <https://www.stratcomcoe.org/download/file/fid/75507> (дата обращения: 11.11.2020)

97. Report on the implementation of the 2016 Joint Framework on countering hybrid threats and the 2018 Joint Communication on increasing resilience and bolstering capabilities to address hybrid threats // European Commission. 28 May 2019. URL:
https://eeas.europa.eu/sites/eeas/files/report_on_the_implementation_of_the_2016_joint_framework_on_countering_hybrid_threats_and_the_2018_joint_communication_on_increasing_resilien.pdf (дата обращения: 11.11.2020)
98. Report on the implementation of the Action Plan Against Disinformation. Joint Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions // EUR-Lex. 14 June 2019. URL: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:JOIN_2019_0012_FIN (дата обращения: 11.11.2020)
99. Reps Lieu and Castro question why state department funds for countering election meddling are unspent // Ted Leu. March 6, 2018. URL: <https://lieu.house.gov/media-center/press-releases/rep-lieu-and-castro-question-why-state-department-funds-countering> (дата обращения: 11.11.2020)
100. Reps M. Recent developments in Ukraine: threats to the functioning of democratic institutions / M. Reps, M. de Pourbaix-Lundin // Report of the Committee on the Honouring of Obligations and Commitments by Member States of the Council of Europe (Monitoring Committee). Parliamentary Assembly of the Council of Europe. 8 April 2014. Doc. 13482. URL: <http://semantic-pace.net/tools/pdf.aspx?doc=aHR0cDovL2Fzc2VtYmx5LmNvZS5pbmQvbncveG1sL1hSZWYvWDJILURXLWV4dHIuYXNwP2ZpbGVpZD0yMDcxMiZsYW5nPUVO&xsl=aHR0cDovL3NlbWFudGljcGFjZS5uZXQvWHNsdC9QZGYvWFJlZi1XRC1BVC1YTUwyUERGLnhzbA==&xsltparams=ZmlsZWlkPTIwNzEy> (дата обращения: 11.11.2020)
101. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. Joint Communication to the European Parliament and the Council // European Commission. 13 September 2017. URL: <https://eur-lex.europa.eu/legal->

- <content/EN/TXT/HTML/?uri=CELEX:52017JC0450&from=en> (дата обращения: 11.11.2020)
102. Resolution 445 – Updating the Responses to Russia’s Hybrid Tactics – CDS // NATO Parliamentary Assembly. 19 November 2018. URL: <https://www.nato-pa.int/document/resolution-445-updating-responses-russias-hybrid-tactics> (дата обращения: 11.11.2020)
103. Resolution of 10 June 2015 on the state of EU-Russia relations // European Parliament. 10 June 2015. URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0225+0+DOC+XML+V0//EN> (дата обращения: 11.11.2020)
104. Resolution of 15 January 2015 on the situation in Ukraine // European Parliament. 15 January 2015. URL: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2015-0011+0+DOC+XML+V0//EN&language=EN (дата обращения: 11.11.2020)
105. Resolution on the Annual Report from the High Representative of the European Union for Foreign Affairs and Security Policy to the European Parliament // European Parliament. 12 March 2015. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52015IP0075&from=EN> (дата обращения: 11.11.2020)
106. Russia - the influence of propaganda on EU countries (topical debate) // European Parliament Debates. 17 January 2018. URL: <http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20180117+ITEM-016+DOC+XML+V0//EN&language=EN>
https://news.vice.com/en_us/article/yw5kak/europe-is-drowning-in-russian-fake-news (дата обращения: 11.11.2020)
107. Russia: Implications for UK defence and security // UK House of Commons Defence Committee. First Report of Session 2016–17. 28 June 2016. URL: <https://publications.parliament.uk/pa/cm201617/cmselect/cmdfence/107/107.pdf> (дата обращения: 11.11.2020)

108. Russian disinformation undermining Western democracy // Resolution adopted at the European People's Party Congress, St. Julian's (Malta), 29 – 30 March 2017. URL: <https://www.epp.eu/papers/russian-disinformation-undermining-western-democracy/> (дата обращения: 11.11.2020)
109. Russian Hackers Indicted. GRU Military Intelligence Officers Targeted Anti-Doping Organizations, Other International Agencies // FBI. October 4, 2018. URL: <https://www.fbi.gov/news/stories/russian-gru-officers-charged-with-hacking-100418> (дата обращения: 11.11.2020)
110. Russian Military Power Assessment // Defence Intelligence Agency, 2017. URL: <https://www.dia.mil/News/Articles/Article-View/Article/1232488/defense-intelligence-agency-releases-russia-military-power-assessment/> (дата обращения: 11.11.2020)
111. S. - 2692. To counter foreign disinformation and propaganda, and for other purposes. Draft law introduced by R. Portman on 16 March 2016 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/senate-bill/2692/> (дата обращения: 11.11.2020)
112. S.2183 - A bill entitled "United States International Programming to Ukraine and Neighboring Regions". Introduced by M. McConnell on 3 April 2014 // US Congress. URL: <https://www.congress.gov/bill/113th-congress/senate-bill/2183> (дата обращения: 11.11.2020)
113. S.2943 - National Defense Authorization Act for Fiscal Year 2017 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/senate-bill/2943> (дата обращения: 11.11.2020)
114. S.3274 - Countering Foreign Propaganda and Disinformation Act. Draft law introduced by R. Portman on 14 July 2016 // US Congress. URL: <https://www.congress.gov/bill/114th-congress/senate-bill/3274> (дата обращения: 11.11.2020)
115. Schiff Statement on Release of Facebook Advertisements // Permanent Select Committee of Intelligence. Washington, May 10, 2018. URL:

<https://intelligence.house.gov/news/documentsingle.aspx?DocumentID=379>

(дата обращения: 11.11.2020)

116. Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy // European External Action Service. June 2016. 60 p. URL: https://eeas.europa.eu/sites/eeas/files/eugs_review_web_0.pdf (дата обращения: 11.11.2020)
117. State-Defense Cooperation on Global Engagement Center Programs and Creation of the Information Access Fund to Counter State-Sponsored Disinformation // Department of State. February 26, 2018. URL: <https://www.state.gov/state-defense-cooperation-on-global-engagement-center-programs-and-creation-of-the-information-access-fund-to-counter-state-sponsored-disinformation/> (дата обращения: 11.11.2020)
118. Statement on the implementation of the Joint Declaration signed by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization // NATO. 6 December 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_138829.htm (дата обращения: 11.11.2020)
119. Steinmeier F.-W. « Grußwort des Bundesministers des Auswärtigen », dans Auswärtiges Amt (Hrsg.) / F.-W. Steinmeier, Jahresabrüstungsbericht 2014, Berlin, 2014, p. I. URL: <http://docplayer.org/77468928-Jahresabruestungsbericht-2014.html> (дата обращения: 11.11.2020)
120. Strategy for Operations in the Information Environment // US Department of Defense. June 2016. 20 p. URL: <https://dod.defense.gov/Portals/1/Documents/pubs/DoD-Strategy-for-Operations-in-the-IE-Signed-20160613.pdf> (дата обращения: 11.11.2020)
121. Summary. Department of defense cyber strategy. 2018. URL: <https://media.defense.gov/2018/Sep/18/2002041658/-1/->

- 1/1/CYBER STRATEGY SUMMARY FINAL.PDF (дата обращения: 11.11.2020)
122. Tackling online disinformation: a European Approach. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions // EUR-Lex. 26 April 2018. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236> (дата обращения: 11.11.2020)
123. The EU and Russia: before and beyond the crisis in Ukraine // House of Lords European Union Committee 6th report of Session 2014–15. 10 February 2015. URL: <https://publications.parliament.uk/pa/ld201415/ldselect/ldeucom/115/115.pdf> (дата обращения: 11.11.2020)
124. The Multinational Capability Development Campaign (MCDC) // NATO. February 2019. URL: https://www.act.nato.int/images/stories/media/opex/2019_MCDC_FUTLEAD.pdf (дата обращения: 11.11.2020)
125. The National Military Strategy of the United States of America 2015 // National Security Strategy Archive. 1 July 2015. P. 4-5. URL: http://nssarchive.us/wp-content/uploads/2020/04/2015_National_Military_Strategy.pdf (дата обращения: 11.11.2020)
126. The United Kingdom's relations with Russia. Seventh Report of Session 2016–17 // House of Commons. Foreign Affairs Committee. URL: <https://publications.parliament.uk/pa/cm201617/cmselect/cmfaaff/120/120.pdf> (дата обращения: 11.11.2020)
127. The United Kingdom's relations with Russia: Government Response to the Foreign Committee's Seventh Report of Session 2016–17, published on 2 March 2017. URL: <https://publications.parliament.uk/pa/cm201719/cmselect/cmfaaff/332/33202.htm> (дата обращения: 11.11.2020)

128. U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations // Department of Justice. October 4, 2018. URL: <https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and> (дата обращения: 11.11.2020)
129. Warsaw Summit Communiqué. Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016 // NATO. 9 July 2016. URL: https://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en (дата обращения: 11.11.2020)
130. Waszczykowski W. The Battle for the Hearts and Minds: Countering Propaganda Attacks Against the Euro-Atlantic Community / W. Waszczykowski // Report for the Committee on the Civil Dimension of Security, NATO Parliamentary Assembly. 20 October 2015. URL: <https://www.nato-pa.int/document/2015-164-cdsdg-15-e-fin-bis-russian-propaganda-waszczykowski-report> (дата обращения: 11.11.2020)
131. White Paper on German Security Policy and the Future of the Bundeswehr 2016 // The Federal Government. 13 July 2016. URL : [https://issat.dcaf.ch/download/111704/2027268/2016 White Paper.pdf](https://issat.dcaf.ch/download/111704/2027268/2016%20White%20Paper.pdf) (дата обращения: 11.11.2020)

Научные и экспертные работы

132. «Гибридные войны» в мировой политике XXI века. Материалы научного семинара (февраль 2015 г., факультет политологии МГУ имени М. В. Ломоносова) // Политическая экспертиза. ПОЛИТЭКС. 2015. Том 11, № 2. С. 208-237.
133. «Гибридные войны» в хаотизирующемся мире XXI века / под ред. П.А. Цыганкова. М.: Издательство Московского университета, 2015. 384 с.

134. Алхименков М. А. Дипломатия США и украинский кризис / М. А. Алхименков // США и Канада: экономика, политика, культура. 2015. № 9 (549). С. 37-52.
135. Арчаков В. Ю. Информационные технологии гибридных войн / В. Ю. Арчаков, О. С. Макаров // Геополитика и безопасность. 2017. №4 (40). С. 22-25.
136. Арчаков В. Ю. Информационный фактор в гибридных войнах. / В. Ю. Арчаков, В. Н. Пунченко, В. Е. Ременчик // Геополитика и безопасностью 2017. №2 (38). С. 16-27.
137. Базаркина Д. Ю. Новые инструменты Европейского союза в борьбе с дезинформацией / Д. Ю. Базаркина // Аналитические записки Института Европы РАН. 2021. № 19 (249). 7 с.
138. Базаркина Д. Ю. Эволюция подхода Европейского Союза к борьбе с дезинформацией / Д. Ю. Базаркина // Власть. 2021. № 6. С.130-138.
139. Баранов Н. А. Стратегии гибридных войн стран НАТО как вызов Российской Федерации / Н. А. Баранов, П. В. Попов // Евразийская интеграция: экономика, право, политика. 2019. № 2. С. 79-86.
140. Бартош А. А. Гибридная война. Учебное пособие / А. А. Бартош. Москва: Кнорус, 2021. 306 с.
141. Бартош А. А. Гибридная война становится новой формой межгосударственного противоборства / А. А. Бартош // Независимое военное обозрение. 7.04.2017. URL: http://nvo.ng.ru/concepts/2017-04-07/1_943_gibryd.html?print=Y (дата обращения: 11.11.2020)
142. Бартош А. А. Сдерживание и принуждение в стратегии гибридной войны / А.А. Бартош // Военная мысль. 2021. № 9. С. 18-34.
143. Баталов А. Национальная киберстратегия США / А. Баталов // Зарубежное военное обозрение. 2019. № 2 (863). С. 3-11.
144. Белобров Ю. А. «Гибридные войны» НАТО: концепции и методы ведения / Ю. А. Белобров // Вестник Дипломатической академии МИД РФ. Россия и мир. 2022. № 4 (34). С. 6-21.

145. Белозеров В. К. Гибридная война в отечественном политическом и научном дискурсе / В. К. Белозеров, А. В. Соловьев // Власть. 2015. № 9. С. 5-11. URL: http://www.isras.ru/files/File/Vlast/2015/2015_9/Belozerov.pdf (дата обращения: 16.10.2018)
146. Гаврилина С. Государство и СМИ Великобритании: форма взаимодействия / С. Гаврилина, И. Сурма // Современная Европа. 2020. № 1. С. 49–58.
147. Герасимов В. В. Организация обороны Российской Федерации в условиях применения противником “традиционных” и “гибридных” методов ведения войны / В. В. Герасимов // Вестник Академии военных наук. 2016. № 2 (55). С. 19-23.
148. Гладышевский В. Л. Сетевая война Запада и обеспечение ресурсного противодействия сетевому сценарию для России/ В. Л. Гладышевский, Е. В. Горгола // Национальные интересы: приоритеты и безопасность. 2017. Т. 13, вып. 2. С. 369-383.
149. Гуменский А. Шествие троллей. Как коммуникации разрушают дипломатию / А. Гуменский // Россия в глобальной политике. 2015. № 5. URL: <http://www.globalaffairs.ru/number/Shestvie-trollei-17745> (дата обращения: 11.11.2020)
150. Иншаков С. М. Гибридная война в системе военных угроз национальной безопасности / С. М. Иншаков. М.: Русайнс, 2018. 306 с.
151. Истомин И. Россия как держава статус-кво / И. Истомин // Россия в глобальной политике. 2020. № 1. URL: <https://globalaffairs.ru/articles/rossiya-kak-derzhava-status-kvo/> (дата обращения: 11.11.2020)
152. Клименко С. Теория и практика ведения «Гибридных войн» (по взглядам НАТО) / С. Клименко // Зарубежное военное обозрение. 2015. № 5. С. 109-112.
153. Коньшев В. Гибридные войны: между мифом и реальностью / В. Коньшев, Р. Парфенов // Мировая экономика и международные отношения. 2019. Том 63, № 12. С. 56-66.

154. Котляр В. К вопросу о «гибридной войне» и о том, кто же ее ведет на Украине / В. Котляр // Международная жизнь. 2018. № 8. С. 57-72.
155. Кошкин П. Г. «Российское досье» как внутривосточный фактор в США / П. Г. Кошкин // Россия и Америка в XXI веке. 2019. Специальный выпуск. URL: <https://rusus.jes.su/s207054760005318-6-1/> (дата обращения: 11.11.2020)
156. Магда Е. Гибридная агрессия России в Украине: уроки для Европы / Е. Магда // Wschód Europy • Восток Европы • East of Europe. 2016. Vol 2, No. 2. С. 85-95.
157. Манойло А. В. Технологии неклассической войны. Генезис. Эволюция. Практика / А. В. Манойло, К.С. Стригунов // М.: Горячая линия – Телеком, 2020. 378 с.
158. Марков С. «Гибридная война» против России / С. Марков. М.: Алгоритм, 2015. 208 с.
159. Месснер Е. Э. Хочешь Мира, Победи Мятеевойну! / Е. Э. Месснер // Москва, 2005. URL: http://militera.lib.ru/science/0/pdf/messner_ea01.pdf (дата обращения: 11.11.2020)
160. Низовцева Н. Ф. Гибридная война как геополитический тренд / Н. Ф. Низовцева, Н. В. Гришанин // Научные труды СЗИУ — филиала РАНХиГС. 2016. Т. 7. Выпуск 3 (25). С. 76-85.
161. Панарин И. Н. Гибридная война: теория и практика / И. Н. Панарин. М.: Горячая линия – Телеком, 2017. 404 с.
162. Першин Ю. Ю. «Гибридная война» как интеллектуальная провокация / Ю. Ю. Першин // Ученые записки Крымского федерального университета имени В. И. Вернадского. Философия. Политология. Культурология. 2015. Том 1 (67). № 1. С. 80–88.
163. Першин Ю.Ю. Гибридная война: много шума из ничего / Ю.Ю. Першин // Вопросы безопасности. 2019. № 4. С. 78–109.

164. Попов П. В. Возможности демократических государств по реагированию и противодействию гибридным угрозам / П. В. Попов // *Via in tempore. История. Политология*. 2020. № 47 (1). С. 187-193.
165. Порывкин В. Н. Классическая, «гибридная» и «холодная» война как понятия в мировой политике / В. Н. Порывкин // *Современные тенденции развития науки и технологии*. 2017. № 2-7. С. 85-89.
166. Риччери М. Стратегическая коммуникация на службе совместного проекта развития отношений между ЕС и Россией. Утопия или действительность? / М. Риччери // *Государственное управление. Электронный вестник*. 2018. Выпуск 68. С. 79-98.
167. Роговский Е. А. Пентагон усиливает кибероборону / Е. А. Роговский, П. А. Шариков // *США и Канада: экономика, политика, культура*. 2011. № 1 (493). С. 51-60.
168. Романова Т. А. Дезинформация (фейковые новости, пропаганда) как угроза стрессоустойчивости: подходы на уровне Евросоюза и Литвы как его члена / Т. А. Романова, Н. И. Соколов, Ю. Ю. Колотаев // *Балтийский регион*. 2020. Т. 12, № 1. С. 53-67.
169. Савин Л. В. Стрелы кентавра. Кибервойна по-американски / Л. В. Савин. М.: Издательский дом «Кислород», 2020. 590 с.
170. Сазонова К. Л. «Гибридная война»: международно-правовое измерение / К. Л. Сазонова // *Право. Журнал Высшей школы экономики*. 2017. № 4. С. 177–187.
171. Саква Р. Россия против остальных. Кризис мирового порядка после окончания холодной войны / пер. с англ. / Р. Саква. М.: Весь мир, 2020. 414 с.
172. Самкова М. А. Дезинформация как средство информационно-психологической войны против России (на материале медиатекстов о хакерских атаках) / М. А. Самкова // *Экология языка и коммуникативная практика*. 2018. № 3. С. 96–115.

173. Собольников В. В. Место и роль психологического воздействия в стратегии ведения «гибридных» войн НАТО / В. В. Собольников // Гуманитарные проблемы военного дела: Военно-научный журнал. 2015. № 3. С. 25-31.
174. Соколов Р. Стратегия действий Министерства обороны в информационной сфере / Р. Соколов // Зарубежное военное обозрение. 2017. № 8. С. 10-12.
175. Сосновская А. М. Идеология и массовые коммуникации: гибридная война на Украине / А. М. Сосновская // Научные труды Северо-Западного Института управления РАНХиГС. СПб 2016. Т. 7. Выпуск 3 (25). С. 134-142. URL: https://spb.ranepa.ru/images/nauka/NT/NT_7_3.pdf (дата обращения: 11.11.2020)
176. Столетов О. В. «Гибридная война» как теоретический концепт и инструмент дискурсивного влияния в современной мировой политике / О. В. Столетов // «Гибридные войны» в хаотизирующемся мире XXI века / под редакцией П.А. Цыганкова. М.: Издательство Московского университета, 2015. С. 105-123.
177. Трапезникова Ю. В. Гибридная война как инструмент достижения мирового господства / Ю. В. Трапезникова, Л. М. Батурин // Политический вектор-про. Комплексные проблемы современной политики. 2017. № 1-2. С. 43-57.
178. Тренин Д. Смягчение конфликта в условиях гибридной войны / Д. Тренин // Московский центр Карнеги. 2018. 25 января. URL: <https://carnegie.ru/2018/01/25/ru-pub-75296> (дата обращения: 11.11.2020)
179. Филимонов Г. Ю. «Гибридная война»: интерпретации и реальность / Г. Ю. Филимонов, Н. С. Данюк // Свободная мысль. 2017. № 2. С. 24-36.
180. Фомина Т. А. Манипулятивные приёмы дезинформации как средство реализации антироссийской пропаганды в заголовках англоязычных СМИ (на примере освещения «дела Скрипалей» в период с марта по октябрь 2018 года) / Т. А. Фомина, Е. Д. Буцык // Филологические науки в МГИМО. 2019. № 19 (3). С. 50-58.
181. Фридман О. «Гибридная война» понятий (интервью) / О. Фридман // Вестник МГИМО. 2016. Т. 5, № 50. С. 79-85.

182. Цыбаков Д. Л. Развертывание политико-информационных коммуникаций НАТО и Евросоюза в прибалтийском регионе / Д. Л. Цыбаков // Электронный научный журнал «ГосРег». 2021. № 3. URL: <http://gosreg.amchs.ru/pdf/files/37number/art/Tcibakov-37.pdf> (дата обращения: 10.02.2022)
183. Цыбаков Д. Л. Фактор политических коммуникаций в процессе милитаризации постсоветского пространства / Д. Л. Цыбаков // Вестник Московского государственного лингвистического университета. Общественные науки. 2021. Вып. 3 (844). С. 98-111.
184. Цыганков П. А. «Гибридная война»: политический дискурс и международная практика / П. А. Цыганков // Вестн. Моск. ун-та. Сер. 18. Социология и политология. 2015. № 4. С. 253-258.
185. Цыганков П. А. Политическая динамика современного мира: теория и практика / Цыганков П. А. 2-е издание. М: МГУ, 2017. 576 с.
186. Чекинов С. Г. О характере и содержании войны нового поколения / С. Г. Чекинов, С. А. Богданов // Военная мысль. 2013. № 10. С. 13-24.
187. Шариков П. А. Подходы РФ и США к проблеме международного обеспечения информационной безопасности / П. А. Шариков // Проблемы национальной стратегии. 2013. № 5 (20). С. 131-144.
188. Шипицин Ю. Б. «Гибридная» война: Моделирование информационных полей: монография / Ю. Б. Шипицин, А. Ю. Шипицина; научный редактор А. Г. Нестеров. Екатеринбург: Издательство Уральского университета, 2018. 136 с.
189. A Civil-Military Response to Hybrid Threats / E. Cusumano, M. Corbe (eds.) Springer, Palgrave Macmillan, 2018. 320 p.
190. Abrams S. Beyond Propaganda Soviet Active Measures in Putin's Russia / S. Abrams // Connections. Winter 2016. Vol. 15, No. 1. P. 5-31.
191. Andersson J. J. Hybrid operations: lessons from the past / J. J. Andersson // European Union Institute for Security Studies Brief. October 2015. 4 p. URL:

- [https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief 33 Hybrid operations.pdf](https://www.iss.europa.eu/sites/default/files/EUISSFiles/Brief%2033%20Hybrid%20operations.pdf) (дата обращения: 11.11.2020)
192. Ashmore W. C. Impact of Alleged Russian Cyber Attacks / W. C. Ashmore // Baltic Security & Defence Review. 2009. Vol. 11. P. 4-40. URL: https://www.baltdefcol.org/files/files/documents/Research/BSDR2009/1_Ashmore - Impact of Alleged Russian Cyber Attacks .pdf (дата обращения: 11.11.2020)
 193. Bajarūnas E. Addressing Hybrid Threats: Priorities for the EU in 2020 and Beyond / E. Bajarūnas // European View. 2020. Vol. 9 (1). P. 62-70.
 194. Banasik M. A Changing Security Paradigm. New Roles for New Actors – The Russian Approach / M. Banasik // Connections. 2016. Vol. 15, No. 4. P. 31-43.
 195. Banasik M. Russia's hybrid war / M. Banasik // Science & Military. 2016. No. 2. P. 39-47.
 196. Banasik M. Russia's Hybrid War In Theory and Practice / M. Banasik // Journal on Baltic Security. 2016. Vol 2, Issue 1. P. 157-182.
 197. Barbin J. La guerre hybride : un concept stratégique flou aux conséquences politiques réelles / J. Barbin // Les Champs de Mars. 2018/1 (No°30 + Supplément). P 109-116. URL : <https://www.cairn.info/revue-les-champs-de-mars-2018-1-page-109.htm> (дата обращения: 11.11.2020)
 198. Bardach-Yalov E. Analyzing Russian propaganda: Application of Siegfried Kracauer's qualitative content analysis method / E. Bardach-Yalov // Journal of Information Warfare. 2012. Vol.11, No. 2. P. 24–36.
 199. Barmin Yu. International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and Information Security / Yu. Barmin, G. Jones, S. Moiseeva, Z. Winkelman // The Quarterly Journal. Fall 2011. P. 73-94.
 200. Basulto D. Russophobia: How Western Media Turns Russia Into the Enemy / D. Basulto. Lightning Source INC. 2015. 286 p.
 201. Bergmann M. Acts of an Adversary. Russia's Ongoing Hostilities Toward the United States and Its Allies / M. Bergmann, C. K. December // Center for

- American Progress. 2017. 48 p. URL: <https://www.americanprogress.org/issues/security/reports/2017/12/05/443574/acts-of-an-adversary/> (дата обращения: 11.11.2020)
202. Bergmann M. War by Other Means. Russian Active Measures and the Weaponization of Information / M. Bergmann, C. Kenney // Center for American Progress. 2017. 45 p. URL: <https://www.americanprogress.org/issues/security/reports/2017/06/06/433345/war-by-other-means/> (дата обращения: 11.11.2020)
203. Bērziņš J. Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy / Bērziņš J. // National Defence Academy of Latvia Center for Security and Strategic Research Policy Paper. April 2014, No 02. 13 p. URL: <https://www.sldinfo.com/wp-content/uploads/2014/05/New-Generation-Warfare.pdf> (дата обращения: 11.11.2020)
204. Blackwill R. D. Containing Russia. How to Respond to Moscow's Intervention in U.S. Democracy and Growing Geopolitical Challenge / R. D. Blackwill, Ph. H. Gordon // Council on Foreign Relations (CFR). Council Special Report No. 80. January 2018, 43 p. URL: https://cdn.cfr.org/sites/default/files/report_pdf/CSR80_BlackwillGordon_ContainingRussia.pdf (дата обращения: 11.11.2020)
205. Bogomolov A. A Ghost in the Mirror: Russian Soft Power in Ukraine / A. Bogomolov, O. Lytvynenko // Chatham House Briefing Paper. 1 January 2012. URL: [https://www.chathamhouse.org/sites/default/files/public/Research/Russia and Eurasia/0112bp_bogomolov_lytvynenko.pdf](https://www.chathamhouse.org/sites/default/files/public/Research/Russia%20and%20Eurasia/0112bp_bogomolov_lytvynenko.pdf) (дата обращения: 11.11.2020)
206. Bond M. S. Hybrid War: A New Paradigm for Stability Operations in Failing States / M. S. Bond // US Army War College Strategy research project. 2007. 25 p. URL: <http://www.dtic.mil/dtic/tr/fulltext/u2/a468398.pdf> (дата обращения: 11.11.2020)
207. Boyd-Barrett O. Ukraine, Mainstream Media and Conflict Propaganda / O. Boyd-Barrett // Journalism Studies. 2017. Volume 18. P. 1016-1034.

208. Boyte K. J. A Comparative Analysis of the Cyberattacks Against Estonia, the United States, and Ukraine: Exemplifying the Evolution of Internet-Supported Warfare / K. J. Boyte // International Journal of Cyber Warfare and Terrorism. April-June 2017, Vol. 7, Issue 2. P. 54-70.
209. Boyte K. J. An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine / K. J. Boyte // Journal of Information Warfare. 2017. Vol. 16, No. 1. P 88-111.
210. Bradshaw S. Government Responses to Malicious Use of Social Media / S. Bradshaw, L.-M. Neudert, Ph. N. Howard // NATO Stratcom CoE. Riga, November 2018. 20 p. URL: <https://www.stratcomcoe.org/government-responses-malicious-use-social-media> (дата обращения: 11.11.2020)
211. Brattberg E. Russian Election Interference. Europe Counter to Fake News and Cyber Attacks / E. Brattberg, T. Maurer // Carnegie Endowment for International Peace. May 2018. 54 p. URL: https://carnegieendowment.org/files/CP_333_BrattbergMaurer_Russia_Elections_Interference_FINAL.pdf (дата обращения: 11.11.2020)
212. Bryant W. D. International Conflict and Cyberspace Superiority. Theory and practice/ W. D. Bryant // Routledge. 2017/ 250 p.
213. Cederberg G. Catching Swedish Phish How Sweden is Protecting its 2018 Elections / G. Cederberg // Belfer Center for Science and International Affairs Report. August 2018. URL: <https://www.belfercenter.org/publication/catching-swedish-phish-how-sweden-protecting-its-2018-elections> (дата обращения: 11.11.2020)
214. Charap S. The Ghost of Hybrid War / S. Charap // Survival. 2015. Vol. 57, No. 6. P. 51-58.
215. Cimbala S. J. A New Cold War? Missile Defenses, Nuclear Arms Reductions, and Cyber War / S. J. Cimbala, R. N. McDermott // Comparative Strategy. 2015. Vol. 34, Issue 1. P. 95-111.

216. Clarke R.A. Cyber War: The Next Threat to National Security and What to Do About It / R.A. Clarke, R.K. Knake // New York: HarperCollins Publishers, 2010. 304 p.
217. Cohen S. F. War with Russia? From Putin & Ukraine to Trump and Russiagate / S. F. Cohen. New York: Hot Books, 2019.
218. Colon Piella G. La doctrina Gerasimov y el pensamiento estratégico ruso / G. Colon Piella // Revista Ejército. Diciembre 2018. No. 933. P. 30-37. URL: <https://www.ugr.es/~gesi/Doctrina-Gerasimov.pdf> (дата обращения: 11.11.2020)
219. Conley H. A. Successfully Countering Russian Electoral Interference 2 // H. A. Conley, J.-B. Jeangène Vilmer // CSIS Briefs. June 2018. URL: <https://www.csis.org/analysis/successfully-countering-russian-electoral-interference> (дата обращения: 11.11.2020)
220. Connell M. Russia's Approach to Cyber Warfare / M. Connell, S. Vog // CNA Analytic Solutions. March 2017. URL: https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf (дата обращения: 11.11.2020)
221. Countering Hybrid Threats: Lessons Learned from Ukraine. Editors: N. Iancu, A. Fortuna, C. Barna and M. Teodor (eds.) // IOS Press. 2016. 286 p.
222. Countering Hybrid Warfare: the Best Uses of SOF in a Pre-Article V Scenario / M. Freeman et al. (Eds.) // CTX. Vol. 6, No. 4. Special Issue. URL: https://www.academia.edu/34094910/Countering_Hybrid_Warfare_The_Best_Uses_of_SOF_in_a_Pre_Article_V_Scenario (дата обращения: 11.11.2020)
223. Countering Russian Propaganda // Concordiam (Journal of George Marshall European Center for Security Studies). Special Edition. 2016. Vol. 7. 40 p.
224. Crandall M. Small States and Big Ideas: Estonia's Battle for Cybersecurity Norms / M. Crandall, C. Allan // Contemporary Security Policy. 2015. Vol. 36, No. 2. P. 346–368.
225. Cross Sh. N. Russia and Countering Violent Extremism in the Internet and Social Media: Exploring Prospects for U.S.-Russia Cooperation Beyond the "Reset" /

- Sh. N. Cross // *Journal of Strategic Security*. 2013. Vol. 6, No. 4. P. 1-24. URL: <http://scholarcommons.usf.edu/jss/vol6/iss4/1> (дата обращения: 11.11.2020)
226. Ćwiek-Karpowicz Ja. Limits to Russian Soft Power in the Post-Soviet Area / Ja. Ćwiek-Karpowicz // *DGAPanalyse*. 2012. No. 8. 16 p. URL: https://dgap.org/system/files/article_pdfs/2012-08_DGAPana_C%CC%81wiek-Karpowicz_www_0.pdf (дата обращения: 11.11.2020)
227. *Cyber War in Perspective: Russian Aggression against Ukraine* / K. Geers (ed.). NATO CCD COE Publications, Tallinn 2015. 175 p. URL: https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf (дата обращения: 11.11.2020)
228. Danyk Y. Hybrid War High-tech, Information and Cyber Conflicts / Y. Danyk, T. Maliarchuk, Ch. Briggs // *Connections*. Spring 2017. Vol. 16, No. 2. P. 5-24.
229. Darczewska J. The Anatomy of Russian Information Warfare the Crimean Operation. A Case Study / J. Darczewska // *OSW Point of View*. May 2014. No. 42. URL: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf (дата обращения: 11.11.2020)
230. Dayspring S. M. Countering Russian Hybrid Warfare: Acknowledging the Character of Modern Conflict / S. M. Dayspring // *Countering Hybrid Warfare: the Best Uses of SOF in a Pre-Article V Scenario*. Ed. Michael Freeman et al. CTX. 2018. Vol. 6, No. 4. Special Issue. P. 20-30.
231. De Wijk R. Hybrid Conflict and the Changing Nature of Actors / R. De Wijk // *The Oxford Handbook of War* / Y. Boyer, J. Lindley-French (eds.). Oxford: Oxford University Press, 2012. P. 359-373.
232. Deibert. R. J. Cyclones in cyberspace: Information shaping and denial in the 2008 Russia–Georgia war / R. J. Deibert, R. Rohozinski, M. Crete-Nishihata // *Security Dialogue*. 2012. Vol. 43, No. 1. P. 3–24.
233. Demchak C. Cybered Conflict, Cyber Power, and Security Resilience as Strategy / C. Demchak // *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World Book* / D. S. Reveron (ed.). Georgetown University

- Press. 2012. URL: <http://www.jstor.org/stable/j.ctt2tt6rz.12> (дата обращения: 11.11.2020)
234. DiResta R. The Tactics & Tropes of the Internet Research Agency. Report on the Internet Research Agency commissioned by the U.S. Senate Intelligence Committee / R. DiResta, K. Shaffer, D. Ruppel et al. New Knowledge, 2018. URL: <https://www.yonder-ai.com/resources/the-disinformation-report/> (дата обращения: 11.11.2020)
235. Efthymiopoulos M. P. NATO's Security Operations in Electronic Warfare: the Policy of CyberDefence and the Alliance's new Strategic Concept / M. P. Efthymiopoulos // Journal of Information Warfare. 2009. Vol. 8, No. 3. P. 61-70.
236. Erol M. S. Hybrid Warfare Studies and Russia's Example in Crimea / M. S. EROL, Ş. OĞUZ // Akademik Bakış. Kış 2015. Cilt 9, Sayı 17. P. 261-277.
237. Fedor J. "We need more clips about Putin, and lots of them:" Russia's state-commissioned online visual culture / J. Fedor, R. Fredheim // The Journal of Nationalism and Ethnicity. 2-17. Vol. 45, Issue 2. P. 161-181.
238. Fisher A. Demonizing the enemy: the influence of Russian state-sponsored media on American audiences // Post-Soviet Affairs. 2020. Vol. 36, No. 4. P. 281-296.
239. Fitton O. Cyber Operations and Gray Zones Challenges for NATO / O. Fitton // Connections. Spring 2016. Vol. 15, No. 2. P. 109-119.
240. Foxall A. Putin Sees and Hears it all: How Russia's Intelligence Agencies Menace the UK / A. Foxall // Henry Jackson Society Report. 5th November 2018. URL: <https://henryjacksonsociety.org/publications/as-many-as-200-russian-case-officers-in-london-handling-up-to-500-agents-and-75000-informants-report-finds/> (дата обращения: 11.11.2020)
241. Foxall A. Putin's Useful Idiots: Britain's Left, Right and Russia / A. Foxall // The Henry Jackson Society Russia Studies Centre. Policy Paper No. 10 (2016). 17 p. URL: <http://henryjacksonsociety.org/wp-content/uploads/2016/10/Putins-Useful-Idiots.pdf> (дата обращения: 11.11.2020)
242. Fridman O. Russian "Hybrid Warfare": Resurgence and Politicization / O. Fridman. Oxford: Oxford University Press, 2018.

243. Fuchs G. F. Hybrid warfare – identifying the cause of potential conflict is important – not the ways and means? / G. F. Fuchs // On-line Journal Modelling the New Europe. 2016. Issue No. 21. P. 77-96.
244. Galeotti M. Heavy metal diplomacy: Russia's political use of its military in Europe since 2014 / M. Galeotti // ECFR Policy Brief. 2016. No. 200. 12 p. URL: http://www.ecfr.eu/page/-/Heavy_Metal_Diplomacy_Final_2.pdf (дата обращения: 11.11.2020)
245. Galeotti M. Hybrid war or gibridnaya voyna? Getting Russia's non-linear military challenge right / M. Galeotti. Mayak Intelligence, 2016. 100 p.
246. Galeotti M. The mythical 'Gerasimov Doctrine' and the language of threat / M. Galeotti // Critical Studies on Security. 2018. Vol. 7, Issue 2. P. 157-161.
247. Gates R. A. Balanced Strategy: Reprogramming the Pentagon for a New Age / R. A. Gates // Foreign Affairs. 2009. Vol. 8, Issue 1. P. 28-40.
248. Gaufman E. Security Threatsand and Public Perceptions. Digital Russia and the Ukraine Crisis / E. Gaufman. Basingstoke: Palgrave Macmillan, 2017. 230 p.
249. Geers K. (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine / K. Geers (Ed.) // Tallinn: NATO CCD COE Publications. 2015. 175 p.
250. Gerber T. P. Does Russian Propaganda Work? / T. P. Gerber, J. Zavisca // The Washington Quarterly. 2016. Vol. 39, No. 2. P. 79-98.
251. Gesley J. Government Responses to Disinformation on Social Media Platforms: Germany / J. Gesley // Government Responses to Disinformation on Social Media Platforms. Report for Congress. September 2019. P. 82-91. URL: <https://www.loc.gov/law/help/social-media-disinformation/social-media-disinformation.pdf> (дата обращения: 11.11.2020)
252. Giles K. "Information Troops" – a Russian Cyber Command? / K. Giles // 2011 3rd International Conference on Cyber Conflict / C. Czosseck, E. Tyugu, T. Wingfield (Eds.). Tallinn, Estonia. 2011. P. 45-60.
253. Glenn R. W. All Glory Is Fleeting. Insights from the Second Lebanon War / R. W. Glenn. Santa Monica, Ca Rand: National Defense Research Institute, 2012.

- 97 p. URL: <https://www.rand.org/pubs/monographs/MG708-1.html> (дата обращения: 11.11.2020)
254. Glenn R. W. Thoughts on “Hybrid” Conflict / R. W. Glenn // Small Wars Journal. 2009. URL: <http://smallwarsjournal.com/mag/docs-temp/188-glenn.pdf> (дата обращения: 11.11.2020)
255. Golovchenko Y. State, media and civil society in the information warfare over Ukraine: citizen curators of digital disinformation / Yu. Golovchenko, M. Hartmann, R. Adler-Nissen // International Affairs. 2018. Vol. 94, Issue 5. P. 975–994.
256. Gude K. Russia’s 5th Column / K. Gude // Center for American Progress. March 2017. 37 p. URL: <https://www.americanprogress.org/issues/security/reports/2017/03/15/428074/russias-5th-column/> (дата обращения: 11.11.2020)
257. Gvosdev N. K. The Bear Goes Digital: Russia and Its Cyber Capabilities / N. K. Gvosdev // Cyberspace and National Security. Book Subtitle: Threats, Opportunities, and Power in a Virtual World Book / D. S. Reveron (ed.). Georgetown: Georgetown University Press, 2012. P. 173–190.
258. Hacks, leaks and disruptions – Russian cyber strategies / N. Popescu, S. Secriery (Eds.) // EU ISS Chaillot papers. 2018. No. 148. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (дата обращения: 11.11.2020)
259. Hall H. K. The new voice of America: Countering Foreign Propaganda and Disinformation Act / H. K. Hall // First Amendment Studies. 2017. Vol. 51, No. 2. P. 49-61.
260. Hanlon B. It’s Not Just Facebook: Countering Russia’s Social Media Offensive / B. Hanlon // The Alliance for Securing Democracy (at the German Marshall Fund of the United States Brief. April 2018. No. 19. URL: <https://securingdemocracy.gmfus.org/its-not-just-facebook-countering-russias-social-media-offensive/> (дата обращения: 11.11.2020)

261. Haukkala H. A Close Encounter of The Worst Kind? The Logic of Situated Actors and the Statue Crisis Between Estonia and Russia / H. A. Haukkala // Journal of Baltic Studies. 2009. Vol. 40, No. 2. P. 201–213.
262. Hellum N. The War at Home: Putin's Information Strategy Toward the Russian Population / N. Hellum // Information Sharing in Military Operations / I. Goldenberg, J. Soeters, W. H. Dean (eds.). Switzerland: Springer International Publishing, 2017. P. 235-250.
263. Herzog S. Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses / S. Herzog // Journal of Strategic Security, 2011. Vol. 4, No. 2. P. 49-60. URL: <http://scholarcommons.usf.edu/jss/vol4/iss2/4> (дата обращения: 11.11.2020)
264. Hoffman F. G. Conflict in the 21-st Century. The Rise of Hybrid Wars / F. G. Hoffman. Arlington: Potomac Institute for policy studies, 2007. 72 p.
265. Hoffman F. G. Further Thoughts on Hybrid Threats / F. G. Hoffman // Small Wars Journal. 2009. March 02. URL: <http://smallwarsjournal.com/jrnl/art/further-thoughts-on-hybrid-threats> (дата обращения: 11.11.2020).
266. Hoffman F. G. Hybrid Warfare and Challenges / F. G. Hoffman// Joint Forces Quarterly. 2009. Issue 52. P. 34-39. URL: <http://smallwarsjournal.com/documents/jfqhoffman.pdf> (дата обращения: 11.11.2020)
267. Hudson V. 'Forced to Friendship?' (Mis-)Understandings of Soft Power and the Implications for Audience Attraction in Ukraine / V. Hudson // Politics. August 2015. Vol. 35, Issue 3. P. 330-346.
268. Huhtinen A-M. Disinformation in Hybrid Warfare: The Rhizomatic Speed of Social Media in the Spamosphere / A-M. Huhtinen, J. Rantapelkonen // Journal of Information Warfare. 2016. Vol. 15, No. 4. P. 50-67.
269. Hybrid Threats and Asymmetric Warfare: What to do? Stockholm 14-15 November, 2017 at the Swedish Defence University, Stockholm, Sweden. Conference proceeding / Ed. Karl Hickman et al. February 2018.

270. Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present / W. Murray, P.M. Mansoor (eds.). Cambridge: Cambridge University Press, 2012. 321 p.
271. Information Sharing in Military Operations / I. Goldenberg, J. Soeters, W. H. Dean (eds.). Springer International Publishing, 2017.
272. Information warfare. The pattern of aggression / I. Chifu, O. Nantoi (eds.). The Publishing House of the Institute of Political Sciences and International Relations "Ion I. C. Brătianu" of the Romanian Academy. Bucharest, 2016.
273. Jaitner M. Applying Principles of Reflexive Control in Information and Cyber / M. L. Jaitner, MAJ. H. Kantola // Journal of Information Warfare. 2016. Vol. 15. No. 4. P. 27-38.
274. Jaitner M. Russian Information Warfare of 2014 / M. Jaitner // 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace / M. Maybaum, A.-M. Osula, L. Lindström (Eds.). Tallinn. NATO CCD COE Publications, 2015. P. 39-52.
275. Jaitner M. L. Russian Information Warfare: Lessons from Ukraine / M. L. Jaitner // Chapter 10 in K. Geers (ed.). Russian Aggression against Ukraine. NATO CCD COE Publications, Tallinn: 2015. P. 87-94. URL: https://ccdcoe.org/uploads/2018/10/Ch10_CyberWarinPerspective_Jaitner.pdf (дата обращения: 11.11.2020)
276. Johnson R. Hybrid War and Its Countermeasures: A Critique of the Literature / R. Johnson // Small Wars & Insurgencies. 2018. Vol. 29, No. 1. P. 141-163.
277. Jones K. M. Cyber war: the next frontier for NATO. Master's Thesis / K. M. Jones // Monterey, California: Naval Postgraduate School. 2015-03. URL: <https://calhoun.nps.edu/handle/10945/45201> (дата обращения: 11.11.2020)
278. Joyner J. Competing Transatlantic Visions of Cybersecurity / J. Joiner // Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World Book / D. S. Reveron (ed.). Georgetown University Press. 2012. P. 159-172. URL: <http://www.jstor.org/stable/j.ctt2tt6rz.14> (дата обращения: 11.11.2020)

279. Jurczyszyn L. Russia's Attempts to Influence the Presidential Election in France / L. Jurczyszyn // The Polish Institute of International Affairs, Bulletin. 28 February 2017. No. 20 (960). 2 p. URL: https://pism.pl/publications/Russia_s_Attempts_to_Influence_the_Presidential_Election_in_France (дата обращения: 11.11.2020)
280. Kari M. Russia: A Cyber Fortress Besieged / M. Kari, R. Kuusisto // Proceedings of the 16th European Conference on Cyber Warfare and Security. 2017. P. 593-602.
281. Keatinga V. Ch. Conservative soft power: liberal soft power bias and the 'hidden' attraction of Russia / V. Ch. Keatinga, K. Kaczmarek // Journal of International Relations and Development. 2017. Vol. 22, No. 2. P. 1-27.
282. Kempf O. L'indirection de la guerre ou le retour de la guerre limitée / O. Kempf // Politique étrangère. 2015. No. 4. P. 157-169.
283. Khaldarova I. Fake News. The narrative battle over the Ukrainian conflict / I. Khaldarova, M. Pantti // Journalism Practice. June 2016. Volume 10, Issue 7. P. 891-901.
284. Kilinskas K. Hybrid Warfare: an Orientating or Misleading Concept in Analysing Russia's Military Actions in Ukraine? / K. Kilinskas // Lithuanian Annual Strategic Review. 2015-2016. Vol. 14. P. 139-159.
285. Kiseleva Y. Russia's Soft Power Discourse: Identity, Status and the Attraction of Power / Y. Kiseleva // Politics. 2015. Vol. 35, No. 3-4. P. 316-329.
286. Kofman M. A Closer look at Russia's "Hybrid War" / M. Kofman, M. Rojansky // Kennan Cable. April 2015. No. 7. URL: https://www.files.ethz.ch/isn/190090/5-KENNAN_CABLE-ROJANSKY_KOFMAN.pdf (дата обращения: 11.11.2020)
287. Kofman M. Russian hybrid warfare and other dark arts / M. Kofman // War on the rocks. 2016. 11 March. URL: <https://warontherocks.com/2016/03/russian-hybrid-warfare-and-other-dark-arts/> (дата обращения: 11.11.2020)
288. Kollars N. Defending Forward: The 2018 Cyber Strategy Is Here / N. Kollars, J. Schneider // War on the rocks. September 20, 2018. URL:

- <https://warontherocks.com/2018/09/defending-forward-the-2018-cyber-strategy-is-here/> (дата обращения: 11.11.2020)
289. Korybko A. Hybrid wars: the indirect adaptive approach to regime change/ A. Korybko. Moscow: Peoples' Friendship University of Russia, 2015. 132 p.
 290. Kostyuk N. Hacking Power Grids: New Tactic of War or Wave of the Future? / N. Kostyuk // Russia Matters. 3 November 2017. URL: <https://www.russiamatters.org/analysis/hacking-power-grids-new-tactic-war-or-wave-future> (дата обращения: 11.11.2020)
 291. Kostyuk N. Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? / N. Kostyuk, Y. M. Zhukov // Journal of Conflict Resolution. 2019. Vol. 63, No. 2. P.317-347.
 292. Kozlowski A. Comparative analysis of cyberattacks on estonia, georgia and kyrgyzstan / Andrzej Kozlowski // European Scientific Journal. February 2014. Special edition. Vol. 3, P. 237–245.
 293. Kragh M. Russia's strategy for influence through public diplomacy and active measures: the Swedish case / M. Kragh, S. Åsberg // Journal of Strategic Studies. 2017. Vol. 40, Issue 6. P. 773-816.
 294. Kruk K. Analyzing the Ground Zero. What Western Countries Can Learn from Ukrainian Experience of Combating Russian Disinformation / K. Kruk // European Values Kremlin Watch Report. 11.12.2017. 24 p. URL: <https://www.europeanvalues.net/wp-content/uploads/2017/12/Analyzing-the-Ground-Zero..pdf> (дата обращения: 11.11.2020)
 295. Laasme H. The Role of Estonia in Developing NATO's Cyber Strategy / H. Laasme // CICERO Foundation. Great Debate Paper. December 2012. No. 12/08. 59 p. (P. 11.) URL: https://www.cicerofoundation.org/wp-content/uploads/Laasme_-Estonia_NATO_Cyber_-Strategy.pdf (дата обращения: 11.11.2020)
 296. Lankina T. 'Russian Spring' or 'Spring Betrayal'? The Media as a Mirror of Putin's Evolving Strategy in Ukraine / T. Lankina, K. Watanabe // Europe-Asia Studies. 2017. Vol. 69, No. 10. P. 1526-1556.

297. Lanoszka A. Disinformation in international politics / A. Lanoszka // *European Journal of International Security*. 2019. Vol. 4, No. 2. P. 227-248.
298. Lanoszka A. Russian hybrid warfare and extended deterrence in eastern Europe / A. Lanoszka // *International Affairs*. 2016/ Vol. 92, No. 1. P. 175-195.
299. Laruelle M. L'idéologie comme instrument du soft power russe. Succès, échecs et incertitudes / M. Laruelle // *Hérodote*. 2017/3 (N° 166-167). P. 23-35.
300. Limonier K. Guerre hybride russe dans le cyberspace / K. Limonier, C. Gérard // *Hérodote*. 2017/3. N° 166-167. P. 145-163.
301. Limonier K. La stratégie d'influence informationnelle et numérique de la Russie en Europe / K. Limonier, M. Audinet // *Hérodote*. 2017/1. No. 164. P. 123-144.
302. Lucas E. Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe / E. Lucas, P. Pomeranzen // *A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. August 2016. 70 p.
303. Lucas E. Winning the Information War. Techniques and Counter-strategies to Russian Propaganda in Central and Eastern Europe / E. Lucas and P. Pomeranzen // *A Report by CEPA's Information Warfare Project in Partnership with the Legatum Institute*. August 2016. 70 p. URL: <https://li.com/wp-content/uploads/2016/08/winning-the-information-war-full-report-pdf.pdf> (дата обращения: 11.11.2020)
304. Lupion M. The Gray War of Our Time: Information Warfare and the Kremlin's Weaponization of Russian-Language Digital News / M. Lupion // *The Journal of Slavic Military Studies*. Vol. 31, No. 3. P. 329-353. URL: <https://doi.org/10.1080/13518046.2018.1487208> (дата обращения: 11.11.2020)
305. Makarychev A. Hard Questions About Soft Power: A Normative Outlook at Russia's Foreign Policy / A. Makarychev // *DGAPanalyse*. 2011. No. 10. 7 p. URL: https://dgap.org/system/files/article_pdfs/2011-10_DGAPanakt_Makarychev_www.pdf (дата обращения: 11.11.2020)
306. Matlock Jr. J. F. Amid 'Russiagate' Hysteria, What Are the Facts? We must end this Russophobic insanity / J. F. Matlock Jr. // *The Nation*. 2018. 1 June. URL:

- <https://www.thenation.com/article/archive/amid-russiagate-hysteria-what-are-the-facts/> (дата обращения: 11.11.2020)
307. Mattis J. Future Warfare: The Rise of Hybrid Wars / James N. Mattis, Frank Hoffman // U.S. Naval Institute, Proceedings Magazine. November 2005, Vol. 132, No. 11. P. 30-32.
 308. Maurer T. Cyber Proxies and Their Implications for Liberal Democracies / T. Maurer // The Washington Quarterly. 2018. Vol. 41, No. 2. P. 171-188.
 309. McDermott R. N. Does Russia Have a Gerasimov Doctrine? / R. N. MaDermott // Parameters. Spring 2016. Vol. 46, No. 1. P. 97-106. URL: <http://www.worldinwar.eu/wp-content/uploads/2017/09/30894f4e5f758d946bbdde0850e9ac4e86f-GERASIMOV-UP.pdf> (дата обращения: 11.11.2020)
 310. Mecklin J. Introduction: The evolving threat of hybrid war / J. Mecklin // Bulletin of the Atomic Scientists. 2017. Vol. 73, No. 5. P. 298-299. URL: <https://doi.org/10.1080/00963402.2017.1362905> (дата обращения: 11.11.2020)
 311. Minasyan S. “Hybrid” vs. “Compound” War. Lessons from the ukraine conflict / S. Minasyan // PONAS Eurasia policy memo. November 2015. No. 401. URL: https://www.ponarseurasia.org/sites/default/files/policy-memos-pdf/Peprm401_Minasyan_Nov2015.pdf (дата обращения: 11.11.2020)
 312. Mölder H. Information Warfare as the Hobbesian Concept of Modern Times – The Principles, Techniques, and Tools of Russian Information Operations in the Donbass / H. Mölder, V. Sazonov // The Journal of Slavic Military Studies. 2018. Vol. 31, No. 3. P. 308-328.
 313. Mulford J. P. Non-State Actors in the Russo-Ukrainian War / J. P. Mulford // Connections. Spring 2016. Vol. 15, No. 2. P. 89-107.
 314. Munteanu R. Hybrid warfare – the new form of conflict at the beginning of the century / R. Munteanu // Strategic Impact. 2015. No. 3. P. 19-25.
 315. McIntosh S. E. International Institutions, and the Russian People: Three Aspects of Russia’s Current Information Campaign in Ukraine / S. E. McIntosh // Journal of Slavic Military Studies. 2015. No. 28. P. 299–306.

316. NATO's Response to Hybrid Treats / G. Lasconjarias, J. A. Larsen (eds.) // NATO Defense colledge, 2015. URL: https://www.files.ethz.ch/isn/195405/fp_24.pdf (дата обращения: 11.11.2020)
317. Nelson E. Measuring RT's Impact on YouTube / E. Nelson, R. Orttung, A. Livshen // Russian analytical digest. 8 December 2015. No. 177. 14 p. URL: <https://www.files.ethz.ch/isn/195347/RussianAnalyticalDigest177.pdf> (дата обращения: 11.11.2020)
318. Nemeth W. J. Future war and Chechnya : a case for hybrid warfare / W. J. Nemeth // Naval Postgraduate School, Mmonterrey, CA. June 2002. 88 p. URL: <https://calhoun.nps.edu/handle/10945/5865> (дата обращения: 11.11.2020)
319. Nimmo B. Sputnik: Propaganda in a New Orbit / B. Nimmo // Information Warfare Initiative. January 2016. Center for European Policy Analysis (CEPA). Paper No. 2. URL: <https://silo.tips/download/propaganda-in-a-new-orbit> (дата обращения: 11.11.2020)
320. Nocetti J. Géopolitique de la cyber-conflictualité / J. Nocetti // Politique étrangère. 2018. No. 2. P. 15-28.
321. Nygren G. Journalism in the Crossfire. Media coverage of the war in Ukraine in 2014 / G. Nygren, M. Glowacki, J. Hök et al. // Journalism Studies. 2018. Vol. 19, Issue 7. P. 1059-1078.
322. Nyst C. State-sponsored trolling. How Governments Are Deploying Disinformation as Part of Broader Digital Harassment Campaigns / C. Nyst, N. Monaco // Digital Intelligence. Institute for the Future. 2018. URL: https://www.iftf.org/fileadmin/user_upload/images/DigIntel/IFTF_State_sponsored_trolling_report.pdf (дата обращения: 11.11.2020)
323. Oğuz Ş. The new NATO: Prepared for Russian hybrid warfare? / Ş. Oğuz // Insight Turkey. 2016. Vol. 18. No. 4. P. 165-180.
324. Paavola J. Understanding the Trolling Phenomenon: The Automated Detection of Bots and Cyborgs in the Social Media / J. Paavola, T. Helo, H. Jalonen et al. // Journal of Information Warfare. 2016, Vol. 15, No. 4. P. 100-111.

325. Pasitselska O. Ukrainian crisis through the lens of Russian media: Construction of ideological discourse / O. Pasitselska // Discourse & Communication. 2017. Vol. 11, No. 6. P. 591-609.
326. Paul C. The Russian “Firehose of Falsehood” Propaganda Model. Why It Might Work and Options to Counter It / C. Paul and M. Matthews // Perspective – RAND Corporation. 2016. 16 p. URL: https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf (дата обращения: 11.11.2020)
327. P. Pernik // Hacks, leaks and disruptions – Russian cyber strategies / N. Popescu, S. Secriery (Eds.) // EU ISS Chaillot papers. 2018. No. 148. P. 53-64. URL: https://www.iss.europa.eu/sites/default/files/EUISSFiles/CP_148.pdf (дата обращения: 11.11.2020)
328. Polyakova A. The Future of Political Warfare: Russia, The West, and The Coming Age of Global Digital Competition / A. Polyakova, S. Boyer // Brookings – Robert Bosch Foundation Transatlantic Initiative. arch 2018. 24 p. URL: <https://www.brookings.edu/research/the-future-of-political-warfare-russia-the-west-and-the-coming-age-of-global-digital-competition/> (дата обращения: 11.11.2020)
329. Polyakova A. The Kremlin Trojan Horses. Russian Influence in Greece, Italy, and Spain. / A. Polyakova, M. Kounalakis, A. Klapsis et al. // Atlantic Council – Eurasia Center. November 2017. 36 p. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/the-kremlin-s-trojan-horses-2-0/> (дата обращения: 11.11.2020)
330. Pomerantsev P. The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. / P. Pomerantsev, M. Weiss // A Special Report presented by The Interpreter, a project of the Institute of Modern Russia. 44 p. URL: https://imrussia.org/media/pdf/Research/Michael_Weiss_and_Peter_Pomerantsev_The_Menace_of_Unreality.pdf (дата обращения: 11.11.2020)

331. Popescu N. Russia's Soft Power Ambitions. Centre for European Policy Studies. / N. Popescu // Policy Brief. 2006 October, No. 115. 4 p. URL: <http://aei.pitt.edu/11715/> (дата обращения: 11.11.2020)
332. Rácz A. Russia's Hybrid War in Ukraine. Breaking the Enemy's Ability to Resist / A. Rácz. The Finnish Institute of International Affairs. 2017. – 208 p.
333. Raik K. A New Era of EU-NATO Cooperation: How to Make the Best of a Marriage of Necessity / K. Raik, P. Järvenpää // International Centre for Defence and Security Report. Tallinn, 2017. 30 p. URL: https://icds.ee/wp-content/uploads/2018/ICDS_Report_A_New_Era_of_EU-NATO.pdf (дата обращения: 11.11.2020)
334. Raugh D. L. "Is the Hybrid Threat a True Threat?" / D. L. Raugh // Journal of Strategic Security. 2016, Vol. 9. No. 2. P. 1-13. URL: <http://dx.doi.org/10.5038/1944-0472.9.2.1507> , <https://scholarcommons.usf.edu/jss/vol9/iss2/2/> (дата обращения: 11.11.2020)
335. Rawnsley G. D. To Know Us is to Love Us: Public Diplomacy and International Broadcasting in Contemporary Russia and China / G. D. Rawnsley // Politics. 2015. Vol. 35, Issue 3-4. P. 273–286.
336. Renz B. Russia and 'hybrid warfare' / B. Renz // Contemporary Politics. 2016. Vol. 22, Issue 3: Russia, the West, and the Ukraine Crisis. P. 283-300.
337. Richards J. Cyber-War: The Anatomy of the Global Security Threat / J. Richards. Basingstoke: Palgrave Macmillan, 2014. 91 p.
338. Richet J.-L. Cybersecurity Policies and Strategies for Cyberwarfare Prevention / J.-L. Richet. GI Global. 2015. 496 p.
339. Ristolainen M. Should 'RuNet 2020' Be Taken Seriously? Contradictory Views about Cyber Security between Russia and the West / M. Ristolainen // Journal of Information Warfare. 2017. Vol. 16, No. 4. P. 113-131.
340. Robets J. Q. Maskirovka 2.0: Hybrid Threats, Hybrid Response / J. Q. Roberts // Joins Special Operations University. Center for Special Operations Study and Research. December 2015.

341. Robotrolling 2017/1. Report prepared by the NATO Strategic Communications Centre of Excellence. Riga, 2017. 6 p. URL: <https://www.stratcomcoe.org/robotrolling-20171> (дата обращения: 11.11.2020)
342. Roman N. Information wars: Eastern Ukraine military conflict coverage in the Russian, Ukrainian and U.S. newscasts / N. Roman, W. Wanta, I. Buniak // The International Communication Gazette. 2017. No. 79 (4). P. 357–378.
343. Rotaru V. Forced Attraction? How Russia is Instrumentalizing Its Soft Power Sources in the “Near Abroad”/ V. Rotaru // Problems of Post-Communism. 2018. Volume 65, Issue 1. P. 37-48.
344. Rühle M. NATO’s Response to Hybrid Threats / M. Rühle // National Institute for Public Policy Information Series. 4 November 2019. Issue No. 448. 6 p. URL: <https://www.nipp.org/wp-content/uploads/2019/11/IS-448.pdf> (дата обращения: 11.11.2020)
345. Rusnáková S. Russian New Art of Hybrid Warfare in Ukraine / S. Rusnáková // Slovak Journal of Political Sciences. 2017, Vol. 17, No. 3–4. P. 343-380.
346. Russel M. Russia's information war: Propaganda or counter-propaganda? / M. Russel // European Parliament. October 2016. URL: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589810/EPRS_BRI\(2016\)589810_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2016/589810/EPRS_BRI(2016)589810_EN.pdf) (дата обращения: 11.11.2020)
347. Russian Social Media Influence. Understanding Russian Propaganda in Eastern Europe / C. Helmus, E. Bodine-Baron, A. Radin et al. // RAND Corporation, 2018. 148 p. URL: https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2237/RAND_RR2237.pdf (дата обращения: 11.11.2020)
348. Rutland P. The limits of Russia’s ‘soft power’ / P. Rutland, A. Kazantsev // Journal of Political Power. 2016. Vol. 9, No. 3. P. 395-413.
349. Sadowski D. Beyond the “Hybrid” Threat: Asserting the Essential Unity of Warfare / D. Sadowski, J. Becker // Small Wars Journal. 2010. January 7. URL: <http://smallwarsjournal.com/blog/journal/docs-temp/344-sadowski-et.al.pdf> (дата обращения: 11.11.2020)

350. Sakwa R. Russian Neo-Revisionism / R. Sakwa // Russian Politics. 2019. Vol. 4, No. 1. P. 1-21.
351. Scheidt M. The European Union versus External Disinformation Campaigns in the Midst of Information Warfare: Ready for the Battle? / M. Scheidt // EU Diplomacy Paper. 2019. No. 1. 34 p. URL: https://www.coleurope.eu/system/tdf/research-paper/edp_1_2019_scheidt.pdf?file=1&type=node&id=51569&force= (дата обращения: 11.11.2020)
352. Schnauffer T. A. II. Redefining Hybrid Warfare: Russia's Non-linear War against the West. / T. A. Schnauffer II // Journal of Strategic Security. 2017. Vol. 10, No. 1. P. 17-31. URL: <http://scholarcommons.usf.edu/jss/vol10/iss1/3> (дата обращения: 11.11.2020)
353. Sergunin A. Understanding Russia's Soft Power Strategy / A. Sergunin, L. Karabeshkin // Politics. 2015. Vol 35, No. 3-4. P. 347–363.
354. Shakarian P. Introduction to Cyber-Warfare. A Multidisciplinary Approach / P. Shakarian, J. Shakarian, A. Ruef. Waltham: Elsevier Inc., 2013. 337 p.
355. Shakarian P. The 2008 Russian Cyber Campaign against Georgia / P. Shakarian // Military Review. November-December 2011. P. 62-68.
356. Shallcross N. J. Social Media and Information Operations in the 21st Century / N. J. Shallcross // Journal of Information Warfare. 2017. Vol. 16, No. 1. P. 1-12.
357. Sherr J. Russia: managing contradictions / J. Sherr // America and a Changed World: A Question of Leadership / R. Niblett (ed.). London: Chatham House/Wiley Blackwell, 2010. P. 162-184. URL: https://www.chathamhouse.org/sites/default/files/public/Research/Americas/us0510_sherr.pdf (дата обращения: 11.11.2020)
358. Sherr J. The Challenge of “Hybrid War” / J. Sherr // National Security and Defense. 2016. No. 9-10 (167-168). – Kiev: Razumkov Centre. 2016. P. 85-86. URL: http://razumkov.org.ua/uploads/journal/eng/NSD167-168_2016_eng.pdf (дата обращения: 11.11.2020)

359. Shuya M. Russian Cyber Aggression and the New Cold War / M. Shuya // Journal of Strategic Security. 2018. Vol. 11, No. 1. P. 1-18.
360. Simons G. Russian public diplomacy in the 21st century: Structure, means and message / G. Simons // Public Relations Review. 2014. Vol. 40, No. 3. P. 440-449.
361. Slobodchikoff M. O. Roots of Russian Soft Power: Rethinking Russian National Identity / M. O. Slobodchikoff, G. D. Davis // Сравнительная политика. 2017. Т. 8, № 2. С. 19-36.
362. Spiegel C. Securing Cyberspace: NATO's Cyber Defence Policy as A Security Dispositive. Master thesis / C. Spiegel. Utrecht University, 2017. 78 p. URL: <http://dspace.library.uu.nl/handle/1874/355079> (дата обращения: 11.11.2020)
363. Strategy of "Constrainment". Countering Russia's Challenge to the Democratic Order. / F.O. Hampson et al. // Atlantic Council. March 16, 2017. URL: <https://www.cigionline.org/publications/strategy-constrainment-countering-russias-challenge-democratic-order> (дата обращения: 11.11.2020)
364. Szostek J. Nothing Is True? The Credibility of News and Conflicting Narratives during "Information War" in Ukraine / J. Szostek // The International Journal of Press/Politics. 2018. Vol. 23 (1). P. 116-135.
365. Szostek J. The Power and Limits of Russia's Strategic Narrative in Ukraine: The Role of Linkage / J. Szostek // Perspectives of Politics. June 2017. Vol. 15, No. 2. P. 379-395.
366. Takacs D. Ukraine's deterrence failure: Lessons for the Baltic States / D. Takacs // Journal on Baltic Security. 2017. No. 3(1). P. 1–10.
367. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations / M. N. Schmitt (ed.). 2nd ed. Cambridge: Cambridge University Press, 2017. 598 p.
368. The Disinformation Report on Foreign Interference in the 2016 Election // Yonder. Dec 17, 2018. URL: <https://www.yonder-ai.com/resources/the-disinformation-report/> (дата обращения: 11.11.2020)
369. The fog of cyber defence / J. Rantapelkonen, M. Salminen (eds.) National Defence University. Department of Leadership and Military Pedagogy

- Publication. Series 2. Article Collection No. 10. Helsinki 2013. 236 p. URL : [https://www.cyberwar.nl/d/20130200_The Fog of Cyber Defence NDU 2013.pdf](https://www.cyberwar.nl/d/20130200_The_Fog_of_Cyber_Defence_NDU_2013.pdf) (дата обращения: 11.11.2020)
370. The IRA, Social Media and Political Polarization in the United States, 2012-2018 / Ph. N. Howard et al. // Computational Propaganda Research Project. University of Oxford. 46 p. URL: <https://www.documentcloud.org/documents/5631936-IRA-Report-17-Dec.html> (дата обращения: 11.11.2020)
371. The Kremlin Trojan Horses. Russian Influence in Greece, Italy, and Spain / A. Polyakova et al. Atlantic Council – Eurasia Center. November 2016. 36 p. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/kremlin-trojan-horses/> (дата обращения: 11.11.2020)
372. Thiele R. D. Hybrid Threats – And how to counter them / R. D. Thiele // ISPSW Strategy Series: Focus on Defense and International Security. Sep. 2016. Issue No. 448. URL: https://www.ispsw.com/wp-content/uploads/2016/09/448_Thiele_Oslo.pdf (дата обращения: 11.11.2020)
373. Thiele R. D. The New Colour of War – Hybrid Warfare and Partnerships / R. D. Thiele // ISPSW Strategy Series: Focus on Defense and International Security. Oct 2015. Issue No. 383.
374. Tikk E. International Cyber Incidents: Legal Considerations / E. Tikk, K. Kaska, L. Vihul // Tallinn: NATO Cyber Defence Centre of Excellence (CCD COE). 2010. 132 p.
375. Trenin D. Should we fear Russia? / D. Trenin. Polity, 2016. 144 p.
376. Tsygankov A. P. Putin’s “Global Hybrid War”: U.S. Experts, Russia, and the Atlantic Council / A. P. Tsygankov, P. A. Tsygankov, H. Gonzales // Russia in Global Affairs. 2021. Vol. 19, No. 1. P. 147-172.
377. Tsygankov A. P. Russia and America: The Asymmetric Rivalry / A. P. Tsygankov. London: Polity, 2019. 272 p.
378. Tsygankov A. P. The Dark Double. US Media, Russia, and the Politics of Values / A. P. Tsygankov. Oxford: Oxford University Press, 2019. 192 p.

379. Tsygankov A. P. The dark double: the American media perception of Russia as a neo-Soviet autocracy, 2008–2014 / A. P. Tsygankov // *Politics*. 2017. Vol. 37, No. 1. P. 19-35.
380. U.S. Comprehensive Strategy Toward Russia / James Jay Carafano (ed.) // Davis institute for national security and foreign policy. Special report No. 173. The Heritage Foundation. December 9, 2015. URL: <https://www.heritage.org/europe/report/us-comprehensive-strategy-toward-russia> (дата обращения: 11.11.2020)
381. Valeriano B. International Relations Theory and Cyber Security: Threats, Conflicts, and Ethics in an Emergent Domain / B. Valeriano, R. C. Maness // *The Oxford Handbook of International Political Theory* / Ch. Brown, R. Eckersley (eds.). Oxford: Oxford University Press, 2018. P. 259-272.
382. Valeriano B. Persistent Enemies and Cyberwar: Rivalry Relations in an Age of Information Warfare / B. Valeriano, R. Mannes // *Cyberspace and National Security. Threats, Opportunities, and Power in a Virtual World* / D. S. Reveron (ed.). Georgetown University Press, 2012. P. 139-158.
383. Van Epps G. Common Ground U.S. and NATO Engagement with Russia in the Cyber Domain / G. Van Epps // *Connections*. Fall 2013. Vol. 12, No. 4. P. 15-50. URL: <https://www.jstor.org/stable/26326340> (дата обращения: 11.11.2020)
384. Veljovski G. The danger of “hybrid warfare” from a sophisticated adversary: the Russian “hybridity” in the Ukrainian conflict / G. Veljovski, N. Taneski, M. Dojchinovski // *Defense & Security Analysis*. 2017. Vol. 33, Issue 4. P. 292-307.
385. Vilson M. The Europeanization of foreign policy in the face of the Russian disinformation war / M. Vilson // *Sõjateadlane* (Estonian Journal of Military Studies). 2016. Vol. 2. P. 114-140.
386. Waggson Ch. Normative Power Europe Caving In? EU under Pressure of Russian Information Warfare / Ch. Waggson, M. Hellman // *CMS*. 2018. Vol. 56, No. 5, pp. 1161–1177.

387. Watanabe K. Measuring news bias: Russia's official news agency ITAR-TASS' coverage of the Ukraine crisis / K. Watanabe // *European Journal of Communication*. 2017. Vol. 32, No. 3. P. 224-241.
388. Wehner M. Hacking, propaganda and electoral manipulation. Moscow's information war on the West / M. Wehner // *Eurozine*. 21 July 2017. URL: <https://www.eurozine.com/hacking-propaganda-and-electoral-manipulation-2/> (дата обращения: 11.11.2020)
389. Wilson A. *Ukraine Crisis: What It Means for the West* / A. Wilson. Yale University Press, 2014. 236 p.
390. Wilson J. L. Russia and China Respond to Soft Power: Interpretation and Readaptation of a Western Construct / J. L. Wilson // *Politics*. 2015. Vol. 35, No. 3-4. P. 287–300.
391. Wiśniewski J. Ukrainian crisis – example of a hybrid war (general lessons) / J. Wiśniewski // *Zeszyty Naukowe AON*. 2015. No. 4 (101). P. 175-187.
392. Wither J. K. Making Sense of Hybrid Warfare / J. K. Wither // *Connections*. Spring 2016. Vol. 15, No. 2. P. 73-87. URL: <https://www.jstor.org/stable/26326441> (дата обращения: 07.08.2018)
393. *Words and Wars: Ukraine facing Kremlin propaganda*. K.: KIC, 2017. 124 p. URL: https://issuu.com/internews-ukraine/docs/words_and_wars (дата обращения: 11.11.2020)
394. Yablokov I. Conspiracy Theories as a Russian Public Diplomacy Tool: The Case of Russia Today (RT) / I. Yablokov // *Polytics*. 2015. Vol. 35, No. 3-4. P. 301–315.
395. Zelenkauskaite A. “Information Warfare” and Online News Commenting: Analyzing Forces of Social Influence Through Location-Based Commenting User Typology / A. Zelenkauskaite, M. Balduccini // *Social Media + Society*. July 1, 2017. Vol. 3, Issue 3. URL: <https://journals.sagepub.com/doi/pdf/10.1177/2056305117718468> (дата обращения: 11.11.2020)

396. Zhabotynska S. New media and strategic narratives: the Dutch referendum on Ukraine – EU Association Agreement in Ukrainian and Russian Internet blogs / S. Zhabotynska, V. Velivchenko // *European Security*. 2019. Vol. 28, No. 3. P. 360-381.

Публикации в СМИ

397. Алиева Ю. NYT: Российские боты активизировались после стрельбы во Флориде / Ю. Алиева // *Русская служба Голоса Америки*. 20 Февраль, 2018. URL: <https://www.golos-ameriki.ru/a/russia-florida-shooting/4262034.html> (дата обращения: 11.11.2020)
398. Антироссийскую сеть планировалось создать на базе университета в Брюсселе // *РИА*. 24.11.2018. URL: <https://ria.ru/20181124/1533417894.html> (дата обращения: 11.11.2020)
399. Бабич Д. ЕС: против России не только "контрпропаганда", но и цензура / Д. Бабич // *Международная жизнь*. 8 июля 2015. URL: <https://interaffairs.ru/news/show/13448> (дата обращения: 11.11.2020)
400. Британские спецслужбы активизировали крупнейшую агентурную сеть под легендой "борьбы с российской дезинформацией" // *Околокремля*. 22.11.2018 URL: <https://okolokremlya.ru/content/5130> (дата обращения: 11.11.2020)
401. Британский МИД обвинил ГРУ в «неизбирательных и безрассудных» кибератаках // *РБК*. 04 окт 2018. URL: <https://www.rbc.ru/politics/04/10/2018/5bb568109a79475eb1173794?from=main> (дата обращения: 11.11.2020)
402. В Wikileaks заявили о российском следе во взломанной почте Макрона // *INTERFAX.RU*. 7 мая 2017. URL: <https://www.interfax.ru/world/561431> (дата обращения: 11.11.2020)
403. В Британии начали три новых расследования против RT // *Газета.ru*. 21.05.2018. URL:

- https://www.gazeta.ru/tech/news/2018/05/21/n_11559871.shtml (дата обращения: 11.11.2020);
404. Великобритания открыла три расследования против RT из-за нарушения принципа объективности // Новая газета. 21 мая 2018. URL: <https://www.novayagazeta.ru/news/2018/05/21/141845-velikobritaniya-otkryla-tri-rassledovaniya-protiv-rt-iz-za-narusheniya-printsipa-ob-ektivnosti> (дата обращения: 11.11.2020)
405. В Госдепартаменте заявили, что США выделили \$40 млн на борьбу с иностранной пропагандой // ТАСС. 30 окт 2018. URL: <https://tass.ru/mezhdunarodnaya-panorama/5739346> (дата обращения: 11.11.2020)
406. В ЕС задумались о новых санкциях из-за российских кибератак // Lenta.ru. 5 октября 2018. URL: <https://lenta.ru/news/2018/10/05/hacker/> (дата обращения: 11.11.2020)
407. В Латвии на три месяца ограничат трансляцию телеканала "Россия" // РИА Новости. 3 апреля 2014. URL: <https://ria.ru/20140403/1002422950.html> (дата обращения: 11.11.2020)
408. В Раду внесли законопроект о противодействии "государству-агрессору в информпространстве" // Страна.ua. 7 сентября 2018. URL: <https://strana.ua/news/160019-v-rade-zarehistrirovan-zakonoproekt-o-protivodejstvii-hosudarstvu-ahressoru-na-tv-.html> (дата обращения: 11.11.2020)
409. В США намерены принять меры против «российской дезинформации» в Македонии // Газета.ru. 08.08.2018. URL: https://www.gazeta.ru/politics/news/2018/08/08/n_11884033.shtml?updated (дата обращения: 11.11.2020)
410. В США обнаружили новую лазейку для российских троллей // Lenta.ru. 20 октября 2018. URL: <https://lenta.ru/news/2018/10/20/startup/> (дата обращения: 11.11.2020)

411. В США опубликовали доклад Мюллера // ТАСС. 18/19 апреля 2019 г. URL: <https://tass.ru/mezhdunarodnaya-panorama/6350715> (дата обращения: 11.11.2020)
412. В Украине происходит полноценная война XXI века, "гибридная" война, – Скипальский // 24 канал. 30.04.2014 URL: https://24tv.ua/ru/v_ukraine_proishodit_polnotsennaya_voyna_xxi_veka_gibridnaya_voyna_skipalskiy_n437989 (дата обращения: 11.11.2020)
413. В Швейцарии задержали двух российских хакеров за попытку атаки на лабораторию WADA // Страна.ua. 24 октября 2018. URL: <https://strana.ua/news/167771-v-shvejtsarii-zaderzhali-dvukh-hrazhdan-rf-podozreniju-v-planirovanii-khakerskoj-ataki-na-laboratoriju-wada.html> (дата обращения: 11.11.2020)
414. Великобритания начала семь расследований против RT за необъективное освещение «дела Скрипаля» // Новая газета. 18 апреля 2018. URL: <https://www.novayagazeta.ru/news/2018/04/18/141080-velikobritaniya-nachala-sem-rassledovaniy-protiv-rt-za-neob-ektivnoe-osveschenie-dela-skripalya> (дата обращения: 11.11.2020)
415. Вендик Ю. Кремлевская пропаганда и тщетность борьбы с ней / Ю. Вендик // BBC News. Русская служба. 30 ноября 2016. URL: <https://www.bbc.com/russian/features-38145898> (дата обращения: 11.11.2020)
416. Вендик Ю. Польша: всем странам ЕС нужно бороться с российской пропагандой / Ю. Вендик // BBC News. Русская служба. 12 декабря 2017. URL: <https://www.bbc.com/russian/features-42316849> (дата обращения: 11.11.2020)
417. Венкина Е. Facebook создаст сайт для отслеживания российской пропаганды / Е. Венкина // DW. 23.11.2017. URL: <https://www.dw.com/ru/facebook-создаст-сайт-для-отслеживания-российской-пропаганды/a-41493405> (дата обращения: 11.11.2020)
418. Власти Латвии заблокировали сайт Sputnik // Коммерсант. 29 марта 2016. URL: <https://www.kommersant.ru/doc/2950533> (дата обращения: 11.11.2020)

419. Гальперович Д. Европа создала новый взб-сервис по разоблачению российской пропаганды / Д. Гальперович // Голос Америки. 14 сентября 2017. URL: <https://www.golos-ameriki.ru/a/eu-fights-disinformation-from-russia/4027827.html> (дата обращения: 11.11.2020)
420. Генерал Бридлав: План НАТО в Восточной Европе // Радио «Голос Америки». 2014. 15 сентября. URL: <https://www.golos-ameriki.ru/a/2450747.html> (дата обращения: 11.11.2020)
421. Герасимов С. Мир на гранях войны / С. Герасимов // Военно-промышленный курьер. 2017. 15 марта. URL: https://vpk.name/news/177000_mir_na_granyah_voiny.html (дата обращения: 11.11.2020)
422. Герасимов В. По опыту Сирии / В. Герасимов // Военно-промышленный курьер. 2016. 7 марта. URL: https://vpk.name/news/150974_po_opytu_sirii.html (дата обращения: 11.11.2020)
423. Герасимов В. Ценность науки в предвидении. Новые вызовы требуют переосмыслить формы и способы ведения боевых действий / В. Герасимов // Военно-промышленный курьер. 26 февраля 2013 URL: <http://www.vpk-news.ru/articles/14632> (дата обращения: 11.11.2020)
424. Герасюкова М. «Россию уже не остановить»: Америка ждёт атаку на выборы. Экс-менеджер Facebook Стамос заявил, что выборы в Конгресс обречены / М. Герасюкова // Газета.ru. 23.08.2018. URL: https://www.gazeta.ru/tech/2018/08/23/11920159/its_too_late.shtml (дата обращения: 11.11.2020)
425. Германия присоединилась к обвинениям США в адрес России // Lenta.ru. 5 октября 2018. URL: <https://lenta.ru/news/2018/10/05/they2/> (дата обращения: 11.11.2020)
426. Госдеп: борьба с "деятельностью РФ в Европе" является приоритетом бюджета на 2020 год. Ведомство рассчитывает получить на эти цели \$661

- млн. // ТАСС. 11 мар 2019. URL: <https://tass.ru/mezhdunarodnaya-panorama/6207314> (дата обращения: 11.11.2020)
427. Демидова О. Google намерен фильтровать российскую пропаганду. Интернет-гигант Google работает над техническим решением, с помощью которого будет понижаться ранжирование сайтов RT и Sputnik / О. Демидова // DW. 21.11.2017. URL: <https://www.dw.com/ru/google-намерен-фильтровать-российскую-пропаганду/a-41461675> (дата обращения: 11.11.2020)
428. Добровольский В. Могерини: ЕС работает над ответом на "пропаганду" на русском языке / В. Добровольский // РИА Новости. 6 марта 2016. URL: <https://ria.ru/20150306/1051245164.html?in=t> (дата обращения: 11.11.2020)
429. Дудина Г. Война до победного словца. Кто и как борется в Европе с «российской пропагандой» / Г. Дудина // Коммерсант. 23 августа 2015. URL: <https://www.kommersant.ru/doc/2795055> (дата обращения: 11.11.2020)
430. Ёлкина А. Общественное ТВ на русском: мост между общинами в Эстонии? / А. Ёлкина // Deutsche Welle. 26 ноября 2015. URL: <https://www.dw.com/ru/общественное-тв-на-русском-мост-между-общинами-в-эстонии/a-18875503> (дата обращения: 11.11.2020)
431. Ерёмина Д. Макрон назвал RT и Sputnik инструментами влияния и пропаганды / Д. Ерёмина // DW. 29.05.2017. URL: <https://www.dw.com/ru/макрон-назвал-rt-и-sputnik-инструментами-влияния-и-пропаганды/a-39035271> (дата обращения: 11.11.2020)
432. Захаров Р. Польша и Великобритания объединятся в борьбе с «российской пропагандой» / Звезда, 21.12.2017. URL: https://tvzvezda.ru/news/vstrane_i_mire/content/201712211613-j3uu.htm (дата обращения: 11.11.2020)
433. Заявление Представителя ОБСЕ по вопросам свободы СМИ о пропаганде во время конфликта // ОБСЕ. 15 апреля 2014 г. URL: <https://www.osce.org/ru/fom/117734> (дата обращения: 11.11.2020)

434. Идеон А. Wikileaks: Эстония отделалась легко / А. Идеон // ИНОСМИ. 11.12.2010. URL: <https://inosmi.ru/baltic/20101211/164825182.html> (дата обращения: 11.11.2020)
435. Как Россию обвиняли во вмешательстве в американские выборы. Досье // ТАСС. 31.10.2017. URL: <https://tass.ru/info/4324773> (дата обращения: 11.11.2020)
436. Коваль И. Как Европарламент решал, что делать с российской пропагандой / И. Коваль // Deutsche Welle. 23 ноября 2016. URL: <https://www.dw.com/ru/как-европарламент-решал-что-делать-с-российской-пропагандой/a-36487561> (дата обращения: 11.11.2020)
437. Козловский В. Если не мы — то кто? Американский суд не внял доводам компании Евгения Пригожина / В. Козловский // Новая газета. 18 ноября 2018. URL: <https://www.novayagazeta.ru/articles/2018/11/18/78631-esli-ne-my-to-kto> (дата обращения: 11.11.2020)
438. Контрпропагандистская группа ЕС выявила за два года свыше 3 тыс. случаев дезинформации от русскоязычных СМИ – Могерини // Интерфакс-Украина. 2 октября 2017. URL: <https://interfax.com.ua/news/general/452361.html> (дата обращения: 11.11.2020)
439. Корниенко С. Пиджак рвётся по шву / С. Корниенко // Радио Свобода. 26.04.2014 URL: <https://www.svoboda.org/a/25362031.html> (дата обращения: 11.11.2020)
440. Кошкин П. А. Пять проблем современной публичной дипломатии и как их решать / П.А. Кошкин // РСМД. 1 июля 2018. URL: <https://russiancouncil.ru/analytics-and-comments/analytics/pyat-problem-sovremennoy-publichnoy-diplomatii-i-kak-ikh-reshat/> (дата обращения: 11.11.2020)
441. Крылов А. В борьбе с «российской пропагандой» Европа становится жертвой собственных СМИ / А. Крылов // Взгляд. 13 декабря 2017. URL: <https://vz.ru/politics/2017/12/13/899464.html> (дата обращения: 11.11.2020)

442. Кулькова О. Как Британия собирается «наказать» Россию? / О. Кулькова // РСМД. 1 октября 2018. URL: http://russiancouncil.ru/analytics-and-comments/analytics/kak-britaniya-sobiraetsya-nakazat-rossiyu/?sphrase_id=20895665 (дата обращения: 11.11.2020)
443. Латвийская соцсеть подверглась кибератаке в день выборов в парламент страны // ТАСС. 6 октября 2018. URL: <https://tass.ru/mezhdunarodnaya-panorama/5645523> (дата обращения: 11.11.2020)
444. Лёвочкин С. Украинский кризис мировой безопасности / С. Лёвочкин // Зеркало недели. 2014. 16 мая. URL: <https://zn.ua/article/print/internal/ukrainskiy-krizis-mirovoy-bezopasnosti-.html> (дата обращения: 11.11.2020)
445. Лукаш Вуйчик (Łukasz Wójcik). Украинская гибридная война // Иносми. 15.05.2014. URL: <https://inosmi.ru/sngbaltia/20140515/220303215.html> (дата обращения: 11.11.2020)
446. Люда и тролли: Как петербурженка борется с «фабрикой кремлеботов» Петербурженка Людмила Савчук судится с «фабрикой троллей» на улице Савушкина. The Village узнал, как живёт женщина, решившая сломать систему пропаганды// The Village. 11 июня 2015. URL: <https://www.the-village.ru/village/city/situation/216161-fabrika-trolley> (дата обращения: 11.11.2020)
447. Маргарита Симоньян сообщила о начале расследования в отношении RT полицией Австралии // Новая газета. 17 июля 2018. URL: <https://www.novayagazeta.ru/news/2018/07/17/143396-margarita-simonyan-soobschila-o-nachale-rassledovaniya-v-otnoshenii-rt-politsiey-avstralii> (дата обращения: 11.11.2020)
448. Медведева Н. В Британии депутаты создали спецгруппу для борьбы с влиянием РФ / Н. Медведева // Ліга.Новости. 20.04.2018. URL: <https://news.liga.net/world/news/v-britanii-deputaty-sozdali-spetsgruppu-dlya-borby-s-vliyaniem-rf> (дата обращения: 11.11.2020)

449. МИД увидел подтекст в задержании российского журналиста в США // Lenta.ru. 11 ноября 2018. URL: <https://lenta.ru/news/2018/11/11/predlog/> (дата обращения: 11.11.2020)
450. Минеева Ю. Сбитый Sputnik. Россия и Британия продолжают медийную гибридную войну / Ю. Минеева // Новая газета. 29 декабря 2018. URL: <https://www.novayagazeta.ru/articles/2018/12/29/79098-sbityy-sputnik> (дата обращения: 11.11.2020)
451. Министр обороны Нидерландов заявила о кибервойне с Россией // Газета.ру. 14 октября 2018. URL: <https://www.gazeta.ru/army/news/2018/10/14/12167533.shtml> (дата обращения: 11.11.2020)
452. Минюст США предъявил обвинения семерым россиянам // РБК. 4 октября 2018. URL: <https://www.rbc.ru/politics/04/10/2018/5bb615fd9a7947871ec01702> (дата обращения: 11.11.2020)
453. Мисник Л. «Вводите санкции»: на Западе испугались «Машу и Медведя» / Л. Мисник // Газета.ру. 17.11.2018. URL: https://www.gazeta.ru/culture/2018/11/17/a_12062767.shtml (дата обращения: 11.11.2020)
454. Нападения на журналистов в Украине должны быть прекращены, сказала Представитель ОБСЕ по вопросам свободы СМИ и выразила готовность посетить Киев // ОБСЕ. 22 января 2014 г. URL: <https://www.osce.org/ru/fom/110465> (дата обращения: 11.11.2020)
455. Нельсон Дж. Информация превращается в оружие / Дж. Нельсон // ИноСМИ. 26 апреля 2015. URL: <https://inosmi.ru/world/20150426/227717819.html> (дата обращения: 11.11.2020)
456. Они все взломали. США и Нидерланды представили отчеты о причастности офицеров военной разведки России к хакерским атакам // Фонтанка.ру.

- 04.10.2018. URL: <https://www.fontanka.ru/2018/10/04/101/?ref=t> (дата обращения: 11.11.2020)
457. ООН призывают усерднее бороться с кремлевской пропагандой // Ліга.Новости. 10.05.2018. URL: <https://news.liga.net/politics/news/oon-prizvali-prilojit-usiliya-k-borbe-s-rossiyskoj-propagandoy> (дата обращения: 11.11.2020)
458. Парламент Франции рассмотрел меры по борьбе с «манипулированием информацией» // RFI. 07/06/2018. URL: <http://www.rfi.fr/ru/frantsiya/20180607-parlament-frantsii-rassmotrel-mery-po-borbe-s-manipulirovaniem-informatsiei> (дата обращения: 11.11.2020)
459. Почепцов Г. Гибридная война в головах и на экране / Г. Почепцов // «Хвиля», 17.05.2018, URL: <http://hvylya.net/analytics/politics/gibridnaya-golova-v-golovah-i-na-ekrane.html> (дата обращения: 11.11.2020)
460. Православие объявлено главной угрозой для Украины // E-News. 17.06.2014. URL: <https://e-news.su/info/14562-pravoslavie-obyavleno-glavnoy-ugrozoy-dlya-ukrainy.html> (дата обращения: 11.11.2020)
461. Пудовкин Е. Евросоюз борется с "российским влиянием". Британский министр поднимет тему пропаганды социальных сетях в ходе визита в Москву / Е. Пудовкин // Независимая газета. 27 ноября 2017. URL: http://www.ng.ru/world/2017-11-27/6_7123_eurosouz.html (дата обращения: 11.11.2020)
462. Пудовкин Е. Миллионы на борьбу с российской пропагандой. Госдеп и Пентагон придумали, как противостоять иностранной дезинформации / Е. Пудовкин // Независимая газета. 27.02.2018. URL: http://www.ng.ru/world/2018-02-27/1_7181_propaganda.html (дата обращения: 11.11.2020)
463. Путин назвал причину ухудшения российско-американских отношений // Известия. 17 июля 2018. URL: <https://iz.ru/767662/2018-07-17/putin-nazval-prichinu-ukhudsheniia-rossiisko-amerikanskikh-otnoshenii> (дата обращения: 11.11.2020)

464. Российских троллей заподозрили в манипулировании американским обществом // Lenta.ru. 26 августа 2018. URL: <https://lenta.ru/news/2018/08/26/trolls/> (дата обращения: 11.11.2020)
465. Российское посольство в США возмутилось давлением на партнера Sputnik // Новая газета. 11 января 2018. URL: <https://www.novayagazeta.ru/news/2018/01/11/138531-rossiyskoe-posolstvo-v-ssha-vozmutilos-davleniem-na-partnera-sputnik> (дата обращения: 11.11.2020)
466. Россию заподозрили в создании помех НАТО // Lenta.ru. 9 ноября 2018. URL: https://lenta.ru/news/2018/11/09/trident_juncture/ (дата обращения: 11.11.2020)
467. Россию официально обвинили во взломе системы GPS во время учений НАТО // Lenta.ru 13 ноября 2018. URL: https://lenta.ru/news/2018/11/13/gps_nato/ (дата обращения: 11.11.2020)
468. Россия – "главная угроза": в Литве опубликовали доклад спецслужб // Sputnik. 2 февраля 2019. URL: <https://lt.sputniknews.ru/politics/20190205/8264040/Rossiya--glavnaya-ugroza-v-Litve-opublikovali-doklad-spetssluzhb.html> (дата обращения: 11.11.2020)
469. Россия и США находятся в состоянии гибридной войны. Это всерьез и надолго. Интервью Дмитрия Тренина // Новая газета. 2018. 1 октября. № 108. URL: <https://novayagazeta.ru/articles/2018/09/27/77969-rossiya-i-ssha-nahodyatsya-v-sostoyanii-gibridnoy-voyny-eto-vseriez-i-nadolgo> (дата обращения: 11.11.2020)
470. Россиян уличили в запугивании американцев прививками // Lenta.ru. 24 августа 2018. URL: <https://lenta.ru/news/2018/08/24/trolls/> (дата обращения: 11.11.2020)
471. Россиянку обвинили во вмешательстве в выборы США 2018 года // Lenta.ru. 19 октября 2018. URL: <https://lenta.ru/news/2018/10/19/onemore/> (дата обращения: 11.11.2020)
472. Рубченко М. Трамп обхитрил сенаторов. Что это значит для России / М. Рубченко // РИА. 13.09.2018. URL:

- https://ria.ru/economy/20180913/1528464933.html?utm_source=smi2obmen&utm_medium=banner&utm_campaign=rian_partners (дата обращения: 11.11.2020)
473. Сафронов Ю. «Несоблюдение норм честности»: за что телеканалу RT вынесли предписание во Франции / Ю. Сафронов // Новая газета. 29 июня 2018. URL: <https://www.novayagazeta.ru/news/2018/06/29/142900-nesoblyudenie-norm-chestnosti-za-chto-telekanalu-rt-vynesli-predpisanie-vo-frantsii> (дата обращения: 11.11.2020)
474. Сафронов Ю. 50 оттенков подрывной деятельности. Франция собирается бороться с российской пропагандой, Москва обвиняет ее в цензуре / Ю. Сафронов // Новая газета. 06 сентября 2018. URL: <https://www.novayagazeta.ru/articles/2018/09/06/77731-50-ottenkov-podryvnoy-deyatelnosti> (дата обращения: 11.11.2020)
475. Сафронов Ю. Макрон примет закон против иностранной пропаганды / Ю. Сафронов // Новая газета. 4 января 2018. URL: <https://www.novayagazeta.ru/articles/2018/01/04/75074-makron-primet-zakon-protiv-inostrannoy-propagandy> (дата обращения: 11.11.2020)
476. Свиридов В. Секретная британская 77-я бригада орудует на Украине? / В. Свиридов // Звезда. 7 декабря 2018. URL: <https://zvezdaweekly.ru/news/t/20181261330-nlqd7.html> (дата обращения: 11.11.2020)
477. Симоньян сообщила о регистрации RT в качестве иностранного агента в США // Новая газета. 13 ноября 2017. URL: <https://www.novayagazeta.ru/news/2017/11/13/136972-simonyan-soobschila-o-registratsii-rt-v-kachestve-inostrannogo-agenta-v-ssha> (дата обращения: 11.11.2020)
478. Скрыпач И. Британия пришла на украинский рынок «борьбы с российской пропагандой» ради «слабеющего» Порошенко / И. Скрыпач // Экономика сегодня. 27 Июня 2018. URL: <https://rueconomics.ru/334749-britaniya-prishla->

- na-ukrainskii-rynok-borby-s-rossiiskoi-propagandoi-radi-slabeyushego-poroshenko (дата обращения: 11.11.2020)
479. Смирнов В. «Игра окончена»: опубликован доклад Мюллера о «российском вмешательстве» / В. Смирнов, А. Лушникова // RT. 18 апреля 2019 г. URL: <https://russian.rt.com/world/article/622799-rossiiskoe-vmeshatelstvo-vybory-prezident-ssha> (дата обращения: 11.11.2020)
480. США выдвинули обвинения в адрес хакеров из войсковой части ГРУ, ранее засвеченной в расследовании The Insider // The Insider. 13 июля 2018. URL: <https://theins.ru/news/109925> (дата обращения: 11.11.2020)
481. США выделяют \$40 млн на борьбу с дезинформацией // Ліга.Новости. 27.02.2018. URL: https://news.liga.net/world/news/ssha_vydelyat_40 mln na borbu s dezinformatsiey (дата обращения: 11.11.2020)
482. США выделяют 40 млн. долларов на борьбу с дезинформацией // DW. 27.02.2018. URL: <https://www.dw.com/ru/сша-выделят-40-млн-долларов-на-борьбу-с-дезинформацией/a-42752523-0> (дата обращения: 11.11.2020)
483. США и Британия выпустили предупреждение о российской киберугрозе // Ліга.Новости. 17.04.2018. URL: <https://news.liga.net/world/news/ssha-i-britaniya-vypustili-preduprejdenie-o-rossiyskoy-kiberugroze> (дата обращения: 11.11.2020)
484. США подкинут странам Балтии \$100 миллионов на борьбу с российской пропагандой. // Наш город – новости Даугавпилса. 21 марта 2020 г. URL: <http://www.gorod.lv/novosti/288554-ministr-oborony-litvy-poradoval-ssha-podkinut-stranam-baltii-100-millionov-na-borbu-s-rossiiskoi-propagandoi> (дата обращения: 11.11.2020)
485. США создают информационные войска в Турции: мишень – Россия // Военно-политическая аналитика. 14 июня 2016. URL: <http://vpoanalytics.com/2016/06/14/ssha-sozdayut-informacionnye-vojska-v-turcii-mishen-rossiya/> (дата обращения: 11.11.2020)

486. Транслятор «Радио Спутник» зарегистрировался в качестве иноагента в США // Новая газета. 17 ноября 2017. URL: <https://novayagazeta.ru/news/2017/11/17/137122-translyator-radio-sputnik-zaregistrirovalsya-v-kachestve-inoagenta-v-ssha> (дата обращения: 11.11.2020)
487. Турция стала второй страной после Латвии, которая заблокировала сайт российского информационного агентства Sputnik // Роскомсвобода. 15 апреля 2016. URL: <https://roskomsvoboda.org/16149/> (дата обращения: 11.11.2020)
488. Фахрутдинов Р. «Заминируем Севастополь»: что придумали британские чиновники. Хакеры Anonymous выложили новые данные по Integrity Initiative / Р. Фахрутдинов // Газета.ru. 15.12.2018. URL: https://www.gazeta.ru/tech/2018/12/15_a_12095869.shtml?updated (дата обращения: 11.11.2020)
489. Фахрутдинов Р. «Макрон вместо свободы слова защищает багет». Корреспондента RT France не пустили в Елисейский дворец / Р. Фахрутдинов. // Газета.ru. 15.01.2018. URL: <https://www.gazeta.ru/social/2018/01/15/11614082.shtml> (дата обращения: 11.11.2020)
490. Фахрутдинов Р. «Срывайте уроки в школе»: британцы раскрыли «план Кремля» / Р. Фахрутдинов // Газета.ru. 06.10.2018. URL: https://www.gazeta.ru/tech/2018/10/06_a_12010915.shtml?updated (дата обращения: 11.11.2020)
491. Фененко А.В. Новая мобилизация? / А.В. Фененко // РСМД. 2018. 26 июля. URL: <http://russiancouncil.ru/analytics-and-comments/analytics/novaya-mobilizatsiya/> (дата обращения: 16.10.2018)
492. Французские власти не нашли следов атаки хакеров из РФ на штаб Макрона // Интерфакс. 1 июня 2017. URL: <https://www.interfax.ru/world/564892> (дата обращения: 11.11.2020)

493. Чен А. Агентство / А. Чен // The New York Times Magazine. 4 June 2015.
URL: <https://www.nytimes.com/2015/06/07/magazine/the-agency-russian.html>
(дата обращения: 11.11.2010)
494. Червоненко В. Как Украина проиграла референдум в Нидерландах / В. Червоненко // BBC. Русская служба. 7 апреля 2016. URL: https://www.bbc.com/russian/international/2016/04/160407_netherlands_ukraine_loss (дата обращения: 11.11.2020)
495. Чехия обвинила Россию в кибератаках на МИД // Коммерсант. 3.12.2018.
URL: <https://www.kommersant.ru/doc/3819587> (дата обращения: 11.11.2020)
496. Шакиров О. «Российская пропаганда»: в соцсетях, в Восточной Европе, далее везде. / О. Шакиров // РСМД. 24 июля 2018.
497. Шаталин В. В Чехии начинают борьбу с российской пропагандой / В. Шаталин // Deutsche Welle. 21 октября 2016. URL: <https://www.dw.com/ru/в-чехии-начинают-борьбу-с-российской-пропагандой/a-36108805> (дата обращения: 11.11.2020)
498. Эйдман И. Кремль уже создал в Европе «Путин-Интерн» / И. Эйдман // Ліга.нет. 01.09.2017. URL: <https://www.liga.net/politics/opinion/kreml-uzhe-sozdal-v-evrope-putin-intern> (дата обращения: 11.11.2020)
499. Экс-генерал СБУ рассказал о «гибридной войне» и украинских олигархах // РИА. 30.04.2014. URL: <https://ria.ru/world/20140430/1006101683.html#ixzz30QtUV51P> (дата обращения: 11.11.2020)
500. Ahmed A. Sh. Obama To Receive A Report On Russia's 2016 Election Meddling Before Leaving Office / A. Sh. Ahmed // Huffpost. Dec 09, 2016. URL: https://www.huffpost.com/entry/obama-report-election-meddling-russia_n_584ad081e4b0e05aded380ff (дата обращения: 11.11.2020)
501. Alex Aiken introduces the Rapid Response Unit. – Government Communication Service. 19 July 2018. URL: <https://webarchive.nationalarchives.gov.uk/20200203104056/https://gcs.civilser>

- [vice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/](https://www.vice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/) (дата обращения: 11.11.2020)
502. Belaïch Ch. «Période de réserve»»: de quoi peut-on parler ce week-end? / Ch. Belaïch // Libération. Apr. 21, 2017. URL: https://www.liberation.fr/politiques/2017/04/21/periode-de-reserve-de-quoi-peut-on-parler-ce-week-end_1564254 (дата обращения: 11.11.2020)
503. Birnbaum M. Sweden is taking on Russian meddling ahead of fall elections. The White House might take note / M. Birnbaum // The Washington Post. 22 February 2018. URL: https://www.washingtonpost.com/world/europe/sweden-looks-at-russias-electoral-interference-in-the-us-and-takes-steps-not-to-be-another-victim/2018/02/21/9e58ee48-0768-11e8-aa61-f3391373867e_story.html (accessed 11.11.2020)
504. Blackwill R. Containing Russia, Again. An Adversary Attacked the United States—It's Time to Respond / R. D. Blackwill, Ph. H. Gordon. // Foreign Affairs. January 18, 2018. URL: <https://www.foreignaffairs.com/articles/russian-federation/2018-01-18/containing-russia-again> (дата обращения: 11.11.2020)
505. Blakely R. Russian accounts fuel French outrage online / R. Blakely // The Times. December 08, 2018. URL: <https://www.thetimes.co.uk/article/russian-accounts-fuel-protesters-outrage-online-xx2f2g8th> (дата обращения: 11.11.2020)
506. Bolzen S. “Die Nato muss auf grüne Männchen vorbereitet sein”. Interview mit Nato-Oberbefehlshaber Philip Breedlove / S. Bolzen // Die Welt. 2014. 17 August. URL: <https://www.welt.de/politik/ausland/article131296429/Die-Nato-muss-auf-gruene-Maennchen-vorbereitet-sein.html> (дата обращения: 11.11.2020)
507. British army to create a unit against Russian propaganda // Voltaire Network. 6 February 2018. URL: <https://www.voltairenet.org/article199602.html> (дата обращения: 11.11.2020)
508. Candau M. MEPs bare teeth in debate over Russian propaganda / M. Candau // EurActiv. 23 January 2018. URL: <https://www.euractiv.com/section/justice->

- home-affairs/news/meps-bear-teeth-in-debate-over-russian-propaganda/ (дата обращения: 11.11.2020)
509. Chalfant M. Denmark, Sweden team up to counter Russian 'fake news' / M. Chalfant // The Hill. 31 August 2017. URL: <https://thehill.com/policy/cybersecurity/348693-denmark-sweden-team-up-to-counter-russian-fake-news> (дата обращения: 11.11.2020)
510. Chesney R. The Law of Military Cyber Operations and the New NDAA / R. Chesney // Lawfare. July 26, 2018. URL: <https://www.lawfareblog.com/law-military-cyber-operations-and-new-ndaa> (дата обращения: 11.11.2020)
511. Coalson R. Russian Disinformation 2.0: Sowing chaos, confusion, and anger in the west / R. Coalson // Radio Free Europe/RadioLiberty. URL: https://internetfreedom.io/rferl_russian-disinformation.html (дата обращения: 11.11.2020)
512. Coughlin C. Russia poses greater threat to Britain than Isil, says new Army chief / C. Coughlin // The Telegraph. 23 November 2018. URL: <https://www.telegraph.co.uk/news/2018/11/23/russia-poses-greater-threat-britain-isil-says-new-army-chief/> (дата обращения: 11.11.2020)
513. Dempsey J. The Kremlin's clampdown on the media and sophisticated propaganda machine are giving the European Endowment for Democracy a new sense of focus / J. Dempsey // Carnegie Europe. 16 March 2015. URL: <https://carnegieeurope.eu/strategieurope/?fa=59377> (дата обращения: 11.11.2020)
514. Emmott R. NATO looks to combat Russia's 'information weapon': document / R. Emmott // Reuters. 27 January 2016. URL: <https://www.reuters.com/article/us-nato-reform-idUSKCN0V51RU> (дата обращения: 11.11.2020)
515. Facebook открывает офис в Риге, где модераторы будут искать язык ненависти на русском // Страна.ua. 21 декабря 2018. URL: <https://strana.ua/news/177824-facebook-otkryvaet-ofis-v-rihe-hde-moderatory-budut-iskat-jazyk-nenavisti-na-russkom.html> (дата обращения: 11.11.2020)

516. Facebook удалил связанные с Россией и Ираном страницы // Газета.ru / 22.08.2018/ URL: https://www.gazeta.ru/tech/news/2018/08/22/n_11933911.shtml (дата обращения: 11.11.2020)
517. Facebook удалила несколько сотен страниц из-за связи с Россией // Газета.ru. 17.01.2019. URL: https://www.gazeta.ru/tech/news/2019/01/17/n_12530875.shtml (дата обращения: 11.11.2020)
518. Galeotti M. 'The 'Gerasimov doctrine' and Russian Non-Linear War'. / M. Galeotti // In Moscow's shadows. 2014. 6 July. URL: <https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/> (дата обращения: 11.11.2020)
519. Galeotti M. I'm Sorry for Creating the 'Gerasimov Doctrine' / M Galeotti // Foreign Policy. 2018. 5 March. URL: <https://foreignpolicy.com/2018/03/05/im-sorry-for-creating-the-gerasimov-doctrine/> (дата обращения: 11.11.2020)
520. Hybrid Warfare And Russia's New 'Great Game' // RadioFreeEurope/RadioLiberty. 27.06.2014. URL : <https://www.rferl.org/a/podcast-hybrid-warfare-and-russias-new-great-game-russia-ukraine/25437993.html> (дата обращения: 11.11.2020)
521. Integrity Initiative. Начало // Окологремля. 23.11.2018. URL: <https://okolokremlya.ru/content/5133> (дата обращения: 11.11.2020)
522. Justice Dept. charges Russian woman with interference in midterm elections / M.Zapotosky et al. // The Washington Post. Oct. 19, 2018. URL: https://www.washingtonpost.com/world/national-security/director-of-national-intelligence-warns-of-ongoing-campaigns-to-interfere-with-elections/2018/10/19/64973a7a-d3b4-11e8-b2d2-f397227b43f0_story.html?utm_term=.413f385d43b5&noredirect=on (дата обращения: 11.11.2020)
523. Landler M. NATO Chief Warns of Duplicity by Putin on Ukraine / M. Landler, M. Gordon // The New York Times. 2014. 8 July. URL:

- https://www.nytimes.com/2014/07/09/world/europe/nato-chief-warns-of-duplicity-by-putin-on-ukraine.html?_r=0 (дата обращения: 11.11.2020)
524. Lithuania 'already under attack' - President Grybauskaitė // BBC News. 6 March 2015. URL: <https://www.bbc.com/news/av/world-europe-31773941/lithuania-already-under-attack-president-grybauskaitė> (дата обращения: 11.11.2020)
525. Maksimovic M. EU officials warn of 'underestimating' Russian propaganda in Balkans / M. Maksimovic // Deutsche Welle. 14 November 2017. URL: <https://www.dw.com/en/eu-officials-warn-of-underestimating-russian-propaganda-in-balkans/a-41371020> (дата обращения: 11.11.2020)
526. Matlack C. France to Probe Possible Russian Influence on Yellow Vest Riots / C. Matlack, R. Williams // Bloomberg. 8 декабря 2018. URL: <https://www.bloomberg.com/news/articles/2018-12-08/pro-russia-social-media-takes-aim-at-macron-as-yellow-vests-rage> (дата обращения: 11.11.2020)
527. Mccann K. Britain to launch counter-propaganda war against Russia as Theresa May unveils 'Fusion Doctrine' defence plan / K. Mccann // The Telegraph. 28 March 2018. URL <https://www.telegraph.co.uk/politics/2018/03/27/britain-launch-counter-propaganda-war-against-russia-theresa/> (дата обращения: 11.11.2020)
528. Microsoft: под прицелом русских хакеров были все кандидаты на выборах во Франции // Газета.ru. 21.08.2018. URL: https://www.gazeta.ru/tech/news/2018/08/21/n_11933131.shtml (дата обращения: 11.11.2020)
529. Microsoft: русские хакеры атакуют весь политический спектр // Газета.ru. 21.08.2018. URL: https://www.gazeta.ru/tech/news/2018/08/21/n_11933191.shtml (дата обращения: 11.11.2020)
530. Miller C. Inside the British Army's secret information warfare machine / C. Miller // Wired. 14 November 2018. URL: <https://www.wired.co.uk/article/inside-the-77th-brigade-britains-information-warfare-military> (дата обращения: 11.11.2020)

531. Nalyvaichenko: Russia making 'hybrid war' against Ukraine // Kyiv Post. 14.07.2014. URL: <https://www.kyivpost.com/article/content/war-against-ukraine/nalyvaichenko-russia-making-hybrid-war-against-ukraine-351866.html> (дата обращения: 01.07.2020)
532. O'Sullivan D. Russians sought to recruit 'assets' through social media, Senate told / D. O'Sullivan // CNN. Business. December 17, 2018. URL: <https://edition.cnn.com/2018/12/17/tech/russia-2016-election-social-media-report/index.html> (дата обращения: 11.11.2020)
533. O'Neill P. H. NATO will establish new cyber command centers / P. H. O'Neill // Cyberscoop. 9 November 2017. URL: <https://www.cyberscoop.com/nato-cyber-command-centers/> (дата обращения: 11.11.2020)
534. Owen J. Government boosts national security comms capability to combat international threats / J. Owen // PRWeek. May 23, 2018. URL: <https://www.prweek.com/article/1465497/government-boosts-national-security-comms-capability-combat-international-threats> (дата обращения: 11.11.2020)
535. Panichi J. EU declares information war on Russia / J. Panichi // Politico. 27 August 2015. URL: <https://www.politico.eu/article/russia-propaganda-ukraine-eu-response-disinformation/> (дата обращения: 11.11.2020)
536. Panichi J. EU Splits in Russian media war / J. Panichi // Politico. 17 September 2015. URL: <https://www.politico.eu/article/eu-russia-propaganda-kremlin-media/> (дата обращения: 11.11.2020)
537. Parubiy says Russia's 'hybrid war' against Ukraine shows need to reform defense sector, NATO ready to help. // Kyiv Post. 20.05.2014. URL: <https://www.kyivpost.com/article/content/war-against-ukraine/parubiy-says-russias-hybrid-war-against-ukraine-shows-need-to-reform-defense-sector-nato-ready-to-help-348538.html?cn-reloaded=1> (дата обращения: 1.07.2020)
538. Paul C. Confessions of a Hybrid Warfare Skeptic / C. Paul // Small Wars Journal. 16 mar 2016. URL : <https://smallwarsjournal.com/jrnl/art/confessions-of-a-hybrid-warfare-skeptic> (дата обращения: 11.11.2020)

539. Pomerantsev P. How Putin Is Reinventing Warfare / P. Pomerantsev // Foreign Policy. 2014, May 5. URL: <https://foreignpolicy.com/2014/05/05/how-putin-is-reinventing-warfare/> (дата обращения: 11.11.2020)
540. Poroshenko Should Remove Journalists from Kiev Blacklist // Sputnik International. 17 September 2015. URL: <https://sputniknews.com/society/201509171027130831/> (дата обращения: 11.11.2020)
541. Rettman A. Dutch-Polish 'content factory' to counter Russian propaganda / A. Rettman // EU Observer. 21 July 2015. URL: <https://euobserver.com/foreign/129724> (дата обращения: 11.11.2020)
542. Rettman A. EU drafts plan on Russia's media 'misuse' / A. Rettman // EUObserver. 23 June 2015. URL: <https://euobserver.com/foreign/129247> (дата обращения: 11.11.2020)
543. Rettman A. EU to strike back at Russian propaganda / A. Rettman // EU Observer. 19 March 2015. URL: <https://euobserver.com/foreign/128071> (дата обращения: 11.11.2020)
544. Rettman A. Poland hosts meeting on countering Russian propaganda / A. Rettman // EU Observer. 10 September 2015. URL: <https://euobserver.com/foreign/130192> (дата обращения: 11.11.2020)
545. Ricks Th. NATO's Little Noticed but Important New Aggressive Stance on Cyber Weapons / Th. Ricks // Foreign Policy. 7 December 2017. URL: <https://foreignpolicy.com/2017/12/07/natos-little-noticed-but-important-new-aggressive-stance-on-cyber-weapons/> (дата обращения: 11.11.2020)
546. Robertson A. Hillary Clinton says 'lives are at risk' because of fake news / A. Robertson // The Verge. 8 December 2016. URL: <https://www.theverge.com/2016/12/8/13893000/hillary-clinton-pizzagate-fake-news-lives-at-risk> (дата обращения: 11.11.2020)
547. Robinson M. Beyond Integrity Initiative: The Scale of UKGOV Counter Disinformation / M. Robinson // UKCOLUMN. 7th February 2019. URL:

- <https://www.ukcolumn.org/article/beyond-integrity-initiative-scale-ukgov-counter-disinformation> (дата обращения: 11.11.2020)
548. Rogers, Comey say no evidence vote tallies were changed in 2016 election // The Washington Post. March 20, 2017. URL: https://www.washingtonpost.com/video/national/rogers-comey-say-no-evidence-vote-tallies-were-changed-in-2016-election/2017/03/20/9a764e16-0d8f-11e7-aa57-2ca1b05c41b8_video.html?noredirect=on&utm_term=.b8d09aeeceb9 (дата обращения: 11.11.2020)
549. Severin I. Putin's use of chemical weapons in hybrid war against Ukraine / I. Severin // UAObserver. 29.04.2014. URL: <http://www.uaobserver.com/2014/04/putins-use-of-chemical-weapons-in-his.html> (дата обращения: 11.11.2020)
550. Sheth S. A new report found that Russia's disinformation operation in the US picked up speed even after it was caught by Mueller / S. Sheth // Business Insider. Dec 17, 2018. URL: <https://www.businessinsider.com/new-knowledge-oxford-reports-russia-disinformation-campaign-senate-intelligence-committee-2018-12> (дата обращения: 11.11.2020)
551. Shynkarenko O. Russia's Hybrid War in Ukraine / Oleg Shynkarenko // IWPR. 11.06.2014. URL: <https://iwpr.net/global-voices/russias-hybrid-war-ukraine> (дата обращения: 11.11.2020)
552. Sky News: Британия собирает наступательные кибервойска для противодействия России // Газета.ru. 21.09.2018. URL: https://www.gazeta.ru/tech/news/2018/09/21/n_12065293.shtml (дата обращения: 11.11.2020)
553. Standish D. Why Is Finland Able to Fend Off Putin's Information War? / D. Standish // Foreign Policy. 1 March 2017. URL: <https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/> (дата обращения: 11.11.2020)

554. Stavridis J. U.S. Needs a Global Alliance Against Russia's Cyberattacks. Washington can coordinate with Europe, the UN, Interpol and nongovernmental groups / J. Stavridis // Bloomberg. 11 октября 2018. URL: <https://www.bloomberg.com/opinion/articles/2018-10-11/u-s-needs-a-global-alliance-against-russia-s-cyberattacks> (дата обращения: 11.11.2020)
555. Sternstein A. The Pentagon Wants To Expand Its Cyber Forces / A. Sternstein // Defense One. 4 February 2015. URL: <https://www.defenseone.com/technology/2015/02/pentagon-wants-expand-its-cyber-forces/104613/> (дата обращения: 11.11.2020)
556. Stolton S. EU Commission hits out at Facebook's disinformation report / S. Stolton // EurActiv. 30 January 2019. URL: <https://www.euractiv.com/section/data-protection/news/facebook-singled-out-in-eu-disinformation-report/> (дата обращения: 11.11.2020)
557. Stolton S. EU raps Facebook, Twitter and Google for inaction on fake news / S. Stolton // EurActiv. 1 March 2019. URL: <https://www.euractiv.com/section/digital/news/eu-wraps-facebook-twitter-and-google-for-inaction-on-fake-news/> (дата обращения: 11.11.2020)
558. Stubbs J. Russia's RT America registers as 'foreign agent' in U.S. / J. Stubbs, G. Gibson // Reuters. November 13, 2017. URL: <https://www.reuters.com/article/us-russia-usa-media-restrictions-rt/russias-rt-america-registers-as-foreign-agent-in-u-s-idUSKBN1DD25B> (дата обращения: 11.11.2020)
559. Stupp C. EU plans aid to prosecute hackers and support member states / C. Stupp // EurActiv. 24 October 2017. URL: <https://www.euractiv.com/section/cybersecurity/news/eu-plans-aid-to-prosecute-hackers-and-support-member-states/> (дата обращения: 11.11.2020)
560. Tamkin E. 10 Years After the Landmark Attack on Estonia, Is the World Better Prepared for Cyber Threats? / E. Tamkin // Foreign Policy. 2017. 27 April. URL: <https://foreignpolicy.com/2017/04/27/10-years-after-the-landmark-attack-on->

- [estonia-is-the-world-better-prepared-for-cyber-threats/](#) (дата обращения: 11.11.2020)
561. Timberg C. Effort to combat foreign propaganda advances in Congress / C. Timberg // The Washington Post. 30 November 2016. URL: [https://www.washingtonpost.com/business/economy/effort-to-combat-foreign-propaganda-advances-in-congress/2016/11/30/9147e1ac-e221-47be-ab92-9f2f7e69d452_story.html](#) (дата обращения: 11.11.2020)
562. Tucker P. The US Is Losing at Influence Warfare. Here's Why // Defense One. 5 December 2016. URL: [https://www.defenseone.com/threats/2016/12/us-losing-influence-warfare-heres-why/133654/](#) (дата обращения: 11.11.2020)
563. U.S. Senators Seek New Center To Counter Russian, Chinese 'Propaganda' // Radio Free Europe / Radio Liberty. 16 March 2016. URL: [https://www.rferl.org/a/us-senators-seek-to-counter-russia-china-propaganda/27617521.html](#) (дата обращения: 11.11.2020)
564. U.S. to Spend \$500,000 Training Baltic Journalists to Counter Russian Propaganda // The Moscow Times. 10 August 2015. URL: [https://www.themoscowtimes.com/2015/08/10/us-to-spend-500000-training-baltic-journalists-to-counter-russian-propaganda-a48855](#) (дата обращения: 11.11.2020)
565. Ukrainian support for EU association agreement declines // Deutsche Welle. 13 July 2013. URL: [https://www.dw.com/en/ukrainian-support-for-eu-association-agreement-declines/a-17189085](#) (дата обращения: 11.11.2020)
566. Weiss M. The Baltic elves taking on pro-Russian trolls/ M. Weiss // The Daily Beast. 2016, 21 March. URL: [https://www.thedailybeast.com/the-baltic-elves-taking-on-pro-russian-trolls](#) (дата обращения: 11.11.2020)
567. Wójcik L. Ukraińska wojna hybrydowa / L. Wójcik // Polityka. 13.05.2014. [https://www.polityka.pl/tygodnikpolityka/swiat/1579805,1,ukrainska-wojna-hybrydowa.read](#) (дата обращения: 11.11.2020)

Електронні ресурси

568. Гибридная война – гибридная ответная реакция. // Вестник НАТО. 1.07.2014. URL: <https://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-crisis-war/RU/index.htm> (дата обращения: 11.11.2020)
569. Делегаты Генеральной Ассамблеи: развивая цифровые медиа, не надо забывать о традиционных СМИ // Новости ООН. 20 октября 2018. URL: <https://news.un.org/ru/story/2018/10/1341102> (дата обращения: 11.11.2020)
570. Манойло А. Гибридная война – плацдарм, где великие державы меряются силами. (Интервью агентству News-Front 2016-05-11) / А. Манойло. URL: <https://www.youtube.com/watch?v=0NnADariaqM> (дата обращения: 11.11.2020)
571. Операция «Монклоа» // Colonelcassad. 22.11.2018 URL: <https://colonelcassad.livejournal.com/4596438.html> (дата обращения: 11.11.2020)
572. Операция Integrity Initiative. // Colonelcassad. 30.11.2018. URL: <https://colonelcassad.livejournal.com/4612495.html> (дата обращения: 11.11.2020)
573. Россия, Украина и Крым: предсказуемый кризис? // Вестник НАТО. 1.07.2014. URL: <https://www.nato.int/docu/review/2014/Russia-Ukraine-Nato-crisis/Russia-Ukraine-Crimea-crisis/RU/index.htm> (дата обращения: 11.11.2020)
574. фон Лорингховен А. Ф. Адаптация разведки Североатлантического союза в поддержку «Единой НАТО» / А. Ф. фон Лорингховен // NATO Review. 8 сентября 2017. URL: <https://www.nato.int/docu/review/ru/articles/2017/09/08/adaptatsiya-razvedki-severoatlanticheskogo-soyuza-v-podderzoku-edinoj-nato/index.html> (дата обращения: 11.11.2020)
575. Яким шляхом іти Україні — до якого союзу приєднуватись? // Київський міжнародний інститут соціології. 3 жовтня 2013. URL:

- <http://www.kiis.com.ua/?lang=ukr&cat=reports&id=196&page=1&y=2013&m=10> , https://dif.org.ua/uploads/pdf/1407765948_3132.pdf (дата обращения: 11.11.2020)
576. 77th Brigade. Influence and Outreach // UK Ministry of Defense. URL: <https://www.army.mod.uk/who-we-are/formations-divisions-brigades/6th-united-kingdom-division/77-brigade/> (дата обращения: 11.11.2020)
577. Alex Aiken introduces the Rapid Response Unit. – Government Communication Service. 19 July 2018. URL: <https://webarchive.nationalarchives.gov.uk/20200203104056/https://gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/> (дата обращения: 11.11.2020)
578. Be aware of Russian and ISIS propaganda, warn foreign affairs MEPs // European Parliament. 10 October 2016. URL: <http://www.europarl.europa.eu/news/en/press-room/20161010IPR46530/be-aware-of-russian-and-isis-propaganda-warn-foreign-affairs-meps> (дата обращения: 11.11.2020)
579. Bringing Plurality & Balance to Russian Language Media - Final Recommendations // European Endowment for Democracy. 25 June 2015. URL: <https://www.democracyendowment.eu/en/news/551-bringing-plurality-balance-to-russian-language-media-final-recommendations.html> (дата обращения: 11.11.2020)
580. Commentary: Means, Goals and Consequences of the Pro-Kremlin Disinformation Campaign // EUvsDisInfo. 19 January 2017. URL: <https://euvsdisinfo.eu/commentary-means-goals-and-consequences-of-the-pro-kremlin-disinformation-campaign/> (дата обращения: 11.11.2020)
581. Countering propaganda: NATO spearheads use of behavioural change science // NATO Strategic Communications Centre of Excellence. 12 May 2015. URL: <https://stratcomcoe.org/countering-propaganda-nato-spearheads-use-behavioural-change-science> (дата обращения: 11.11.2020)

582. Cyber Capacity Building Task Force // EU ISS. 26 March 2018. URL: <https://www.iss.europa.eu/content/cyber-capacity-building-task-force-0> (дата обращения: 11.11.2020)
583. Denmark And Sweden: "Russian Fake News Is A Danger To Our Countries" // EUvsDisInfo. 1 September 2017. URL: <https://euvsdisinfo.eu/denmark-and-sweden-russian-fake-news-is-a-danger-to-our-countries/> (дата обращения: 11.11.2020)
584. Emerson J. B. Exposing Russian Disinformation // Atlantic Council UkraineAlert Blog. 29 June 2015. URL: <https://www.atlanticcouncil.org/blogs/ukrainealert/exposing-russian-disinformation> (дата обращения: 11.11.2020)
585. Fried D. Democratic Defense Against Disinformation. / D. Fried, A. Polyakova // Atlantic Council – Eurasia Center. February 2018. URL: <https://www.atlanticcouncil.org/in-depth-research-reports/report/democratic-defense-against-disinformation/> (дата обращения: 11.11.2020)
586. Funke D. A guide to anti-misinformation actions around the world / D. Funke, D. Flamini // Poynter. 2018. URL: <https://www.poynter.org/ifcn/anti-misinformation-actions/#france> (дата обращения: 11.11.2020)
587. Galeotti M. Controlling Chaos: How Russia Manages Its Political War in Europe / M. Galeotti // European Council on Foreign Relations Brief. August 2017. URL: https://ecfr.eu/wp-content/uploads/ECFR228 - CONTROLLING_CHAOS1.pdf (дата обращения: 11.11.2020)
588. Garraway A. Russian interference in UK politics and society / A. Garraway, B. Smith // Research Briefing. House of Commons Library. 19 December, 2017. URL: <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/CDP-2017-0255> (дата обращения: 11.11.2020)
589. Giles K. Countering Russian Information Operations in the Age of Social Media / K. Giles // Council on Foreign Relations Report. 21 November 2017. URL: <https://www.cfr.org/report/countering-russian-information-operations-age-social-media> (дата обращения: 11.11.2020)

590. Giles K. The Next Phase of Russian Information Warfare / K Giles // Prepared by the NATO Strategic Communications Centre of Excellence. 2015. URL: <https://www.stratcomcoe.org/next-phase-russian-information-warfare-keir-giles> (дата обращения: 11.11.2020)
591. Guerra híbrida: ¿una oportunidad para la colaboración OTAN-UE? // La Revista de la OTAN. URL : <https://www.nato.int/docu/review/2014/Also-in-2014/Deterring-hybrid-warfare/ES/index.htm> (дата обращения: 11.11.2020)
592. Hanlon B. Twitter Release Reveals the Kremlin's News Impersonation Game / B. Hanlon // Alliance for Securing Democracy. 21 June 2018. URL: <https://securingdemocracy.gmfus.org/twitter-release-reveals-the-kremlins-news-impersonation-game/> (дата обращения: 11.11.2020)
593. Hybrid threats and the EU. State of play and future progress // EU ISS Conference Report. 2-3 October 2017. URL: [https://www.iss.europa.eu/sites/default/files/EUISSFiles/EE hybrid event report.pdf](https://www.iss.europa.eu/sites/default/files/EUISSFiles/EE%20hybrid%20event%20report.pdf) (дата обращения: 11.11.2020)
594. Illarionov A. Speech by Mr. Andrei Illarionov at NATO Parliamentary Assembly. Committee on Economics and Security. 31 May 2014 / A. Illarionov // Livejournal.com. 11 июня 2014. URL: <https://aillarionov.livejournal.com/696630.html> (дата обращения: 11.11.2020)
595. Jordan J. Hybrid Warfare: A Catch-all Concept / J. Jordan // GESI Mosaic Blog. 2017. 17 October. URL: <https://global-strategy.org/hybrid-warfare-a-catch-all-concept/> (дата обращения: 11.11.2020)
596. Key Steps for Countering Russian Propaganda. A toolkit for journalists // Political Capital Institute. Budapest, March 2017. URL: https://www.stopfake.org/content/uploads/2017/05/Toolkit_RussianPropaganda_Journalists_170509.pdf (дата обращения: 11.11.2020)
597. Kochis D. Countering Russian Propaganda Abroad / D. Kochis // The Heritage Foundation. Issue Brief. No. 4286. 21 October 2014. 4 p. URL: <http://report.heritage.org/ib4286> (дата обращения: 11.11.2020)

598. Mijatovic D. Вовсе нет противоречия: <http://osce.org/ru/fom/116314> и <http://osce.org/ru/fom/116900> запрет ТВ каналов без законного основания – вот форма цензуры // Twitter. URL: https://twitter.com/Dunja_Mijatovic/status/449537285592477697 (дата обращения: 11.11.2020)
599. Moore D. Why We Are Unconvinced NATO's Cyber Policy Is More Aggressive, and That's a Good Thing / D. Moore // Council on Foreign Relations Blog. 6 February 2018. URL: <https://www.cfr.org/blog/why-we-are-unconvinced-natos-cyber-policy-more-aggressive-and-thats-good-thing> (дата обращения: 11.11.2020)
600. Rasmussen A. F. A NATO for a Dangerous World. Russian aggression has made it clear. We need an alliance that is fitter, faster and more flexible / A. F. Rasmussen, Ph. Breedlove // Wall Street Journal. 2014. 17 August. URL: <https://www.atlanticcouncil.org/blogs/natosource/a-nato-for-a-dangerous-world> (дата обращения: 11.11.2020)
601. Royce E. Countering Putin's Information Weapons of War / E. Royce // Wall Street Journal. 14 April 2015. URL: <https://www.wsj.com/articles/countering-putins-information-weapons-of-war-1429052323> (дата обращения: 11.11.2020)
602. Satter D. The Last Gasp of Empire: Russia's Attempts to Control the Media in the Former Soviet Republics / D. Satter // CIMA report. 8 January 2014. URL: https://www.cima.ned.org/wp-content/uploads/2015/02/CIMA-Russia-report_David_Satter.pdf (дата обращения: 11.11.2020)
603. Stamos A. An Update On Information Operations On Facebook / A. Stamos // Facebook. September 6, 2017. URL: <https://newsroom.fb.com/news/2017/09/information-operations-update/> (дата обращения: 11.11.2020)
604. Taylor M. L. Combating disinformation and foreign interference in democracies: Lessons from Europe / M. L. Taylor // Brookings Cybersecurity and Election Interference Series. 31 July 2019. URL: <https://www.brookings.edu/blog/techtank/2019/07/31/combating->

disinformation-and-foreign-interference-in-democracies-lessons-from-europe/

(дата обращения: 11.11.2020)