А.Э. ПОПАДЮК

ГИБРИДНАЯ ВОЙНА: ИНТЕРПРЕТАЦИЯ В РАМКАХ КОНЦЕПЦИИ ПОСТМОДЕРНИЗМА

Аннотация. *В статье предпринята попытка интерпретации феномена «гибридная война» в рамках концепции постмодернизма, предложенной И.А. Чихаревым. Представлены различные аспекты «гибридной войны» на основе сравнительного анализа зарубежной научной литературы. В качестве основных методов исследования, помимо общенаучных методов (анализ, синтез, индукция, дедукция) в работе применяется сравнительный подход, позволивший выявить сходства и различия между различными трактовками понятия «гибридная война», предложенными зарубежными экспертами, а также системный подход, позволивший рассмотреть ряд аспектов гибридной войны на основе классических понятий концепции постмодернизма: диффузия субъекта и симулятивность.*
Ключевые слова: *гибридная война, диффузия субъекта, симулятивность, постмодернизм, мировая политика.*

HYBRID WAR: INTERPRETATION WITHIN THE FRAMEWORK OF THE CONCEPT OF POSTMODERNISM

Abstract. *The article attempts to interpret the phenomenon of «hybrid war» within the framework of the concept of postmodernism proposed by I.A. Chikharev. Various aspects of the hybrid war are presented based on a comparative analysis of foreign scientific literature. In addition to general scientific methods (analysis, synthesis, induction, deduction), the present work used a comparative approach as the main research methods, which allowed us to identify similarities and differences between various interpretations of the concept of «hybrid war» proposed by foreign experts, as well as a systems approach, which allowed us to consider a number of aspects of hybrid war based on the classical concepts of the concept of postmodernism: diffusion of the subject and simulation.*
Keywords: *hybrid war, diffusion of the subject, simulation, postmodernism, world politics.*

Как в мире в целом, так и у границ нашего государства развивается ряд конфликтов. При этом определенный круг научного сообщества [2, с. 160–175; 6; 24] и некоторые СМИ [3; 4] относят часть из этих конфликтов

ПОПАДЮК Алла Эдуардовна – кандидат политических наук, старший преподаватель кафедры политологии факультета социальных наук и массовых коммуникаций Финансового университета при Правительстве Российской Федерации, г. Москва

к «гибридным». Несмотря на популярность этого термина, его общепринятая трактовка так и не выработана. Для анализа данного понятия за основу взята постмодернистская концепция И.А. Чихарева [7; 8], по мнению которого одно из основных свойств современных войн в общем и гибридных войн в частности — это «диффузия субъекта». Критическое осмысление представлений о субъекте является классическим для этого направления философии [5]. Диффузия субъекта преобразует конфликт и создает новые формы ее реализации. Гибридные войны становятся «деперсонализированными», а как следствие, конфликт данного типа превращается в «перманентный». Если нет субъекта, значит нет конкретных целей, как и нет конкретных «правил игры».

* * *

В частности, А. Хиншоу, А. Борбели и К. Красти описывают гибридную войну как киберпреступления, незаконное финансирование, шпионаж, слияния и поглощения, включая противоборствующих государственных субъектов, государственные похищения и незаконные задержания, где агрессор/нападающий (реальное лицо, принимающее решения) может быть неизвестен. Авторы выделяют две основные черты гибридной войны: нападающая сторона действует в тени и может даже не быть известна атакующему; объект воздействия, как правило, узнает в конце игры, что он является целью, и может даже не знать, кто является нападающим [17].

Гибридная война позволяет субъектам-агрессорам «оставаться в тени» или хуже того — выдавать себя за представителей гражданского общества. Так, по мнению Ф. Хоффмана, участниками гибридной войны являются не только национальные суверенные государства, но и негосударственные субъекты. Он определяет гибридную войну как военную стратегию, сочетающую обычную, нерегулярную тактику и кибервойну, терроризм и преступное поведение в пределах боевого пространства для достижения политических целей. Кроме того, Хоффман утверждает, что проблема заключается в вовлеченности государственных и негосударственных субъектов, скрывающихся среди гражданского населения, создавая транснациональную угрозу, которая должна быть высокоприоритетной областью обсуждения [17].

Н.Р. Хайдин описывает перманентность субъекта-агрессора гибридной войны. Она убеждена, что термин «гибридная война» был придуман для обозначения борьбы различных политических фракций внутри одного государства. Гибридная война воспринимается как сочетание обычных военных и нерегулярных вооруженных групп, таких как партизаны, повстанцы и террористы, с общей политической целью [16].

Ряд ученых полагает, что диффузия субъекта является причиной столь широкого круга технологий и методов ведения гибридной войны. Конфликт переносится в виртуальную или кибернетическую среду. Теперь в результате «гибридизации» конфликта взаимодействуют не люди, а, например, беспилотники. Так, С. Бахманн, Д. Паттер, Г. Дучински утверждают, что понятие

«гибридная война» включает в себя полный спектр различных режимов ведения войны, в том числе обычные возможности, террористические акты, неизбирательное насилие, принуждение и преступный беспорядок. По их мнению, гибридные войны могут вестись как государствами, так и различными негосударственными субъектами (с государственной поддержкой или без нее) [10].

Перманентный характер гибридной войны позволяет субъектам-агрессорам использовать разные сферы воздействия на «мишень». Гибридизация войны размывает представления о том, где война начнется и чем закончится. Профессор Базельского университета А. Петриг считает, что отличительной чертой гибридных войн является то, что они ведутся не только на суше, море и в воздухе, но и распространяются на информационную, кибер- и, что здесь важно, -правовую сферы. На ее взгляд, основная проблема заключается в том, что нет единой яркой линии, отделяющей мирное время от правового режима военного времени. Участники гибридной войны используют различные технологии, которые позволяют им оставаться на пороге между войной и миром, но при этом достигать своих конечных целей [22].

Деперсонификация войны снимает ответственность с агрессоров, уничтожает границу между понятиями «война» и «мир». Г. Бурцис рассматривает понятия «гибридная война» и «гибридные угрозы» как часть более обширного концепта «гибридный бизнес» — способность сочетать военные и гражданские, а также секретные и явные средства, направленные на создание двусмысленности между категориями «войны» и «мира», одновременно усиливая сомнения в этом вопросе. К понятию «гибридная война» автор относит ситуации, в которых акторы используют внутренние слабости государств с помощью невоенных средств [11].

Гибридная война — проявление бесконтактной войны. В современных условиях национальная безопасность страны может быть осуществлена только в условиях комплексных мер по защите государства. Так, А.Б. Москера и С.Д. Бахманн обращают внимание на использование закона как оружия (Lawfare), подчеркивая, что гибридная война берет свое начало в методах ведения войны прошлых конфликтов; она необязательно нова как категория конфликта, но при этом способна изменить будущее. Они утверждают, что гибридная война — это сочетание обычных и нетрадиционных методов войны, а также кинетических и некинетических средств в самых различных оперативных условиях. Данное понятие включает четыре существующих метода и категории войны: нерегулярная (например, терроризм и борьба с повстанцами), асимметричная (нетрадиционная война, такая как партизанская война), комбинированная (где нерегулярные силы используются против противника) и обычная война [21].

Бессубъектность противостояния поднимает актуальную проблему права в рамках гибридной войны. Современное состояние международных

отношений находится под угрозой, так как в наше время необходимость соблюдения наднациональных соглашений, канонов международного права, логика разоружения и многое другое теряют свою актуальность. Гибридная война позволяет оставаться агрессорам в «серой зоне» права, не нарушая порогов применения международных правовых норм.

Так, доцент университета Тарту (Эстония) Р. Вярк полагает, что понятие «гибридная война» представляет собой военные и невоенные меры нелинейным и дополнительным образом. Она подчеркивает, что различные средства и методы необязательно эффективны в отдельности, но именно их синергия приводит к желаемому результату. Вярк убеждена, что право также стало методом ведения войны. Так, государства намеренно используют правовые сложности для укрепления своих собственных позиций и подрыва позиций противников. Они могут пожелать сохранить интенсивность применяемых мер ниже порога «применения или угрозы силы», чтобы утверждать, что международное право не было нарушено и что противники не могут осуществлять самооборону [25].

«Неопределенность права» в гибридных войнах рассматривают С.Д. Бахманн и М. Джонс, трактующие гибридную войну как синтез из четырех существующих методов и категорий войны: терроризм, борьба с повстанцами, асимметричная и комбинированная войны, в которых используются регулярные и нерегулярные силы. Они указывают на элемент «правовой неопределенности» как следствие или цель гибридной войны, напоминающие о новой тенденции по созданию «серой зоны» [19].

* * *

Вторым свойством гибридной войны в рамках анализируемой идеи является симулятивность, относящаяся к ключевым классическим терминам постмодерна [1]. Другими словами, описательное поле в СМИ и реальное противостояние в гибридной войне обычно сильно разнятся. Кроме того, прямое противостояние, характерное классическим боевым действиям в гибридной войне, обычно подменяется противостоянием в виртуальном мире или даже киберпространстве.

М. Галеотти дает свою трактовку понятия «гибридная война» — это скрытая подрывная деятельность, дезинформация, кибератаки и различные незаконные способы сбора информации о противниках [15]. В свою очередь, С. Алкон и С. Кауфман, ссылаясь на данную трактовку, утверждают, что ряд возможных сценариев гибридной войны соответствует этому широкому определению [14]. Примерами здесь являются кибератаки, включающие требования выкупа за освобождение баз данных, замороженных вредоносным программным обеспечением [26]. Так, массовая атака программы-вымогателя на VMware ESXi в феврале 2023 года — яркий пример гибридной войны. На момент написания статьи во Франции было взломано более 900 серверов, а в США — около 400 [20].

Участник-агрессор не видит напрямую объект своего воздействия. Гибридная война использует кибератаки, информационные атаки и тому подобное. Таким образом, современный конфликт снимает необходимость в непосредственном соприкосновении участников противостояния. По мнению С. Алкон и С. Кауфман, гибридные военные атаки нацелены на такие ключевые общественные службы, как электро- или водоснабжение, или другие объекты муниципальной инфраструктуры [13; 23]. В 2019 году было совершено по меньшей мере 104 кибератаки с использованием программ-вымогателей на административные системы в школах и государственных учреждениях. Подобные действия выводят из строя ключевые сервисы и функции сети, поскольку хакеры, как правило, требуют крупный выкуп, как бы удерживая в заложниках правительственные учреждения или школы [13].

А.А. Ариди дает свое определение «гибридной войны», называя ее централизованно разработанной, координируемой и контролируемой войной, в которой используются скрытая и/или открытая тактика, военные и невоенные средства, обычная сила, экономическое давление, кибероперации, принудительные и подрывные методы, поддерживаемые повстанцами или используемые в качестве маскировки государственной агрессии под маской в том числе таких гуманитарных вмешательств, как, например, защита меньшинств [9].

Симуляционный характер гибридной войны может подменять основных участников конфликта посредниками в рамках прокси-войны. Х.С.Л. Кастро уверен, что победа на президентских выборах Жаира Болсонару в Бразилии в 2018 году является кризисом для страны и последствием гибридной войны. Он перечисляет ряд событий, которые, по его мнению, являются неотъемлемой частью такой войны. Например, демонстрации против повышения цен на проезд в городском транспорте в ряде городов под руководством «Движения за свободный проход» (MPL), — беспартийной по своей природе, но в целом прогрессивной организации со значительным участием сторонников тактики «черного блока», выступающей за уничтожение таких «капиталистических символов», как банки и магазины. В то же время в условиях чрезмерных репрессий со стороны полиции растет народное одобрение протестующих. Одновременно основные средства массовой информации, обычно освещавшие протесты как вандализм, начинают их воспринимать совершенно иначе, стремясь наложить на них печать консервативной повестки дня вроде борьбы с коррупцией. К акциям присоединяются и крайне правые группы, которые выступают с транспарантами и плакатами с просьбой о военном вмешательстве [12].

* * *

«Бессубъектность» гибридной войны формирует отсутствие организованной силы. Основными участниками могут быть военизированные группы, партизаны, бандформирования и так далее. Таким образом, гибридизация конфликта является проявлением «теневой стороны» глобализации,

а ее «перманентность» позволяет применить ряд новых инструментов и технологий гибридной войны. Как следствие, противостояние осуществляется в условиях многомерности пространства: экономические санкции, партизанские действия, демографические войны и так далее.

Отсутствие правил игры в гибридных войнах формирует «правовую неопределенность», субъекты-агрессоры осуществляют свои действия в так называемой «серой зоне», тем самым не оставляют возможности использовать международное право и традиционную самооборону [7; 8].

«Симуляция конфликта» как второе свойство рассматриваемой концепции указывает на проблему дифференциации информационного и реального поля в рамках противостояния в гибридной войне. В данном случае, «симуляция» актуализирует такие злободневные феномены как «фейковые новости» и «постправда», которые требуют отдельного обсуждения в научном сообществе.

Список литературы

1. Бодрийяр Ж. Прозрачность зла [Текст]: сб. эссе / Ж. Бодрийяр; пер. Л. Любарская, пер. Е. Марковская. М.: Добросвет, 2000. 258 с.
2. Евстафьев Д.Г., Манойло А.В. Гибридные войны в контексте постглобализации // Контуры глобальных трансформаций: политика, экономика, право. 2021. Т. 14. № 4. С. 160–175. DOI: 10.23932/2542-0240-2021-14-4-10.
3. Пашкова Л., Зыкина Т. Polskie Radio узнало о первых санкциях ЕС за «гибридные действия» России // РБК. 15 дек. 2024. URL: https://www.rbc.ru/politics/15/12/2024/675f1ebc9a7947416e98c943.
4. Строкань С. Гибридная война с Трампом // Коммерсантъ. 2019. 25 окт. № 196.
5. Фуко М. Слова и вещи. Археология гуманитарных наук // Прогресс. М. 1977.
6. Цыганков П.А. «Гибридные войны» в XXI веке: социальные и политические аспекты // Вестн. Моск. ун-та. Сер. 18. Социология и политология. 2015. № 4.
7. Чихарев И.А., Бровко В.Ю. Гибридная война: к проблеме политологической интерпретации // Вестн. Моск. ун-та. Сер. 12. Политические науки. 2020. № 5.
8. Чихарев И.А. «Гибридная война»: реконструкция vs. деконструкция / Материалы научного семинара «„Гибридные войны“ в мировой политике XXI века» (февраль 2015 г., факультет политологии МГУ имени М.В. Ломоносова) // ПОЛИТЭКС. 2015. Том 11. № 2.
9. Aridi A.A. How Hybrid Is Modern Warfare? // International Network of Doctoral Studies, 2017–5th International Conference of PhD Students and Young Researchers, How Deep Is Your Law? Brexit. Technologies. Modern Conflicts // Journal on Baltic Security 5(1): 17–26. April 27, 2017. DOI: 10.2478/jobs-2019-0002. URL: https://www.researchgate.net/publication/334967002_Hybrid_warfare_and_hybrid_threats_today_and_tomorrow_towards_an_analytical_framework.
10. Bachmann S.D., Putter D., Duczynski, G. Hybrid warfare and disinformation: A Ukraine war perspective. Global Policy, 00, 1–12. 2023. URL: https://www.globalpolicyjournal.com/articles/conflict-and-security/hybrid-warfare-and-disinformation-ukraine-war-perspective.

11. Bourtzis G. The Conduct of 'Hybrid Operations': Concept, Challenges and Application of The Rules of International Law on The Use of Force // University of Groningen Faculty of Law Research Paper. № 2. 2023. URL: https://www.researchgate.net/publication/349857107_The_Interpretation_and_Application_of_the_'Sphere_of_application_of_CISG'_Formation_and_Modification_of_CISG_Contracts_and_Fundamental_Breach_of_Obligations_of_CISG_Parties_and_their_Remedies_Some_Evi.
12. Castro J.C.L. Neoliberalismo, guerra híbrida e a campanha presidencial de 2018 (Neoliberalism, Hybrid Warfare and the 2018 Presidential Campaign) // CASTRO, J. C.L. Neoliberalismo, guerra híbrida e a campanha presidencial de Bolsonaro // Comunicação & Sociedade, São Bernardo do Campo (SP), v. 42, n. 1, p. 261–291, janeiro-abril de 2020. URL: https://www.researchgate.net/publication/351708948_Neoliberalismo_guerra_hibrida_e_a_campanha_presidencial_de_2018.
13. Cranley E. 8 cities that have been crippled by cyberattacks — and what they did to fight them // Business Insider. Jan 27, 2020. URL: https://www.businessinsider.com/cyberattacks-on-american-cities-responses-2020–1.
14. Cynthia A., Kaufman S. A Theory of Interests in the Context of Hybrid Warfare: It's Complex // Cardozo Journal of Conflict Resolution. July 1, 2023. Vol. 24, No. 3, 2023, Texas A&M University School of Law Legal Studies Research Paper No. 23–29. URL: https://ssrn.com/abstract=4541434.
15. Galeotti M. The Weaponisation of Everything: A Field Guide to the New Way of War// Journal of Security & Strategic Analyses. — July 2023. 9(1): 94–96. DOI: 10.57169/jssa.009.01.0250. URL: https://www.researchgate.net/publication/372360900_The_Weaponisation_of_Everything_A_Field_Guide_to_the_New_Way_of_War.
16. Hajdin N.R. What is Hybrid War? — The Terminology Used to Describe Modern Warfare and Current Authority Under International Law // Juridisk Publikation // Faculty of Law, Stockholm University Research Paper № 107. 2021. URL: https://www.researchgate.net/publication/340006068_Hybrid_War_as_a_Form_of_modern_international_Conflicts.
17. Hinshaw A., Borbely A., Chrustie C. Where Is Negotiation in Hybrid Warfare? // 24 CARDOZO J. OF CONFL. RES. 517. 2023. URL: https://www.researchgate.net/publication/334959464_War's_Future_The_Risks_and_Rewards_of_Grey_Zone_Conflict_and_Hybrid_Warfare.
18. Hoffman F.G., Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies Arlington, Virginia, 2007. 72 p.
19. Jones M., Bachmann S.D. Syria — A Hybrid War Case Study // Journal of Military and Strategic Studies. Volume 21, Issue 1. 2021. URL: https://jmss.org/article/view/73754.
20. Massive ransomware operation targets VMware ESXi: How to protect from this security threat // TechRepublic. February 7, 2023. URL: https://www.techrepublic.com/article/massive-ransomware-operation-targets-vmware-esxi.
21. Mosquera A.B., Bachmann S.D. Lawfare in Hybrid Wars: The 21st Century Warfare // journal of international humanitarian legal. Studies 7 (2016) 63–87. DOI: 10.1163/18781527-00701008. URL: https://www.researchgate.net/publication/312072465_Lawfare_in_Hybrid_Wars_The_21st_Century_Warfare.

22. Petrig A. Use of Force in Hybrid Naval Warfare Contexts: Applicability of the Law Enforcement or Conduct of Hostilities Rules? // Alexander Lott, Maritime Security Law in Hybrid Warfare // Brill. 2024. URL: https://ius.unibas.ch/fileadmin/user_upload/ius/09_Upload_Personenprofile/01_Professuren/Petrig_Anna/Publications_pdf/Manuscripts/Petrig_Use_of_Force_in_Hybrid_Naval_Warfare_Contexts_version_published_on_SSRN.pdf.
23. Schappert S. Two California Cities Hit with Ransomware in Two Days, Police Forced to Patrol Using Handheld Radios, CYBERNEWS (Feb. 11, 2023). URL: https://cybernews.com/news/oakland-modesto-ransomware-attack-old-school-policing/ [https://perma.cc/K82Y-GE22].
24. Simons G. Operational implications and effects of informational and political dimensions of western hybrid warfare // Вестник Московского государственного областного университета. 2021. № 3. URL: www.evestnik-mgou.ru.
25. Värk R. Legal Complexities in the Service of Hybrid Warfare // Kyiv-Mohyla Law and Politics Journal. December 2020. DOI: 10.18523/kmlpj220732.2020-6.27-43. URL: https://www.researchgate.net/publication/347961882_Legal_Complexities_in_the_Service_of_Hybrid_Warfare.
26. Venkat A. Massive Ransomware Attack Targets VMware ESXi Servers Worldwide, CSO U.S. (Feb. 6, 2023, 10:44 AM). URL: https://www.csoonline.com/article/3687095/massive-ransomware-attack-targets-vmware-esxi-servers-worldwide.html.