

МОРАЛЬНЫЕ ВЫЗОВЫ ИНФОРМАЦИОННЫХ ВОЙН**Николай Александрович Шавеко,**

Институт философии и права
Уральского отделения Российской академии наук
Екатеринбург, Россия,
nickolai_91@inbox.ru

Получена 26.09.2025.

Поступила после рецензирования 30.01.2026.

Принята к публикации 03.02.2026.

Для цитирования: Шавеко Н.А. Моральные вызовы информационных войн // Дискурс-Пи. 2026. Т. 23. № 1. С. 44–61. https://doi.org/10.17506/18179568_2026_23_1_44

Аннотация

Рассматриваются основные моральные вызовы, связанные с актуализацией феномена информационных войн. Утверждается, что человечество стоит на пороге новой эры, в которой регулирование в области информационного взаимодействия будет становиться все более детальным, а обеспечение прав человека будет во многом связано с борьбой за равноправие именно в информационной сфере. Более того, сама теория прав человека должна быть пересмотрена в свете реалий информационного общества. В то же время теория справедливой войны, судя по всему, остается неизменной и вполне может быть применена, в том числе, и к информационным войнам. В первую очередь следует бороться с соблазном объявить дозволительными превентивные войны, а также с соблазном освободить участников информационных войн от соблюдения принципа крайнего средства. Вместе с тем некоторые принципы справедливой войны, выглядящие спорными в контексте информационных войн, в действительности могут быть подвергнуты сомнению и вне этого контекста, поэтому сами по себе информационные войны не являются здесь фактором, делающим необходимой моральную переоценку. В свою очередь моральные дилеммы, связан-

© Шавеко Н.А., 2026



ные со сложностью применения на практике некоторых принципов справедливой войны, решаются вне связи с проблематикой информационных войн.

Ключевые слова:

информация, информационные войны, теория справедливой войны, кибервойны, права человека

Источники финансирования:

исследование выполнено за счет гранта Российского научного фонда № 25–78–00001, <https://rscf.ru/project/25-78-00001/>

UDC 327.56

DOI: 10.17506/18179568_2026_23_1_44

THE MORAL CHALLENGES OF INFORMATION WARFARE

Nikolai A. Shaveko,

Institute of Philosophy and Law of the Ural Branch
of the Russian Academy of Sciences
Yekaterinburg, Russia,
nickolai_91@inbox.ru

Received 26.09.2025.

Revised 30.01.2026.

Accepted 03.02.2026.

For citation: Shaveko, N.A. (2026). The Moral Challenges of Information Warfare. *Discourse-P*, 23(1), 44–61, (In Russ.). https://doi.org/10.17506/18179568_2026_23_1_44

Abstract

The main moral challenges associated with the actualization of the information warfare are considered. It is argued that humanity is on the threshold of a new era in which regulation in the field of information interaction will become more and more detailed, and ensuring human rights will be largely linked to the struggle for equality in the information sphere. Moreover, the theory of human rights itself must be revised in the light of the realities of the information society. At the same time, the theory of just war, apparently, remains unchanged and may well be applied, including to information wars. First of all, it is necessary to fight the temptation to declare preventive wars permissible, as well as the temptation to exempt participants in information wars from observing the principle of last resort. At the same time, some principles of a just war that look questionable in the context of

information warfare can actually be questioned outside of this context, therefore, information wars themselves are not a factor here that makes a moral reassessment necessary. In turn, the moral dilemmas associated with the difficulty of applying certain principles of just war in practice are solved outside of the context of information warfare.

Keywords:

information, information warfare, theory of just war, cyber warfare, human rights

Funding:

the study was funded by the Russian Science Foundation grant No. 25-78-00001, <https://rscf.ru/project/25-78-00001/>

Введение: о понятии информационных войн

Роль информации в функционировании современных обществ трудно переоценить: не случайно еще в последней трети XX века была сформулирована концепция «информационного общества» (Masuda, 1981; Katz, 1988). Со временем особое внимание академического сообщества, средств массовой информации и общественных деятелей привлек также феномен информационных войн. Следует констатировать, что роль информационных войн в функционировании общества постоянно возрастает. В то же время, исследования данного феномена редко носят нормативный характер: рассматривая конкретные способы ведения информационных войн и их эффективность, делая прогнозы дальнейшего развития информационной сферы, ученые, как правило, не задаются вопросом, как все это должно изменить нашу этику. Представляется, однако, что ввиду своей сегодняшней роли информационные войны нуждаются в моральной оценке и осмыслении, то есть в теоретических исследованиях, осуществляемых в том числе на стыке военной и информационной этики.

В первую очередь, необходимо определиться с понятием информационной войны. В зарубежной литературе распространено широкое понимание данного термина как любого агрессивного или оборонительного задействования информации и информационных систем (в качестве оружия, искомого ресурса или мишени) в военно-политических целях (Hauschild, 1999; Ventre, 2009, pp. 288–289). В США популярна классификация (военных) информационных операций, предложенная Комитетом начальников штабов, согласно которой существуют следующие виды информационных операций (Poisel, 2013, p. XV; Ventre, 2016, pp. 26–27):

- 1) психологические операции;
- 2) военный обман;
- 3) обеспечение защиты информации;
- 4) радиоэлектронная борьба (РЭБ);
- 5) операции с компьютерными сетями.

Иногда в этот перечень добавляют военные операции по физическому уничтожению информационных систем противника (Waltz, 1998, p. 26).

Нередко в литературе также приводится точка зрения М. Либицки (1995, p. 7) – одного из главных теоретиков информационных войн – согласно которой существуют семь основных категорий информационных войн:

- 1) физическая атака на системы командования и контроля противника;
- 2) разведывательная деятельность;
- 3) электронная война (в области физической передачи информации, включая РЭБ и криптографические войны);
- 4) психологическая война (включая пропаганду и дезинформацию);
- 5) хакерская война (атаки на информационные системы);
- 6) экономическая информационная война (связанная с коммерчески значимой информацией);
- 7) кибервойна (виртуальные сражения).

Последним трендом в развитии информационных войн называют борьбу за большие данные, используемые в том числе для обучения нейронных сетей (Ventre, 2016, pp. 326–327). Так или иначе, информационные атаки затрагивают, во-первых, физические объекты, во-вторых, информационную инфраструктуру, в-третьих, сферу индивидуального сознания (Waltz, 1998, p. 27).

Очевидно, что столь широкие определения информационных войн и операций включают как тысячелетние военные практики, так и совершенно новые явления. С учетом изложенного со временем стали предприниматься попытки вычленить более конкретные явления. Так, «с конца первого десятилетия нынешнего века четкое разделение информационных и кибервойн стало общепринятым стандартом», при этом под кибервойнами сегодня предлагается понимать целенаправленное деструктивное воздействие программного кода на материальные объекты (значимую инфраструктуру) (Ларина, Овчинский, 2014, с. 18–19). В отечественной литературе информационные войны понимаются более узко, чаще всего лишь как психологическое воздействие (львиную долю такого рода информационных войн можно объединить понятием «пропагандистская война»).

Помимо этого, в научной литературе существуют дискуссии относительно выделения тех или иных поколений войн с учетом применяемых тактик, стратегий и технологий. Устоявшимся стало выделение четвертого поколения войн, под которым понимают войны с участием негосударственных акторов. Таким войнам свойственны асимметричность, низкая интенсивность и высокая длительность, использование партизанской, повстанческой, террористической тактики, транснациональный характер и другие связанные признаки. Но, помимо этого, предпринимаются попытки выделить и пятое поколение войн, особенностью которого являются некинетические военные действия (социальная инженерия, дезинформация, кибератаки и т. д.), а также использование новых технологий, таких как искусственный интеллект и роботизированное оружие (Abbott, 2010). Поскольку характеристика войн четвертого поколения также включает психологические атаки и борьбу за идентичность, постольку рядом авторов высказываются сомнения в необходимости выделения пятого поколения войн. Не следует забывать и тот факт, что как асимметричность и другие признаки войн четвертого поколения, так и некинетические формы агрессии и защиты, со ссылкой на которые выделяется

пятое поколение войн, не являются сугубо достоянием современности. Вместе с тем, все они достаточно успешно подчеркивают известные тренды современных военных конфликтов, создавая ощущение перманентной войны. Подобно вирусу, поразившему человечество, эта война не поддается точной локализации, ее невозможно увидеть (наблюдаемы лишь отдельные обострения и симптомы), и никогда нельзя быть до конца уверенным в том, что она осталась позади.

В целом мы видим, что информационные войны не обязательно являются войнами четвертого или пятого поколений, а последние, в свою очередь, не всегда являются информационными, однако в любом случае нельзя не замечать ключевой значимости фактора информации и информационных технологий для современных войн. Какие же новые моральные вопросы при этом возникают?

Об опасности информационных войн

В качестве основного морально значимого фактора информационных войн в академической литературе называется то обстоятельство, что вред, который может быть причинен информационной атакой, вполне соизмерим со вредом, причиняемым кинетическим оружием. Отсюда, как представляется, крайне важно рассматривать информационную войну именно как войну, а некинетическое оружие – именно как оружие. Война в толковом словаре С.И. Ожегова определяется как вооруженная борьба между государствами, народами или классами¹, а в энциклопедии «Британника» как конфликт между политическими группами, характеризующийся значительной продолжительностью и масштабом². Таким образом, война в любом случае связывается с враждой, агрессией и насилием, но не с любыми их проявлениями, а, во-первых, лишь с участием политических групп, во-вторых, лишь определенной степени серьезности. В свою очередь оружием, согласно толковым словарям, может называться любое изделие, предназначенное для борьбы со своими противниками³. Но в нашем случае важно подчеркнуть, что использование информации, информационных технологий и систем в борьбе со своими противниками в определенных случаях можно и нужно квалифицировать как вооруженную борьбу (тот или иной вид военных действий), то есть как нечто настолько серьезное, что его следует называть войной. Впрочем, тут важно выработать четкие критерии, чтобы не квалифицировать как войну любое недобровольное информационное взаимодействие.

В качестве контраргумента иногда указывают, что последствия информационных атак, как правило, сопоставимы с последствиями экономических санкций (и те и другие направлены на причинение вреда экономике противника), хотя экономические санкции не расцениваются международным правом как военные действия, и могут применяться легально. Однако теоретики справедливой войны уже давно подметили разрушительный потенциал экономических санкций,

¹ Война. Взято 20 сентября 2025, с <https://slovarozhegova.ru/word.php?wordid=3653>

² War. Retrieved September 20, 2025, from <https://www.britannica.com/topic/war>

³ Оружие // Энциклопедический словарь Брокгауза и Ефрона. Т. XXII (1897): Опека-Оутсайдер. С. 214.

заставляющий сделать их моральную переоценку. Так, по мнению Х. Сисе, экономические санкции, во-первых, воздействуют прежде всего на гражданское население, во-вторых, могут быть не менее смертоносными, чем оружие. В этой связи их далеко не всегда можно рассматривать как предпочтительную войну альтернативу (Сисе, 2007, с. 96–98). У. Штейнхофф, в свою очередь, указывает на гибель полумиллиона мирных жителей Ирака из-за экономических санкций, введенных в отношении этой страны, и пишет, что «иногда война – меньшее зло, причем даже при наличии альтернативных средств для достижения той же цели...; ибо некоторые средства вызывают более высокие моральные издержки, чем война, в том числе и особенно с точки зрения человеческих жизней» (Steinhoff, 2007, pp. 28–29). Как представляется, разрушительный и неизбирательный характер экономических санкций (включая бойкоты, эмбарго и др. меры) заставляет нас хотя бы в некоторых случаях расценивать их применение как экономическое оружие, то есть как акт войны, а значит и пересмотреть соответствующее международно-правовое регулирование. Таким образом, схожесть последствий информационных войн с экономическими санкциями не влияет на квалификацию тех и других как войн. Здесь применимо понятие гибридных войн, включающих как информационные и экономические, так и иные атаки (включая поддержку повстанцев и бунтовщиков, диверсии и секретные операции т. п.). Основная опасность гибридных войн, объединяющих в себе признаки войн различных поколений, а также иные методы политического давления, состоит в том, что нападающая сторона, координируя различные типы действий, имеет возможность правдоподобно отрицать свою вовлеченность в конфликт.

Таким образом, общее следствие современной трансформации способов ведения конфликтов состоит в том, что граница между войной и миром становится размытой. Это означает, что моральную и юридическую оценку должны получить недружественные действия (информационные, экономические и др.) различной степени интенсивности и разрушительности. В частности, необходимо решить вопрос, насколько применимы к ним теория справедливой войны, а также традиционные юридические категории, такие как применение силы или угрозы силой, акт агрессии, вмешательство во внутренние дела государства и т. д. (пп. 1, 4 ст. 2 Устава ООН).

Трансформация теории прав человека

Реалии информационного общества, в том числе информационные войны, делают необходимым пересмотр теории прав человека. Следует признать очевидный факт, что регулирование и, соответственно, ограничения в области информации и информационных технологий неизбежны. Это касается, в том числе, устройств «интернета вещей», а также социальных сетей, мессенджеров, платформ и экосистем, сайтов, приложений с их собственными политиками обработки персональных данных, системами модерации, алгоритмами продвижения контента и предоставления рекламных услуг. В политическом аспекте особое значение приобретает борьба с «fake news», манипуляцией, языком ненависти, радикализмом и экстремизмом, «фабриками троллей», социальной разобщенностью, снижением рациональности политиков и политических дис-

курсов, неравенством в доступе к информации, трансформирующимся в другие виды социального неравенства, влиянием технологических гигантов на политику и социальные связи, новыми информационными угрозами, включая незаконную деятельность в darknet, киберпреступления и т. п. Информационные технологии также повышают возможности для злоупотребления государственной властью. Как бы то ни было, мечты о полной свободе в интернете должны быть отброшены не только на практике, но и в теории. Даже с либеральной точки зрения любая свобода должна соотноситься с безопасностью и другими факторами, обеспечивающими использование других, не менее важных свобод. В условиях же, когда информация оказывается важнейшим фактором безопасности, подробное регулирование ее сбора, хранения, обработки и распространения неизбежно. Таким образом, речь идет о переходе к новой парадигме информационного взаимодействия.

С нашей точки зрения, изменения касаются как минимум следующих направлений: 1) разработка информационно-коммуникационных технологий; 2) сбор и хранение информации; 3) распространение информации. Так, реальностью становятся все новые ограничения на сбор и хранение информации, как той, что составляет государственную, коммерческую или частную тайну, так и той, что к тайне не относится, и зачастую находится в открытом доступе (или же предоставляется добровольно), но, будучи собранной в большом количестве, может быть использована как оружие в информационной войне. Сегодня, в частности, мы наблюдаем особый тип политики – психополитику, в которой управление массами строится на прогнозировании и программировании на бессознательном уровне поведения людей с помощью такой информации (Хан, 2025, с. 29–40, 71). Эта политика становится возможной, благодаря перманентному и во многом бесконтрольному сбору информации о гражданах. Но не только сбор и хранение, а также и распространение информации должно быть отчасти ограничено. В первую очередь это касается ложной, явно манипулятивной или общественно вредной информации. Кроме того, не только государство и цифровые гиганты, но и отдельные индивиды должны проявлять ответственность, соблюдая требования информационной безопасности.

Сказанное предполагает важные технологические, институциональные и мировоззренческие новшества. Во-первых, необходимы ограничения на технологии сбора информации, с целью пресечь саму возможность сбора чувствительных персональных данных, а также ограничения на технологии передачи информации, чтобы та информация, распространение которой было выгодно владельцу данной технологии (например, алгоритма подбора контента), соотносилось с общественным интересом. Во-вторых, неизбежной представляется политика маркировки контента, внедрения обязательных систем модерации контента, независимого фактчекинга, замедления/приостановки коммуникации и т. д. В-третьих, требуется создание публичного пространства, в котором дискуссии разворачиваются, а информация передается свободно, но по определенным правилам (равные возможности и т. п.). Необходимо содействовать таким способам обсуждения, при которых у участников отсутствуют стимулы, связанные с прибылью и властью. Подобное публичное пространство представляет собой здоровую альтернативу политике продвижения официальной

идеологии, национальной идеи, скреп, традиционных ценностей и т.п. Во всех подобных нововведениях крайне важно пройти между Сциллой государства и Харибдой рынка, находить различные способы саморегуляции внутри общества, механизмы общественной экспертизы и т.п. Требуется также формирование новой политической культуры, продвигающей критическое мышление и нетерпимой к обману и манипуляции, тайному сбору персональных данных и информационным атакам.

В целом, по всей видимости, мы являемся свидетелями новой эры, в которой регулирование информационного взаимодействия будет становиться все более детальным, а обеспечение прав человека будет во многом связано с борьбой за равноправие именно в информационной сфере. Нынешняя логика развития прав человека, как представляется, схожа с той трансформацией, которая имела место 100–150 лет назад при постепенном моральном и легальном утверждении социально-экономических прав: это новое поколение прав, с одной стороны, было направлено на предоставление каждому человеку условий для саморазвития, с другой стороны, накладывало ограничение на служащие той же самой цели личные и политические права, а кроме того, создавало риск для различных злоупотреблений со стороны государства, на которое теперь возлагалась функция перераспределения общественных доходов и богатств. Применительно к информационным войнам также встает проблема возрастания рисков злоупотреблений властью, но теперь уже в связи с тем, что государство получает контроль над информационной сферой: противоположной по отношению к множеству замкнутых на себе «племен» крайностью является тоталитарное государство, контролирующее доступ к информации, и его унифицированная пропаганда. Вероятно, это заставляет нас переосмыслить роль государства как основного гаранта прав человека. Вместе с тем, намечающаяся альтернатива тотальному государственному контролю информационной сферы также вызывает тревогу у исследователей. Речь идет о «надзорном капитализме» (Зубофф, 2022), «технофеодализме» (Варуфакис, 2025) и т.п. концепциях, отражающих олигополию нескольких частных игроков (технологических гигантов), навязывающих свою волю не только отдельным гражданам, но и государствам. Одним из выходов из этого тупика могут стать системы общественного (т.е. и не государственного, и не частного) контроля.

Современная трансформация теории прав человека также связана с провозглашением новых фундаментальных прав. Так, например, ведутся активные дебаты относительно «права на забвение» (имеется в виду удаление информации об индивиде в поисковых системах, в России оно закреплено с 2016 г.) и его соотношения со свободой слова и свободой доступа к информации, в том числе имеющей публичную, художественную или научную ценность. Практически бесспорным на сегодняшний день является право на защиту персональных данных, включая цифровой след, однако полная анонимность в Интернете вызывает вопросы (по крайней мере, у правоохранителей должна оставаться возможность отследить интернет-преступников). Исследователи также разрабатывают такие права, как право на доступ в Интернет, переосмысливают право на информацию (ст. 29 Конституции РФ) с учетом того, например, что некоторая информация является общественно-вредной, и не подлежит распространению, а также с учетом того, что у каждого человека должен быть доступ именно к правдивой инфор-

мации. Отсюда дискуссии о праве на истину или, по крайней мере, на защиту от дезинформации. Поскольку одним из важнейших ресурсов сегодня является внимание, достигаемое зачастую «информационным бомбардированием» граждан, важную роль, с нашей точки зрения, приобретает также право на защиту от (!) информации (причем как политического, так и неполитического характера, поскольку грань здесь условна). В настоящее время данное право обеспечивается лишь частично (например, существуют ограничения на политическую агитацию, на места по размещению рекламы, а также ограничения на распространение нежелательной информации среди детей), то есть имеется огромная сфера, не урегулированная должным образом. По всей видимости, речь должна идти о защите не только от конкретной информации (например, экстремистского или порнографического характера, а также от заведомо ложной информации), но и от информационных атак в целом. При этом некоторая общественно-значимая информация, наоборот, должна доводиться в обязательном порядке.

Право на защиту персональных данных и право на забвение, наряду с правом на информацию и на защиту от ложной и нежелательной информации, демонстрируют, что развитие технологий вынуждает нас искать новое соотношение публичного и частного. С одной стороны, в нынешней «экономике слежения» (основанной на захвате персональных данных) (Зубофф, 2022; Кин, 2015, с. 49) и «экономике внимания» (основанной на захвате внимания с помощью алгоритмов, работающих на основе больших данных) (Lanham 2006) необходимо отгородить людей от негативного вмешательства в их частную жизнь. С другой стороны, ни одно из перечисленных прав, как видно из изложенного, не является абсолютным, поскольку может вступать в противоречие с публичным интересом.

Моральные вызовы для теории справедливой войны

Другой вопрос состоит в том, применима ли к информационным войнам теория справедливой войны. Указанная теория является направлением в военной этике, занимающем промежуточное положение между реализмом (представлением о том, что война не должна оцениваться с моральных позиций) и пацифизмом (радикальным неприятием войны). Теоретики справедливой войны полагают, что война может считаться справедливой, если удовлетворяет определенным принципам. К таким принципам относятся, в частности (Шавеко, 2024, с. 7–8):

- 1) принцип правого дела (должна иметь место справедливая причина для войны);
- 2) принцип соразмерности (предполагаемые выгоды от войны должны быть соразмерны предполагаемым издержкам войны);
- 3) принцип крайнего средства / необходимости (к военным действиям допустимо прибегать только в том случае, если иные способы разрешения конфликта не сработали или явно неадекватны ситуации);
- 4) принцип добрых намерений (решение о военных действиях должно быть обусловлено правильными целями);
- 5) принцип легитимности (войну может начать только законная власть);
- 6) принцип дискриминации (атаковать можно только военные объекты, а не мирную инфраструктуру, и только армию противника, а не гражданских лиц).

Соответственно, вопрос состоит в том, применимы ли указанные принципы к информационным войнам.

Далее будут рассмотрены факторы, на которые обычно обращается внимание при обсуждении данного вопроса. Предварительно отметим, что в зарубежной литературе соответствующие дискуссии начались на рубеже XX и XXI вв. со статьи Дж. Аркви́ллы, в которой он пришел к выводу, что информационные войны оставили в прошлом значительную часть традиционной теории справедливой войны (Arquilla, 1999, p. 394). Соглашаясь со многими суждениями указанного автора, мы, однако, далее придем к прямо противоположному выводу, а именно что традиционная теория справедливой войны вполне применима к информационным войнам. Поскольку соответствующие дискуссии в зарубежной литературе сегодня ведутся вокруг следующих трех понятий: риски, права и ответственность (The Ethics of Information Warfare, 2014, p. VII), мы также будем использовать их как отправную точку.

Итак, во-первых, риски, связанные с осуществлением информационной агрессии, значительно меньше рисков, которыми сопровождается атака кинетическим оружием (в связи с «бескровностью» и «удаленностью» информационных атак) (Ajir & Vaillant, 2018).

Данный фактор, по-видимому, проблематичен лишь в том плане, что делает войну более вероятной, а вовсе не потому, что он ставит под сомнение принципы справедливой войны. Действительно, достаточно сложно привести аргументы в пользу утверждения, что вышеперечисленные принципы не должны применяться к информационным войнам лишь потому, что эти войны превратились в привычное явление.

Некоторые исследователи утверждают, что поскольку ущерб от кибератак может быть значительно меньше, чем ущерб от традиционных атак, постольку к информационным войнам неприменим принцип крайнего средства. С точки зрения соответствующих авторов, кибератаки вполне допустимы не как крайнее, а как первоочередное средство (Lee, 2014; Taddeo, 2014, pp. 129–130). Другие авторы на основании принципа необходимости утверждают, что применение менее разрушительного и опасного кибероружия вместо более разрушительного и опасного кинетического оружия является моральным долгом участника войны (Denning & Strawser, 2014). Комментируя указанные взгляды, в первую очередь необходимо отметить, что содержательно принципы крайнего средства и необходимости едины, и означают, что более опасные и разрушительные средства должны применяться только в случае, если иные средства оказались негодными. Если руководствоваться указанной формулировкой, то окажется, что данные принципы применимы к любым типам войн, в том числе информационным. При этом кибератаку или иную информационную атаку все же нельзя рассматривать как первоочередное средство, если существует возможность переговоров и дипломатии. Следовательно, принцип крайнего средства (необходимости) остается актуальным.

Высказывается также тезис, что если традиционная трактовка принципа правого дела не допускает превентивную войну, то информационные атаки ввиду своей малой разрушительности вполне могут осуществляться превентивно (например, с целью помешать созданию оружия массового уничтожения) (Arquilla,

1999, р. 387). Вместе с тем, очевидно, что дозволение превентивных информационных атак сомнительно даже с учетом их малой разрушительности, так как может спровоцировать «войну всех против всех», что не будет отвечать принципам соразмерности и необходимости (фактически мы уже сейчас наблюдаем скрытую глобальную войну, в которой в долгосрочном плане рискуют проиграть все). Кроме того, хотя создание оружия массового уничтожения само по себе может рассматриваться как правонарушение, требующее ответных действий, но любые такие действия, по общему правилу, должны осуществляться в рамках существующего международного правопорядка на основе легитимных решений.

Таким образом, особенности информационных войн заставляют внимательно относиться к расчету возможного ущерба от информационных атак и к сопоставлению его с имеющимися альтернативами, но вряд ли являются основанием для переосмысления самих моральных принципов. Тот факт, что информационные войны на первый взгляд характеризуются меньшими рисками, не отменяет существующих моральных требований, в частности принципов крайнего средства (необходимости) и соразмерности, и не дает оснований для оправдания превентивной информационной войны.

Во-вторых, информационные атаки зачастую направлены на объекты, не являющиеся военными; сами эти атаки также могут быть осуществлены через «гражданские» компьютеры и веб-сайты.

Этот фактор проблематичен потому, что размывает границу между военными и гражданскими объектами и целями. Следует признать, что уже войны четвертого поколения подняли ряд острых вопросов, касающихся, например, статуса партизан, частных спонсоров войны или объектов двойного назначения, включая транспортную, энергетическую и информационную инфраструктуру. Это заставляет выработать четкие общие правила разграничения законных и незаконных целей войны (например, таких традиционных критериев разграничения комбатантов и некомбатантов, как ношение оружия и военной формы и состояние в действующей армии, здесь явно недостаточно). Таким образом, поводы для переосмысления принципа дискриминации появились задолго до т. н. «информационного взрыва», актуализировавшего информационные войны. В этой связи и в отношении последних можно было бы ограничиться общим выводом, что сама по себе сложность определения допустимой цели не может служить оправданием атаки в отношении цели недопустимой. Однако проблема в том, что в пропагандистских войнах граница между комбатантами и некомбатантами не просто сложно определяется, но и в принципе исчезает. Так, применительно к классическим войнам военная этика предполагает недопустимость поражения гражданских лиц и объектов мирной инфраструктуры. «Новые войны» вскрыли проблематику, связанную с бойцами, не являющимися частью регулярной армии, с деятельностью по финансированию и разжиганию войны, а также эксплуатацией и поражением объектов двойного назначения (что актуально и для кибервойн), но все же сохранили саму возможность разграничения тех, кто участвует в войне, и кто в ней не участвует. Однако в пропагандистской войне человек одновременно является объектом и субъектом атаки: будучи «пораженным» пропагандой, он сознательно совершает действия в интересах одной из сторон

конфликта, и причиняет вред другой стороне (Шатилов, 2017). Таким образом, информационные войны проблематизируют принцип дискриминации.

Также в рассматриваемом контексте исследователи обычно обращают внимание на то, что у правительств появляются дополнительные основания для ограничения прав своих граждан. Действительно, здесь имеет место серьезная моральная дилемма, однако выше мы уже показали, что трансформация теории и практики прав человека, по всей видимости, неизбежна.

В-третьих, использование информационных технологий (анонимность, или же намеренная вероломная подмена личности) делает очень сложным определение того, кто инициировал кибератаку (Taddeo, 2012), а также квалификацию ее именно как атаки, а не как случайного сбоя (Greenberg et al., 1997, pp. 21–23). Помимо анонимности и потенциальной бесследности исследователи называют такие признаки кибервойн, как неопределенность времени их начала, а также отсутствие привычных понятий фронта и тыла (Ларина, Овчинский, 2014, с. 23–27). Впрочем, эти характеристики свойственны и любым «новым войнам». Следует указать также на возможную неясность серьезности последствий информационной атаки, что затрудняет выбор пропорционального ответа (Lin et al., 2014, pp. 42–43).

Указанные факторы, как представляется, также связаны лишь со сложностью применения традиционных принципов справедливой войны, но не с их моральной значимостью. Понятно, что для того, чтобы осудить агрессора и нанести ему ответный удар, мы должны понимать, кто именно является агрессором, и какие именно угрозы (как для материальных, так и для нематериальных объектов) от него исходят. Но выяснение этого обстоятельства – дело практической необходимости, а не моральная проблема. С позиции морали в любом случае недопустимо применять силу против субъекта, в отношении которого нельзя сказать достоверно, является он агрессором или нет; морально недопустим также и непропорциональный ответ. Представляется, что установление на международном и национальном уровнях четких сфер ответственности за происходящее в цифровом пространстве могло бы стать решением данной проблемы. В этом случае может отпасть необходимость в выявлении конкретного агрессора, поскольку ответственным в любом случае будет субъект, не предпринявший достаточных мер по нейтрализации возможности указанной агрессии, а также по поиску киберпреступников.

В связи с анонимностью источника информационных атак некоторые проблемы возникают с определением того, соблюден ли принцип легитимности. Но, во-первых, данный принцип может быть подвергнут обоснованному сомнению и вне контексте информационных войн, а потому его лучше рассматривать лишь как оспоримую презумпцию того, что война является прерогативой легитимной власти затронутой территории. Во-вторых, во всех случаях, когда источник атаки известен, степень его легитимности, равно как и характер его связи с политическими властями, как представляется, должны быть приняты во внимание, то есть указанная презумпция будет действовать, в том числе, и для информационных войн. Например, хакерские атаки в целях самообороны политического сообщества должны осуществляться только под руководством или с согласия легитимных властей этого сообщества, за исключением случаев,

когда связь с ними невозможно установить (из-за атаки противника на информационную инфраструктуру). Иными словами, здесь действует общее правило (применимое, например, и к партизанской войне), а сложности касаются лишь установления фактических обстоятельств.

Кроме того, моральные вопросы возникают в связи с ответственностью за последствия применения роботизированного оружия, так как в данном случае не ясно, кто именно должен эту ответственность нести. Тема ответственности обычно поднимается в рамках теории справедливой войны, а именно *jus post bellum* (справедливости после войны), однако не имеет отношения к принципам развязывания (*jus ad bellum*) и ведения войны (*jus in bello*), поэтому в рамках настоящего исследования вопросы ответственности рассматриваться не будут. Тем не менее, констатируем, что в этом отношении развитие информационных технологий ставит новые моральные проблемы.

Таким образом, особые характеристики информационных войн в целом вряд ли являются основанием для трансформации моральных принципов развязывания и ведения войны. Однако, как было сказано выше, определенные сложности возникают с пропагандистскими войнами, которые по своей сути отрицают принцип дискриминации. Вероятно, применительно к пропагандистским войнам не все действия, нарушающие этику информационного взаимодействия, и потому считающиеся морально недопустимыми, должны отвергаться именно на основании принципа дискриминации, поскольку зачастую они характеризуются малой опасностью.

Сложности практического применения военной этики

Что касается сложностей применения требований военной этики, то любые такие сложности на теоретическом уровне решаются в трех направлениях.

1. Принципы справедливой войны мыслимы не только в бинарной логике (в рамках которой тот или иной принцип либо соблюдается, либо нет), но и в логике «скользящей шкалы» (в рамках которой действие с точки зрения каждого из принципов может быть оценено как более или менее (не) справедливое). Отсюда, даже частичное их воплощение имеет моральную значимость. Например, военные действия могут не отвечать требованиям необходимости и соразмерности (и в этом смысле быть несправедливыми), но в любом случае чем меньше разрушений они влекут, тем лучше (то есть можно сделать их менее несправедливыми). В результате сложность выполнения соответствующих принципов в конкретных случаях не заставляет нас отказываться от них, ведь любое стремление к их соблюдению оправдано: они выступают для нас своего рода «путеводной звездой», по направлению к которой есть смысл плыть, даже если понимаешь, что никогда ее не достигнешь.

2. При оценке действий конфликтующих сторон нельзя забывать про критерий вины. Иногда обстоятельства таковы, что просто невозможно выполнить моральное требование, но если это действительно так, то это невыполнение и не вменяется субъекту в вину. В этом смысле частота и серьезность несправедливостей на войне сами по себе не имеют морального значения. Его имеет лишь то, выполнили ли участники военных действий требования, которые предъявля-

ются к ним как к рациональным агентам. Следовательно, даже если формальное нарушение принципов неизбежно, это еще не влечет их несостоятельность.

3. Моральные требования должны формулироваться таким образом, чтобы их соблюдение было принципиально возможно для рациональных агентов. Проблем не возникает, если для выполнения требования достаточно лишь воздержаться от определенных несправедливых действий. Однако ситуация меняется, когда речь идет о позитивных обязанностях (т. е. обязанностях по совершению активных действий). Именно такие обязанности как минимум в некоторых случаях подразумевает принцип правого дела. Например, государство не просто вправе, но и обязано защищать своих граждан от внешней агрессии. Следовательно, формулируя обязанности государства по такой защите, нельзя предъявлять к нему заведомо невыполнимых требований. Здесь возможна аналогия с обязанностями по обеспечению внутреннего правопорядка: нельзя требовать от государства устранения преступности как таковой, но можно требовать выполнения сотрудниками полиции своих должностных обязанностей. В случаях же, когда государства не имеют возможности или права обеспечивать защиту от информационной атаки, они должны предусматривать право жертвы на самооборону (Lin et al., 2014).

Как видно, многие теоретические трудности, связанные с невыполнимостью принципов справедливой войны, решаются на более абстрактном уровне, и не связаны с проблематикой информационных войн.

Заключение

Информационные войны бросают нам множество моральных вызовов. В первую очередь, некоторые информационные атаки (равно как и некоторые экономические санкции и т. п. приемы гибридной войны) следует квалифицировать как применение силы или угрозы силой, акт агрессии, вооруженное нападение и как вмешательство во внутренние дела государства согласно международному праву. В конечном счете, реалии информационного общества, в том числе информационные войны, делают необходимым пересмотр теории прав человека, и выработку этики информационного взаимодействия. Речь идет не только о новых ограничениях (мечты о полной свободе в интернете должны быть отброшены), но и о провозглашении новых прав. Эти новые права, с одной стороны, направлены на предоставление каждому человеку условий для саморазвития, с другой стороны, накладывают ограничения на уже существующие права, что создает условия для различных злоупотреблений со стороны государства, получившего полномочия по контролю информационной сферы. В то же время теория справедливой войны в целом остается неизменной и вполне может быть применена, в том числе, и к информационным войнам (однако применительно к «пропагандистским» войнам сложно отстаивать принцип дискриминации в строгих формулировках). В первую очередь следует бороться с соблазном объявить дозволительными превентивные войны, а также с соблазном освободить участников информационных войн от соблюдения принципа крайнего средства. В то же время некоторые принципы справедливой войны, выглядящие сомнительными в контексте информационных войн, в действительности могут быть

подвергнуты сомнению и вне этого контекста, поэтому сами по себе информационные войны не являются здесь фактором, делающим необходимой моральную переоценку. В свою очередь моральные дилеммы, связанные со сложностью применения на практике некоторых принципов справедливой войны, решаются вне связи с проблематикой информационных войн.

Список литературы:

1. Варуфакис, Я. (2025). *Технофеодализм*. М.: Ад Маргинем.
2. Зубофф, Ш. (2022). *Эпоха надзорного капитализма. Битва за человеческое будущее на новых рубежах власти*. М.: Издательство Института Гайдара.
3. Кин, Дж. (2015). *Демократия и декаданс медиа*. М.: Издательский дом Высшей школы экономики.
4. Ларина, Е., Овчинский, В. (2014). *Кибервойны XXI века. О чем умолчал Эдвард Сноуден*. М.: Книжный мир.
5. Сисе, Х. (2007). *Справедливая война? О военной мощи, этике и идеалах*. М.: Весь Мир.
6. Хан, Б.-Ч. (2025). *Инфократия*. М.: АСТ.
7. Шавеко, Н.А. (2024). *Принципы справедливой войны*. М.: Инфра-М.
8. Шатилов, А.Б. (2017). Современные информационные войны: феномен «Диванной мобилизации» (на примере «Украинского конфликта» 2014–2017 гг.). *Дискурс-Пи*, 27(2), 141–145.
9. Abbott, D. (2010). *The Handbook of Fifth-Generation Warfare*. Ann Arbor: Nimble Books.
10. Ajir, M., & Vaillant, B. (2018) Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70–89.
11. Arquilla, J. (1999). Ethics and information warfare. In Z.M. Khalilzad, J.P. White, & A. Marshall (Eds.), *The changing role of information in warfare* (pp. 379–401). Santa Monica: RAND.
12. Denning, D.E., & Strawser, B.J. (2014). Moral Cyber Weapons. In L. Floridi, & M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 85–104). Cham: Springer International Publishing.
13. Hauschild, E. (1999). Modern and information warfare: A conceptual approach. In K.R. Spillmann, & J. Krause (Eds.), *International Security Challenges in a Changing World (Studies in Contemporary History and Security Policy, vol. 3)* (pp. 199–210). Bern: Peter Lang Publ.
14. Greenberg, L.T., Goodman, S.E., & Soo Hoo, K.J. (1998). *Information Warfare and International Law*. Washington D.C.: National Defense University Press.
15. Katz, R.L. (1988). *The Information Society: An International Perspective*. New York: Praeger.
16. Lanham, R. A. (2006). *The Economics of Attention: Style and Substance in the Age of Information*. Chicago: University of Chicago Press.
17. Lee, S.P. (2014). *The Ethics of Cyberattack*. In L. Floridi, M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 105–122). Cham: Springer International Publishing.

18. Libicki, M. (1995). *What Is Information Warfare?* (Working paper). Washington DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University.
19. Lin, P., Allhoff, F., & Abney, K. (2014). In Warfare the Right Frame for the Cyber Debate? In L. Floridi, & M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 39–60). Cham: Springer International Publishing.
20. Masuda, Y. (1981). *The information Society as Post-Industrial Society*. Washington D.C.: World Future Society.
21. Poisel, R. A. (2013). *Information Warfare and Electronic Warfare Systems*. Norwood (MA): Artech House.
22. Steinhoff, U. (2007). *On the Ethics of War and Terrorism*. New York: Oxford University Press.
23. Taddeo, M. (2014). Information Warfare and Just War Theory. In L. Floridi, & M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 123–140). Cham: Springer International Publishing.
24. Taddeo, M. (2012). Information Warfare: A Philosophical Perspective. *Philosophy and Technology*, 25(1), 105–120. <https://doi.org/10.1007/s13347-011-0040-9>.
25. Floridi, L., & Taddeo M. (Eds.). (2014). *The Ethics of Information Warfare*. Cham: Springer International Publishing.
26. Ventre, D. (2009). *Information warfare* (1st ed). London, Hoboken: ISTE Ltd and John Wiley & Sons, Inc.
27. Ventre, D. (2016). *Information warfare* (2nd ed). London, Hoboken: ISTE Ltd and John Wiley & Sons, Inc.
28. Waltz, E. (1998). *Information warfare: principles and operations*. Norwood (MA): Artech House.

References:

1. Abbott, D. (2010). *The Handbook of Fifth-Generation Warfare*. Ann Arbor: Nimble Books.
2. Ajir, M., & Vaillant, B. (2018). Russian Information Warfare: Implications for Deterrence Theory. *Strategic Studies Quarterly*, 12(3), 70–89.
3. Arquilla, J. (1999). Ethics and information warfare. In Z.M. Khalilzad, J.P. White, & A. Marshall (Eds.), *The changing role of information in warfare* (pp. 379–401). Santa Monica: RAND.
4. Denning, D.E., & Strawser, B.J. (2014). Moral Cyber Weapons. In L. Floridi, M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 85–104). Cham: Springer International Publishing.
5. Floridi, L., & Taddeo M. (Eds.). (2014). *The Ethics of Information Warfare*. Cham: Springer International Publishing.
6. Greenberg, L.T., Goodman, S.E., & Soo Hoo, K.J. (1998). *Information Warfare and International Law*. Washington D.C.: National Defense University Press.
7. Han, B.-Ch. (2025). *Infokratija* [Infocracy]. Moscow: ACT.
8. Hauschild, E. (1999). Modern and information warfare: A conceptual

approach. In K.R. Spillmann, & J. Krause (Eds.), *International Security Challenges in a Changing World (Studies in Contemporary History and Security Policy, vol. 3)* (pp. 199–210). Bern: Peter Lang Publ.

9. Katz, R.L. (1988). *The Information Society: An International Perspective*. New York: Praeger.

10. Keane, J. (2015). *Demokratija i dekadans media* [Democracy and media decadence]. Moscow: Izdatel'skij dom Vysshej shkoly jekonomiki.

11. Lanham, R. A. (2006). *The Economics of Attention: Style and Substance in the Age of Information*. Chicago: University of Chicago Press.

12. Larina, E., & Ovchinskij, V. (2014) *Kibervojny XXI veka. O chem umolchal E'dvard Snouden* [Cyberwars of the XXI century. What Edward Snowden didn't mention]. Moscow: Knizhnyj mir.

13. Lee, S.P. (2014). The Ethics of Cyberattack. In L. Floridi, & M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 105–122). Cham: Springer International Publishing.

14. Libicki, M. (1995). *What Is Information Warfare?* (Working paper) Washington DC: Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University.

15. Lin, P., Allhoff, F., & Abney, K. (2014). In Warfare the Right Frame for the Cyber Debate? In L. Floridi, M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 39–60). Cham: Springer International Publishing.

16. Masuda, Y. (1981). *The information Society as Post-Industrial Society*. Washington D.C.: World Future Society.

17. Poisel, R.A. (2013). *Information Warfare and Electronic Warfare Systems*. Norwood (MA): Artech House.

18. Shatilov, A.B. (2017). Sovremennyye informacionnyye vojny: fenomen "Divannoj mobilizacii" (na primere "Ukrainskogo konflikta" 2014–2017 gg.) [Modern information wars: a phenomenon of "sofa mobilization" (using the case of "Ukrainian conflict" 2014–2017)]. *Diskurs-Pi*, 27(2), 141–145.

19. Shaveko, N.A. (2024). *Principy spravedlivoy vojny* [Principles of a just war]. Moscow: Infra-M.

20. Steinhoff, U. (2007). *On the Ethics of War and Terrorism*. New York: Oxford University Press.

21. Syse, H. (2007). *Spravedlivaja vojna? O voennoj moshhi, jetike i idealah* [Just war? About military power, ethics and ideals]. Moscow: Ves' Mir.

22. Taddeo, M. (2012). Information Warfare: A Philosophical Perspective. *Philosophy and Technology*, 25(1), 105–120. <https://doi.org/10.1007/s13347-011-0040-9>.

23. Taddeo, M. (2014). Information Warfare and Just War Theory. In L. Floridi, M. Taddeo (Eds.), *The Ethics of Information Warfare* (pp. 123–140). Cham: Springer International Publishing.

24. Varoufakis, Y. (2025). *Tekhnofeodalism* [Technofeudalism]. Moscow: Ad Marginem.

25. Ventre, D. (2009). *Information warfare* (1st ed). London, Hoboken: ISTE Ltd and John Wiley & Sons, Inc.

26. Ventre, D. (2016). *Information warfare* (2nd ed). London, Hoboken: ISTE

Ltd and John Wiley & Sons, Inc.

27. Waltz, E. (1998). *Information warfare: principles and operations*. Norwood (MA): Artech House.

28. Zuboff, Sh. (2022). *Jepoha nadzornogo kapitalizma. Bitva za chelovecheskoe budushhee na novykh rubezhah vlasti*. [The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power]. Moscow: Izdatel'stvo Instituta Gajdara.

Информация об авторе

Николай Александрович Шавеко, кандидат юридических наук, старший научный сотрудник, Институт философии и права Уральского отделения Российской академии наук, Екатеринбург, Россия, ORCID: <https://orcid.org/0000-0002-5481-7425>, e-mail: nickolai_91@inbox.ru

Information about the author

Nikolai Aleksandrovich Shaveko, Candidate of Law Sciences, Senior Researcher, Institute of Philosophy and Law of the Ural Branch of the Russian Academy of Sciences, Ekaterinburg, Russia, ORCID: <https://orcid.org/0000-0002-5481-7425>, e-mail: nickolai_91@inbox.ru
