ФИЛОСОФИЯ И СОВРЕМЕННОСТЬ

DOI: 10.17805/zpu.2016.3.4

Новые виды войн и безопасность России

И. А. Крылова
(Институт философии РАН)

В статье дан социально-философский анализ войн нового поколения. Показано, что в условиях однополярного мира и доминирования США на мировой арене наряду с опасностью ядерной войны резко возросла угроза войн нового поколения: экономических, «элитных»; сетецентричных, информационных, кибервойн. Речь идет о повышении роли невоенных факторов, направленных на разрушение социальных и экономических основ другого государства, его окружения, культурных и духовных ценностей, общественного уклада и политического режима с помощью новых средств борьбы и видов оружия. Подчеркивается, что ныне Россия столкнулась с очень серьезным вызовом — угрозой войны и в прежних, и в новых форматах.

В условиях глобализации широкое распространение получили экономические войны. Ведущие страны стремятся к достижению своих целей на мировой арене воздействием на политику других государств экономическими методами, например введением экономических санкций. В современных «элитных» войнах широко используются новейшие достижения прикладной психологии, которые позволяют точно реконструировать личности лидеров, выявлять их сильные и слабые стороны, а также прогнозировать их возможные действия. Не меньшую угрозу для России в настоящее время представляет вид сетевых войн, имеющих военное происхождение. Их особенностью является то, что в них невоенными средствами достигается реальная военная победа, осуществляется захват территорий и устанавливается контроль над ними.

Информационная война представляет собой одну из новых форм борьбы между государствами, а также систему мер, осуществляемую одним государством с целью подрыва информационной безопасности. Если главными объектами воздействия и защиты при информационно-технической борьбе являются информационно-технические системы (системы связи, телекоммуникационные системы, радиоэлектронные средства), то при информационно-психологической борьбе — психика политической элиты и населения противостоящих сторон, системы формирования общественного сознания, мнения, выработки и принятия решений. Особый вид информационно-технической войны представляет собой систему мер, направленных на достижение информационного превосходства путем воздействия на информацию и информационные системы противника при одновременной защите собственной информации и своих информационных систем. Виртуальное пространство, киберпространство стало еще одним пространством, в котором проходят конфликты.

Ключевые слова: Россия; США; Запад; экономическая война; элитная война; сетецентричная война; информационная война; информационно-психологическая война; информационно-техническая борьба; кибервойна; национальная безопасность

ВВЕДЕНИЕ

Начало нового XXI в. наряду с усилением военной угрозы (в том числе ядерной) ознаменовалось опасностью возникновения войн нового поколения, главной целью которых является разгром экономического потенциала противника, среды его обитания, культуры, ценностной базы, смена политического режима. Речь идет не о снижении роли военной силы, которая была и остается важнейшей опорой национальной безопасности, а о повышении роли невоенных факторов, направленных на разрушение социальных и экономических основ другого государства, среды его обитания, культурных и духовных ценностей, общественного уклада и политического режима. Дело в том, что в условиях разбалансирования климата на планете все более очевидной становится экологическая угроза.

В то же время прямое военное столкновение, особенно с крупной ядерной державой, имеющей достаточный военно-технический потенциал, предстает как экономически нецелесообразное и экологически опасное для всех. Поэтому одной из характерных особенностей современной войны является ставка на разрушение других государств путем ведения нетрадиционных войн: экономических, «элитных»; сетецентричных, информационных, кибервойн и др. с помощью невоенных средств борьбы и видов оружия. Их социально-философский анализ будет целью данной статьи.

ЭКОНОМИЧЕСКИЕ ВОЙНЫ

В условиях глобализации широкое распространение получили экономические войны. В XXI в. ведущие страны стремятся к достижению своих целей на мировой арене не только военным путем, но и воздействием на политику других государств невоенными, в частности экономическими, методами. Например, введением экономических санкций — «экономическим принуждением» и иностранной помощью — «экономическим поощрением». Причем эти средства тесно взаимосвязаны: отказ в иностранной помощи или ее прекращение могут рассматриваться как экономическая санкция, а отмена эмбарго — как поощрение.

Многочисленные факты свидетельствуют о том, что экономические санкции в условиях глобализации представляют мощное многоцелевое оружие. Дезорганизуя экономическую деятельность в стране-объекте, они наносят ей существенный урон. Экономические санкции способны резко снизить уровень материального благосостояния населения страны-объекта, вызвать голод, широкое распространение болезней и другие тяжелые бедствия. Более того, они могут привести страну к общему экономическому и политическому краху. В конечном счете, экономические санкции используются ведущими странами, прежде всего США, в качестве «аркана», на котором страны-объекты насильственно «втягиваются» в новый мировой порядок. При этом США, пытаясь сохранить мировое господство в новом столетии, нередко действуют в обход решений и структур ООН. В результате механизм, призванный содействовать поддержанию глобальной безопасности, превращается в инструмент подрыва самого ее фундамента.

И если во времена СССР, обладавшего мощным экономическим и научно-техническим потенциалом, вопрос о степени защищенности нашей страны от угрозы экономических санкций практически никогда не возникал (даже гипотетически), то для современной России ситуация кардинальным образом изменилась. После

крушения Советского Союза «чрезвычайно опасными в экономическом и военно-экономическом отношениях оказались результаты плохо продуманных и неудачно осуществляемых процессов реформирования российской экономики. Надо полагать, что при этом интересы национальной безопасности России вряд ли учитывались в должной мере, а возможность применения против нее жестких экономических санкций, судя по всему, вовсе не была принята во внимание» (Фарамазян, Борисов, 2001: 17). В результате Россия стала крайне уязвимой для экономических санкций по многим позициям, что представляет угрозу ее национальной безопасности.

С 2007 г. Россией был взят курс на осознанное отстаивание национальных интересов, что не устраивает США и западных политиков, которые пытаются наказать нашу страну санкциями после присоединения в 2014 г. Крыма к Российской Федерации. Как известно, Б. Обама в 2015 г. заявил о том, что он «разорвал экономику России в клочья» и что режим антироссийских санкций будет сохраняться до тех пор, пока не будут выполнены Минские соглашения, а Крым будет оставаться в составе Российской Федерации, которая названа в числе главных угроз США.

«ЭЛИТНЫЕ» ВОЙНЫ

Широкое проникновение виртуальной реальности в современное общество кардинально изменило способы ведения войны не только на техническом, тактическом уровне, но и на уровне большой стратегии. Появилась возможность конструирования мира, «прозрачного» для военных и спецслужб. По словам американского технического специалиста и бывшего сотрудника ЦРУ и Агентства национальной безопасности США Э. Сноудена, спецслужбы США держат ныне «под колпаком» более 1 млрд человек более чем в 50 странах мира. Однако у этой технологии есть своя ахиллесова пята, которую наглядно продемонстрировали Дж. Ассанж и его портал Wikileaks. Дело в том, что при наличии «огромного массива распределенной информации и развитых компьютерных сетей нельзя быть уверенным, что тайное довольно быстро не станет явным» (Иванов, Малинецкий, 2015: 29). Другое дело, что, имея секретную информацию, можно легко управлять элитами, а главное — лидерами тех или иных стран.

Надо сказать, что в современных «элитных» войнах широко используются новейшие достижения прикладной психологии, которые позволяют точно реконструировать личности лидеров, выявлять их сильные и слабые стороны, а также прогнозировать их возможные действия. Известно, что в разработке тактики ведения переговоров между Р. Рейганом и М. Горбачевым в Рейкьявике по сокращению стратегических вооружений, на которых фактически были сданы позиции СССР по ряду ключевых направлений, огромную роль сыграл выдающийся специалист по рефлективному управлению В. Лефевр (там же: 16).

Что касается современной России, то в настоящее время именно отечественная элита является болевой точкой нашего общества, так как принадлежащие ей 500 млрд долларов находятся в зарубежных банках. «При этом около половины уходящего из России капитала оседает за рубежом вслед за его собственниками, — справедливо пишет С. Глазьев, — скупающими за границей элитную недвижимость и приобретающими иностранное гражданство» (Глазьев, 2015: 82). И это

прекрасно понимают западные политики. Поскольку реально страной «управляют» около 80 человек, достаточно иметь возможность ими манипулировать, чтобы достичь своих целей без разрушительных кровопролитных войн. «Достать» представителей отечественной элиты можно либо через их собственность и банковские вклады за рубежом, либо через родных и близких людей, создавая угрозы их жизни и благополучию, либо через компрометирующую информацию личного характера (Иванов, Малинецкий, 2015: 15).

Поэтому сейчас одним из наиболее опасных вариантов разрушения России являются именно «элитные» войны.

СЕТЕЦЕНТРИЧНЫЕ ВОЙНЫ

Не меньшую угрозу для России в настоящее время представляет вид сетевых войн. Эта технология имеет военное происхождение. Разработчиком теории сетецентричных войн считается американский стратег, полковник вооруженных сил США Дж. Уордон. Особенностью сетецентричных войн является то, что в них невоенными средствами достигается реальная военная победа, т. е. «осуществляется захват территорий и установление контроля над ними» (Коровин, 2013: Электронный ресурс). В связи с этим понимание новых реалий в современных условиях требует кардинального пересмотра существующих подходов к ведению военных действий и достижению военных результатов.

Дело в том, что в индустриальную эпоху боевые действия велись с использованием военной силы. «Военное столкновение происходило лобовым образом — противники сталкивались непосредственно, а победа зависела от того, у кого вооружение и техника более совершенны, кто имеет численный перевес в живой силе. Сама победа измерялась количеством потерь с той или иной стороны и установлением военного контроля над захваченной территорией с другой. Это категории войны эпохи модерна, — подчеркивает директор Центра геополитических экспертиз В. Коровин. — С наступлением информационной эпохи, известной в парадигмальном смысле как эпоха постмодерна, данный подход изменился» (там же). Поэтому в информационную эпоху военная победа над противником может быть одержана невоенными средствами.

По мнению автора, схематически это можно представить следующим образом: национальное государство, которое лежит в основе современного мироустройства, рассматривается стратегами сетевых войн в виде концентрических кругов. В центре находится лидер, как правило, это глава государства (например, президент той или иной страны), вокруг которого располагаются политические элиты, затем экспертное сообщество, которое формирует политические смыслы и медиапространство, переводящее все на язык масс. Следующий слой — это сами массы: общество, население страны. Наконец, в качестве наружного слоя выступает армия, вооруженные силы как средство защиты всей этой концентрической конструкции. «Основой стратегии, которая получила название Effects-bases operations (операции, основанные на эффектах или “на базе эффектов” — ОБЭ), является то, что агрессия в отношении такой модели государства осуществляется не извне, т. е. не против вооруженных сил, не напрямую... — подчеркивает В. Коровин. — Более эффективным становится так называемая концепция ведения войны изнутри наружу» (там же).

Первый удар наносится по центру этой системы, т. е. по лидеру, путем идеологического, идейного воздействия на первое лицо государства или его замены и даже физического устранения.

Наглядным примером являются события конца 1980 — начала 1990-х годов в нашей стране, когда американские политики активно «работали» с М. Горбачевым, что в конечном итоге привело к распаду СССР и замене лидера на еще более прозападного — Б. Ельцина, который опирался на атлантистски ориентированные элиты. После этого произошло «переформатирование» в проамериканском, прозападном ключе экспертного и медийного сообщества. Затем «перепрограммировалось» население, являющееся продуктом воздействия медиапространства. И наконец, последний, внешний круг — армия — разлагалась под воздействием всей этой конструкции, трансформация которой как раз и происходила по линии «изнутри — наружу».

С приходом к власти В. Путина также была осуществлена смена лидера — центра конструкции. Однако это повлекло за собой кардинальную смену курса, прежде всего в вопросах внешней политики и в отношении к такому понятию, как суверенитет. Президент Российской Федерации, пишет автор, «начал восстанавливать патриотический баланс внутри страны, утверждая ценности суверенитета как базовые. Конечно, во многом он оказывался и до сих пор находится под влиянием либерального окружения, но, тем не менее, процесс пошел в обратную сторону» (там же). В результате отношение США и Запада к России стало негативным, а Президент РФ переместился в плеяду лидеров государств, входящих, по американским представлениям, в «ось зла».

В настоящее время для реализации проекта США по десуверенизации и распаду нашей страны на «осколочные» государства (который временно приостановлен) против России начата сетевая война. «Сценарий сетевого переворота был запланирован на 2008-й, но из-за уступки, которую Путин осуществил в пользу Запада, назначив преемником Медведева, этот сценарий был отложен, но никак не отменен, — считает В. Коровин. — Следующая попытка — массовые выступления в декабре 2011 — начале 2012 — также не дала желаемого для Запада результата» (там же).

По мнению экспертов, сетевые технологии будут использованы таким образом, что у России не будет возможности ответить с помощью сил ядерного сдерживания, которые являлись таковыми только в период обычных войн и обычных вооружений. Мир столкнулся с совершенно новыми технологиями. И, к сожалению, в России пока нет центров, которые могли бы ответить на эти новые технологии и вызовы. Таким образом, Президент Российской Федерации В. Путин стоит ныне фактически перед выбором: либо продолжать отстаивать суверенитет России, либо подчиниться диктату США и Запада, чтобы сохранить стабильность в стране и избежать «оранжевой революции». И от этого выбора зависит историческая судьба России.

ИНФОРМАЦИОННЫЕ ВОЙНЫ

Термин «информационная война» появился в начале 1990-х годов в связи с развитием новых информационных технологий и нового глобального информационного общества, о чем уже мы упомянули ранее. «Современные информационные

технологии находят применение во всех сферах общественной жизни, изменяют мировоззрение людей, трансформируют еще вчера казавшиеся вполне устоявшимися образование, бизнес, управление государством, создавая тем самым новую информационную среду существования человека — информационное общество... Информационная революция сделала возможным, в числе прочих, и такое явление, как информационная война» (Петрова, 2016: 427).

В настоящее время термин «информационная война» в широком смысле используется для обозначения противоборства в инфосфере и средствах массовой информации для достижения различных политических целей (Международная безопасность ... , 1998: 66).

Информационная война представляет собой одну из новых форм борьбы между государствами, а также систему мер, осуществляемую одним государством с целью подрыва информационной безопасности другого государства, при одновременной защите от подобных действий противостоящей стороны. Целью такого противоборства является нарушение информационной безопасности другого государства, а в ряде случаев целостности (устойчивости) системы государственного и военного управления других государств, эффективное информационное воздействие на их руководство, политическую элиту, системы формирования общественного мнения и принятия решений, а также обеспечения собственной информационной безопасности (Глобалистика ... , 2003: 387).

Если главными объектами воздействия и защиты при информационно-технической борьбе являются информационно-технические системы (системы связи, телекоммуникационные системы, радиоэлектронные средства), то при информационно-психологической борьбе — психика политической элиты и населения противостоящих сторон, системы формирования общественного сознания, мнения, выработки и принятия решений. Объектами воздействия в информационных войнах могут являться: информационно-технические, информационно-аналитические, информационно-технические системы, включающие человека; информационные ресурсы; системы формирования общественного сознания и мнения, базирующиеся на средствах массовой информации и пропаганды; психика человека (там же: 381).

ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКАЯ ВОЙНА

Как правило, об информационно-психологической борьбе речь идет в тех случаях, когда информационное оружие прямо или опосредованно используется против психики человека (или социальной группы). Под информационно-психологической войной понимается «латентное воздействие информации на индивидуальное, групповое и массовое сознание при помощи методов пропаганды, дезинформации, манипулирования с целью формирования взглядов на социально-политическую организацию общества через изменение ценностных ориентаций и базовых установок личности» (Кунакова, 2012: 93).

В ходе информационных войн, как показывает их уже нынешняя практика, используется специальное структурирование информации, организация ее подачи, манипулирование, дозирование, направленное на использование информационных средств и технологий с целью воздействия на сознание людей и через него на содержание общественной ситуации в целом. Злоупотребление информацией

в политических целях «постепенно приняло форму особой войны, где средством поражения выступает “мягкое” информационно-психологическое оружие» (Глобалистика … , 2003: 388).

Особенность деструктивных акций информационного (точнее было бы сказать — дезинформационного) типа состоит в том, что они могут вестись на чужой территории, в любой точке информационного пространства, постоянно, анонимно и главное — незаметно. «Информационная война по своей сути, — пишет Е. К. Петрова, — это коммуникативная технология воздействия на массовое сознание. Целью этого воздействия является изменение картины мира той аудитории, на которую направлено воздействие (то есть изменения в массовом сознании противника)» (Петрова, 2016: 429). При этом объектом нападения выступает культурное пространство противника, его сознание, и он долгое время вообще может не осознавать, что стал объектом нападения или управления извне.

Информационные войны могут носить как военный, так и невоенный характер. Что касается невоенной формы информационной войны, то она представляет собой целенаправленное воздействие информационными технологиями одной страны на информационные, властные и управленческие системы другого государства, а также сознание населения с целью его деформации и насильственного навязывания своей культуры и идеологии вместо военных действий. Видный российский эксперт в этой области Л. И. Шершнев определял такую форму враждебного воздействия как «манипулятивную». Главным ее средством, считает он, являются стратегия «непрямых действий», «организованный хаос», «подрывные операции, деструктивное информационное, психологическое воздействие на индивидуальное, групповое и массовое сознание людей» (Шершнев, 2000: 9). По мнению автора, такая война «бьет по сущностной основе человека, его культурному ядру, нравственности, ментальности… превращает целые народы в объект манипулирования и обмана, формирует упрощенного, усредненного и легко внушаемого человека... навязывает им чуждые психологические комплексы» (там же: 10). Следует учитывать, что современное качество технологий и формирование единого информационного пространства позволяет осуществлять такие дезинформационные операции в глобальном масштабе.

Последствия информационной войны могут иметь самый различный характер. К ним можно отнести: получение выгоды в политической, экономической, финансовой и военных сферах; трансформацию общественного сознания, дискредитацию общественно-политических порядков; информационное прикрытие политического, экономического и военного влияния; нарушение информационной безопасности государства, общества и личности; нарушение сетей и информационных систем; добывание конфиденциальной информации и вскрытие системы доступа к электронным системам и сетям и т. п. (Глобалистика … , 2003: 386–387).

В XXI в. методы социологии и социальной психологии, а также высокие технологии, средства массовой информации, Интернет многократно расширили возможности управления обществом. «Оранжевые революции», в ходе которых огромные массы людей, следуя ложным смыслам и символам, совершают действия, которые в действительности противоречат их интересам и потребностям, стали эффективным инструментом информационных войн. Огромную эффективность такого образа действий показал украинский кризис.

«За постсоветский период Российская Федерация в различных формах оказала экономическую помощь Украине в объеме более $ 200 млрд, в то же время США вложили $ 5 млрд. Но эти средства были вложены в сферу массового сознания. Украинские коллеги рассказывают, — пишут В. Иванов и Г. Малинецкий, — что школьные учебники с акцентом на возрождение “украинства”, отпечатанные в США, были доставлены в страну уже в конце 1991 года. Ставка на трансформацию массового сознания жителей Украины позволила переориентировать элиты, осуществить государственный переворот, развязать гражданскую войну и нанести огромный, разнообразный ущерб России, изменить ее место в мировом геополитическом и геоэкономическом пространстве» (Иванов, Малинецкий, 2015: 28).

В XXI в. возрастает угроза информационных войн. Крушение СССР и развал Югославии, цветные революции во многих странах мира свидетельствуют о том, что невоенные средства и формы борьбы приобретают системных характер. Причем следует учитывать, что они применяются постоянно и в мирное, и в военное время. По существу, можно утверждать, что возникает новое феноменальное явление в области политического противоборства. А именно возможность достижения политических целей, социального, экономического и духовного распада государства, навязывания соответствующих моделей развития без применения военной силы — путем ведения целенаправленной информационной, идеологической, психологической и иных форм борьбы.

Прошедшие двадцать пять лет показывают, что Россия оказалась совершенно неподготовленной к новому типу войн, и прежде всего — информационной, направленной на подрыв национальной культуры и духовно-нравственных ценностей и замену их чуждыми — «западными». Вместе с тем, несмотря на превосходство противника в умении вести информационную войну, в последние годы ситуация складывается в целом в пользу России. Наконец, в Военной доктрине Российской Федерации (от 26 декабря 2014 г.) официально признано, что против России ведется информационная война. К основным внешним и внутренним опасностям отнесена «деятельность по информационному воздействию на население, в первую очередь на молодых граждан страны, имеющая целью подрыв исторических, духовных и патриотических традиций в области защиты Отечества» (Военная доктрина … , 2014: Электронный ресурс). Статистика также свидетельствует о произошедшем переломе в информационной войне в пользу России. С 2007 по 2015 г. число россиян, которые не доверяют западным СМИ, увеличилось в семь раз — до 50% (Более половины россиян … , 2015: Электронный ресурс).

Однако в настоящее время США и Запад не только пролонгируют антироссийские санкции, но и открыто заявляют о разработке новых проектов по ведению информационной войны против нашей страны, что констатировал недавно пресс-секретарь Президента РФ Д. Песков: «…сейчас мы находимся в состоянии информационной войны с законодателями моды в информационном пространстве, прежде всего с англосаксами, их СМИ» (Латухина, 2016: Электронный ресурс). А это означает, что Россия должна быть готова к новому витку информационной войны.

ИНФОРМАЦИОННО-ТЕХНИЧЕСКАЯ БОРЬБА

В узком смысле слова термин «информационная война» применяется для обозначения военного противоборства в военной инфосфере для достижения «одно-

сторонних преимуществ в получении, сборе, обработке и использовании информации на поле боя (в операции, сражении)» (Международная безопасность ... , 1998: 66). Такая форма представляет собой систему мер, направленных на достижение информационного превосходства путем воздействия на информацию и информационные системы противника при одновременной защите собственной информации и своих информационных систем. Назовем этот тип войны информационно-технической борьбой. Основные усилия в таком случае концентрируются не на поражении личного состава и боевой техники противника, а на выведении из строя его компьютерных сетей и сетей связи главных штабов.

Информационные компьютерные и телекоммуникационные технологии могут использоваться вооруженными силами как средства подавления войск противника, дезорганизации его управления, внесения хаоса в работу вычислительных центров и сетей связи, уничтожения пунктов военно-политического руководства и командования войск, дезинформации и морально-психологического подавления личного состава его армии, а также населения.

Фактически еще в ходе вьетнамской войны широко применялось новое средство информационного воздействия на население всей страны — телевидение. Информационные средства использовались также во время вторжения войск США в Гренаду (1983 г.), на Панаму (1989 г.). Однако первой действительно полномасштабной информационной войной следует считать войну США и НАТО в Персидском заливе в 1991 г. против Ирака. На территорию Ирака было переброшено около 500 тыс. солдат стран антииракской коалиции, еще 300 тыс. были в резерве. «Однако в большей степени победа была одержана благодаря деятельности 2000 сотрудников, не выезжавших из США и сидевших за терминалами. Именно они разрушали системы управления, наводили самолеты на цели, перехватывали секретные сообщения, блокировали банковские счета иракских офицеров и их родственников» (Иванов, Малинецкий, 2015: 28). Эта война наглядно показала, что защищаться в данной сфере очень трудно. В Ираке широко применялись современные информационные и автоматические системы управления. В. Иванов и Г. Малинецкий пишут: «...по войскам и другим объектам Ирака были нанесены высокоточные огневые удары, американские мобильные генераторы “Сэдкребс” внесли полный хаос в длинноволновую связь, что в значительной мере парализовало управление войсками Ирака. Он был вынужден прекратить войну и согласиться со всеми требованиями, которые предъявляли западные государства» (там же: 81).

Опыт войны в Ираке был использован затем в Югославии и многих других странах, где современные информационные средства также нашли масштабное и многоплановое применение. Это свидетельствует о том, что воздействие на информационный ресурс государства представляет новый источник угроз национальной безопасности в XXI в..

КИБЕРВОЙНЫ

Виртуальное пространство, киберпространство фактически с 1970-х годов стало еще одним пространством, в котором проходят конфликты, а в настоящее время идет подготовка к намного более масштабным кибервойнам — войнам будущего. Кибервойна представляет собой один из видов войны, основанный на совре-

менных информационных технологиях. «Это не самостоятельный вид противоборства, кибервойна всегда является составной частью *информационной войны* и в целом выступает элементом полномасштабной военной кампании, включающей как недавно возникшие, так и более привычные способы борьбы. Кибервойна не существует вне традиционной, хотя конкретные кибероперации могут проводиться (и ныне проводятся во многих регионах планеты) вне войны как таковой. Кибервойна представляет собой угрозы атак и со стороны отдельных хакеров, и со стороны террористических групп и государств. Она предполагает нарушение деятельности или полный вывод из строя систем управления государством и вооруженными силами за счет воздействия на компьютерные сети, в результате чего государственные и военные институты могут оказаться полностью парализованными и неспособными к организации сопротивления агрессору» (Капто, 2013: 616).

В последние годы наряду с доктринальной институализацией кибервойны происходит становление ее понятийного аппарата: окончательно утвердились такие термины, как кибертехнологии, киберпространство, кибератака, кибероружие, кибершпионаж, киберагрессор, киберструктура, кибервраг, государственные кибервойска, киберконфликт, киберугроза, киберпреступность, кибертерроризм, киберинцидент, интернет-зависимость, кибербезопасность. «Под “кибербезопасностью” понимают свойство киберпространств, киберсистем и т. д. противостоять намеренным и ненамеренным угрозам, а также реагировать на них и восстанавливаться в случае реализации этих угроз. Кибербезопасность (как и употребляемое наряду с ним понятие “кибероборона”) включает также развитие наступательных возможностей — защита и атака в этом смысле неразделимы» (там же: 617).

В середине 1980-х годов научным сотрудником Американского института безопасности и разведки Б. Колином был введен термин «кибертерроризм» для обозначения возможных террористических действий в виртуальном пространстве. Причем его автор считал, что человечество столкнется с реальным кибертерроризмом только в XXI в. Однако первые кибератаки были зафиксированы уже в начале 1990-х годов.

Так, первым случаем применения кибероружия считается взрыв на сибирском газопроводе «Уренгой — Сургут — Челябинск» в 1982 г., который имел стратегическое значение для Советского Союза (многие СМИ связывали его с планом диверсии против экономики СССР президента США Р. Рейгана).

В конце 1990-х годов была проведена кибератака под названием «Лабиринт лунного света» на серверы НАСА, Министерства обороны США и ряда университетов США (инициированная якобы Китаем). В середине 2000-х годов известна хакерская операция «Титановый дождь» против НАСА и трех американских фирм, связанных с оборонной промышленностью (исполнителем которой также считается Китай).

Первая межгосударственная кибервойна произошла в апреле 2007 г. в связи с решением эстонского правительства перенести памятник Воину-освободителю из центра Таллина на его окраину, когда атакам подверглась система «электронного правительства», в чем ряд западных стран обвинил Россию (хотя впоследствии выяснилось, что кибератаки совершались с территорий 76 стран). В 2008 г. бы-

ло осуществлено кибернападение на одну из закрытых сетей военного ведомства США. Это привело к утечке данных из американских военных систем, в результате которой зарубежными спецслужбами была получена информация технического, оперативного и разведывательного характера военного ведомства США и их партнеров по НАТО. В этом же году атаке подверглись компьютерные сети Центрального командования вооруженных сил США (там же: 617–618).

Наглядным примером боевого использования виртуального пространства стала масштабная диверсия весной 2010 г. в ядерном комплексе Ирана, на тщательно охраняемом заводе по разделению изотопов в г. Натанзе. Однако компьютерный вирус, специально созданный для этой цели, перевел центрифуги в недопустимый режим работы, что привело к выходу их из строя и отбросило ядерную программу Ирана на несколько лет (Иванов, Малинецкий, 2015: 28).

В июле 2011 г. хакеры взломали компьютерную сеть Министерства обороны США и похитили 24 тыс. документов, которые имели гриф секретности и содержали данные о конструкции новейших американских самолетов и подводных лодок, информацию о последних разработках США в области спутниковых систем наблюдения и компьютерной безопасности. 22 сентября 2011 г. произошла компьютерная атака на ведущие корпорации японского военно-промышленного комплекса. Полученная информация «перекачивалась» на 14 сайтов за границей, в том числе в Китае, Гонконге, США и Индии.

Исключением не является и наша страна, которая также подвергается кибернападениям: «...только на сайты Президента РФ, Государственной Думы и Совета Федерации ежедневно осуществляется до 10 тыс. атак; от хакеров страдает и российский бизнес. В этом контексте, а также ввиду отсутствия четкой стратегии компьютерной безопасности на государственном уровне разработка концептуальных основ кибервойн с учетом уже накопленного зарубежного опыта является актуальной задачей» (Капто, 2013: 618). По оценкам экспертов, ежегодный ущерб от кибератак в мире составляет более 0,5 млрд долл.

Исследования показывают, что в режиме кибервойны, к которой готовятся компьютерные войска, созданные во многих ведущих странах мира, результаты дезорганизации компьютерных систем, перехвата управления рядом объектов могут во много раз превзойти нынешние ожидания. В связи с этим актуальнейшей становится задача выработки международных соглашений, которые бы определяли «правила игры» в киберпространстве — для граждан, бизнеса и государства. Как известно, США блокировали резолюцию по кибербезопасности на уровне ООН, так как считали, что доминируют в киберпространстве, поэтому ни одна страна в мире не может с ними конкурировать. В действительности оказалось, что Соединенные Штаты не менее уязвимы перед угрозой кибератак со стороны как отдельных хакеров, так и террористических групп или тех или иных государств. Темпы разрастания опасности свидетельствуют о том, что если недавно, согласно мнению экспертов, лишь пять стран были способны вести полномасштабную кибервойну (США, КНР, Индия, Израиль, Россия), то в настоящее время наступательными возможностями разного уровня обладают более 100 стран (там же: 624).

Поскольку кибероружие становится все более доступным и простым в использовании, возникает вопрос: как обеспечить безопасность мирового интернет-про-

странства? Речь идет о необходимости выработки универсального всеобъемлющего международно-правового документа, который должен «констатировать наличие угроз международной информационной безопасности военно-политического, преступного, в том числе террористического, характера и предусматривать сценарии осуществления совместных мер по минимизации ущерба национальным интересам отдельных государств и интересам международного сообщества в целом» (там же: 625). В разработке такого документа заинтересована и Россия, как и в создании компьютерных войск (которые формируются во многих странах мира) в целях обеспечения как собственной информационной безопасности, так и информационной безопасности других государств.

ЗАКЛЮЧЕНИЕ

Очевидно, что санкции Запада носят долговременный характер (введены даже не на годы, а скорее, на десятилетия подобно поправке Джексона-Веника[1]) и включают в себя полный спектр инструментов экономического, политического и информационного давления на Россию. В конечном счете они направлены на дестабилизацию социально-экономической ситуации, смену лидера и политического режима в нашей стране. Однако необходимо осознавать, что они наносят ущерб не только нашей экономике, но прежде всего самим странам Запада, в частности Евросоюза, которые находятся в глубочайшем кризисе.

ПРИМЕЧАНИЕ

[1] Поправка 1974 г. к Закону о торговле США, ограничивающая торговлю со странами, препятствующими эмиграции, а также нарушающими другие права человека.

СПИСОК ЛИТЕРАТУРЫ

Более половины россиян перестали доверять зарубежным СМИ (2015) [Электронный ресурс] // Lenta.ru. 7 мая. URL: https://lenta.ru/news/2015/05/07/distrust/ (дата обращения: 12.04.2016).

Военная доктрина Российской Федерации (2014) [Электронный ресурс] // Российская газета. 30 декабря. URL: https://rg.ru/2014/12/30/doktrina-dok.html (дата обращения: 12.04.2016).

Глазьев, С. (2015) Украинский кризис: от американской агрессии к мировой войне? М. : Книжный дом. 352 с.

Глобалистика. Энциклопедия (2003) / ред. И. И. Мазур, А. Н. Чумаков. М. : ЦНПП Диалог, ОАО «Издательство “Радуга”». 1328 с.

Иванов, В., Малинецкий, Г. (2015) Наука и войны будущего (доклад Изборскому клубу) // Изборский клуб. Русские стратегии. № 5 (29). С. 6–37.

Капто, А. С. (2013) Кибервойна: генезис и доктринальные очертания // Вестник РАН. № 7. С. 616–625.

Коровин, В. (2013) «Значит, снова война» [Электронный ресурс] // Взгляд. 13 декабря. URL: http://vz.ru/opinions/2013/12/13/663426.html (дата обращения: 12.04.2016).

Кунакова, Л. Н. (2012) Информационная война как объект научного анализа (понятие и основные характеристики информационной борьбы) // Альманах современной науки и образования. № 6. С. 93–96.

Латухина, К. (2016) Песков: РФ находится в состоянии информационной войны с англосаксами [Электронный ресурс] // Российская газета. 26 марта. URL: http://rg.ru/2016/

03/26/peskov-rf-nahoditsia-v-sostoianii-informacionnoj-vojny-s-anglosaksami.html (дата обращения: 12.04.2016).

Международная безопасность и обороноспособность государств. Понятия, определения, термины (1998) / под общ. ред. О. К. Рогозина. М. : Конверс АВИА. 488 с.

Петрова, Е. В. (2016) Информационные войны и биосоциальная природа человека // Философия войны и мира (к 70-летию Великой Победы). Материалы Всероссийской научно-практической конференции «Философия войны и мира: к 70-летию Победы в Великой Отечественной войне». 28–29 апреля 2015 г. Москва. Институт философии РАН. М. : Российское философское общество, ООО «СиДиПрессАрт». С. 426–440.

Фарамазян, Р., Борисов, В. (2001) Экономические санкции в системе мер по поддержанию международной стабильности и безопасности // Пути к безопасности. Вып. 1/21. С. 7–14.

Шершнев, Л. И. (2000) Россия и мир: движение к новой безопасности в XXI веке // Безопасность. № 1. С. 5–13.

Дата поступления: 12.03.2016 г.

NEW TYPES OF WAR AND RUSSIA'S NATIONAL SECURITY

I. A. Krylova

(Institute of Philosophy, Russian Academy of Sciences)

The article provides a social and philosophical analysis of the new generation of warfare. In the unipolar world dominated by the USA, the threat of economic, 'elite', networked, informational and cybernetic wars has dramatically increased, thus exacerbating the situation already destabilized by the nuclear threat. These new types of warfare are characterized by a greater role of non-combat factors aimed at the destruction of social and economic foundations of a state, its place in the international system, its cultural and moral values, social order and political regime, all made possible by new types of weapon and new styles of warfare. Russia is now facing the threat of war in both its old and new formats.

Under globalization, economic warfare have become mainstream. Leading powers in the global system strive to achieve their goals by exerting economic pressure on other states — e.g., by introducing economic sanctions. Contemporary 'elite' wars make wide use of cutting-edge discoveries in applied psychology, which help model the political personae of global leaders, their strengths and weaknesses and predict their reactions and decisions. Another threat for Russia lies in networked warfare of military origin. Without resorting to real weaponry, perpetrators of such war can achieve a real military victory, i.e. take control over a territory.

Information wars are a new type of struggle between states. They include a series of actions aimed at undermining the information security of an enemy state. Information war can damage the enemy's infrastructure (communication and telecommunication lines, radio and electronic devices) and/or the morale of the political elites and populations, the public opinion and the mechanism of decision making. Another subtype of information war in the sphere of technology is to achieve informational superiority by simultaneously attacking the enemy's informational systems and protecting those on your side. Virtual space and cyberworld have also become a battleground for conflicts of these new types.

Keywords: Russia; USA; the West; economic warfare; 'elite' war; networked warfare; information wars; psychological warfare; technological struggle; cyberwars; national security

REFERENCES

Bolee poloviny rossiian perestali doveriat' zarubezhnym SMI (2015). *Lenta.ru*, 7 May [online] Available at: https://lenta.ru/news/2015/05/07/distrust/ (access date: 12.04.2016). (In Russ.).

Voennaia doktrina Rossiiskoi Federatsii (2014). *Rossiiskaia gazeta*, 30 December [online] Available at: https://rg.ru/2014/12/30/doktrina-dok.html (access date: 12.04.2016). (In Russ.).

Glaz'ev, S. (2015) *Ukrainskii krizis: ot amerikanskoi agressii k mirovoi voine?* Moscow, Knizhnyi dom. 352 p. (In Russ.).

Globalistika. Entsiklopediia (2003), ed. I. I. Mazur and A. N. Chumakov. Moscow, TsNPP Dialog, OAO Izdatel'stvo «Raduga». 1328 p. (In Russ.).

Ivanov, V. and Malinetskii, G. (2015) Nauka i voiny budushchego (doklad Izborskomu klubu). *Izborskii klub. Russkie strategii*, no. 5 (29), pp. 6–37. (In Russ.).

Kapto, A. S. (2013) Kibervoina: genezis i doktrinal'nye ochertaniia. *Vestnik RAN*, no. 7, pp. 616–625. (In Russ.).

Korovin, V. (2013) «Znachit, snova voina». *Vzgliad*, 13 December [online] Available at: http://vz.ru/opinions/2013/12/13/663426.html (access data: 12.04.2016). (In Russ.).

Kunakova, L. N. (2012) Informatsionnaia voina kak ob»ekt nauchnogo analiza (poniatie i osnovnye kharakteristiki informatsionnoi bor'by). *Al'manakh sovremennoi nauki i obrazovaniia*, no. 6, pp. 93–96. (In Russ.).

Latukhina, K. (2016) Peskov: RF nakhoditsia v sostoianii informatsionnoi voiny s anglosaksami. *Rossiiskaia gazeta*, 26 Mart [online] Available at: http://rg.ru/2016/03/26/peskov-rf-nahoditsia-v-sostoianii-informacionnoj-vojny-s-anglosaksami.html (access date:12.04.2016). (In Russ.).

Mezhdunarodnaia bezopasnost' i oboronosposobnost' gosudarstv. Poniatiia, opredeleniia, terminy (1998), ed. O. K. Rogozina. Moscow, Konvers AVIA. 488 p. (In Russ.).

Petrova, E. V. (2016) Informatsionnye voiny i biosotsial'naia priroda cheloveka. In: *Filosofiia voiny i mira (k 70-letiiu Velikoi Pobedy). Materialy Vserossiiskoi nauchno-prakticheskoi konferentsii «Filosofiia voiny i mira: k 70-letiiu Pobedy v Velikoi Otechestvennoi voine». 28–29 aprelia 2015 g. Moskva. Institut filosofii RAN*. Moscow, Rossiiskoe filosofskoe obshchestvo, OOO «SiDiPressArt». Pp. 426–440. (In Russ.).

Faramazian, R. and Borisov, V. (2001) Ekonomicheskie sanktsii v sisteme mer po podderzhaniiu mezhdunarodnoi stabil'nosti i bezopasnosti. *Puti k bezopasnosti*, vol. 1/21, pp. 7–14. (In Russ.).

Shershnev, L. I. (2000) *Rossiia i mir: dvizhenie k novoi bezopasnosti v XXI veke*. Bezopasnost', no. 1, pp. 5–13. (In Russ.).

Submission date: 12.03.2016.

Крылова Ирина Анатольевна — доктор философских наук, ведущий научный сотрудник сектора социальной философии Института философии РАН. Адрес: 109240, Россия, г. Москва, ул. Гончарная, д. 12, стр. 1. Тел.: +7 (495) 697-98-93. Эл. адрес: tatyanawings@gmail.com

Krylova Irina Anatolievna, Doctor of Philosophy, Leading Research Fellow, Institute of Philosophy, Russian Academy of Sciences. Postal address: 12 Bldg.1 Goncharnaya St. 109240 Moscow, Russian Federation. Tel.: + 7 (495) 697-98-93. E-mail: tatyanawings@gmail.com