§10 ВОЙНА И МИР

Старкин С. В.

ПРОТИВОСТОЯНИЕ В КИБЕРПРОСТРАНСТВЕ В КОНТЕКСТЕ РАЗВИТИЯ ВОЕННОЙ СТРАТЕГИИ

Аннотация. *Проблемные вопросы, поставленные автором в данной работе, сформулированы следующим образом: во-первых, что фактически означает концепт «кибервойна» для политикоформирующих кругов? Во-вторых, насколько концепт «кибервойна» применим для понимания глобальных тенденций, будущего военной стратегии и инструментов ее реализации? В статье автор проводит исследование стратегического контекста, в котором в настоящее время проходят дебаты о «кибервойне» (в частности, усматриваемое некоторыми исследователями снижающееся значение прямой военной силы), а также анализирует сложность достижения действительного стратегического эффекта посредством «чистых» кибератак. В работе, с учетом поставленных задач, использованы традиционные для гуманитарных дисциплин методы сравнительного анализа, исследование case studyes, теория принятия политических решений. Основным выводом проведенного исследования является то, что военная кибермощь не обладает настолько стратегически мощным потенциалом, как его рисовали в последние годы. По мнению автора, есть все основания полагать, что, подобно военно-воздушной мощи, она будет представлять собой важный элемент в будущих совместных операциях сухопутных, воздушных и морских сил, но концепция кибервойны, как стратегически решающая форма межгосударственного противостояния, представляет собой вводящее в заблуждение и бессмысленное отвлечение сил и средств на негодный объект.*

Ключевые слова: *кибербезопасность, киберреволюция, противостояние в киберпространстве, киберугрозы, национальная безопасность, международная безопасность, информационная безопасность, Россия, США, НАТО.*

Работа поддержана (частично поддержана) грантом (соглашение от 27 августа 2013 г. № 02.B.49.21.0003 между МОН РФ и ННГУ) The research is supported (partly supported) by the grant (the agreement of August 27, 2013 № 02.B.49.21.0003 between The Ministry of education and science of the Russian Federation and Lobachevsky State University of Nizhni Novgorod)

DOI: 10.7256/1812–8696.2015.3.14566

Review. *The problematic issues raised by the author in this paper, are worded as follows: firstly, what does the concept of «cyberwar» actually mean for the political establishment? Secondly, to what extent is the concept of «cyberwar» applicable for the understanding of global trends, the future of military strategy and instruments for its implementation? The author is conducting a study of the strategic context in which there are currently undergoing debates about «cyberwar» (in particular, the declining value of direct military force perceived by some researches), and also analysing the difficulty of achieving the real strategic effect through «pure» cyber attacks.In this paper, taking into account the objectives, traditional for the humanities comparative methods are used, as well as case studies, and the theory of political decision-making.The main conclusion of the study is that the military cyberpower does not have enough of strategically strong potential, as it was painted in recent years. According to the author, there is every reason to believe that, like military air power, it will be an important element in future joint operations of ground, air and naval forces; but the concept of cyberwar as a strategically crucial form of interstate conflict is misleading and meaningless diversion of efforts and resources on useless objects.*

Keywords: *international security, national security, cyber-threats, confrontation in cyberspace, cyberrevolution, cybersecurity, information security, Russia, USA, NATO.*

В настоящее время так называемое киберпространство представляет собой один из наиболее стимулирующих работу мысли терминов в научных и экспертных дискуссиях. Выдвигаются серьезные доводы «за» и «против» увеличения влияния мероприятий в киберпространстве на проведение военных операций. Ряд исследователей утверждает, что взаимодействие в рамках сетей «меняет все», возможно, даже то, как люди мыслят — базовую природу человека [1]. Другая группа экспертов указывает, что возможности виртуального мира всего лишь позволяют индивиду, государству и обществу осуществлять повседневные действия, но несколько иным способом [2].

Проблемные вопросы, интересующие нас в данной работе, можно сформулировать следующим образом: что фактически означает концепт «кибервойна» для политикоформирующих кругов, озабоченных балансировкой целей, способов и средств в современном вооруженном конфликте? Насколько данный концепт применим для понимания глобальных тенденций, будущего военной стратегии и инструментов ее реализации?

Ответы на эти вопросы можно получить, во-первых, в ходе исследования стратегического контекста, в котором в настоящее время проходят дебаты о «кибервойне» (в частности, усматриваемое некоторыми исследователями снижающееся значение прямой военной силы); во-вторых, на основе анализа формирования военного киберпотенциала с учетом соответствующих исторических событий, например, эволюции теории воздушной мощи, популярной в период между двумя мировыми войнами; и, в-третьих, в результате обсуждения сложности достижения действительного стратегического эффекта посредством «чистых» кибератак.

Популярный дискурс по вопросам кибервойны имеет тенденцию фокусироваться на уязвимости «физической составляющей» киберпространства от кибератак и методах, с помощью которых она может позволить даже слабым государствам и негосударственным акторам осуществлять противодействие сверхдержавам, в ряде случаев без человеческих жертв. Китайские авторы Киао и Ванг — авторы текста о будущей войне «*Неограниченная Война*» — особенно впечатлены следующей идеей: «Поле боя находится рядом с вами и враг в сети. Только не ощущаются ни запах пороха, ни крови … Один хакер с одним модемом причинят врагу такие ущерб и потери, которые будут почти равны ущербу и потерям, понесенным во всей конвенциональной войне» [3].

Противостояниае в киберпространстве стимулирует экспертов рассматривать движущие силы перемен в комплексе, с учетом соответствующих исторических прецедентов, которые при узком фокусировании исключительно на технологиях можно упустить. Соответствующий стратегический контекст — не просто отрезок времени с момента изобретения микрочипа, скорее это более

DOI: 10.7256/1812–8696.2015.3.14566

чем столетний период, в течение которого, в результате сочетания ряда политических, экономических и технологических причин, влияние крупномасштабных военных столкновений неуклонно снижалось [4]. Одним из наиболее важных теоретических выводов К. Клаузевица в работе «*О войне*» было разграничение между «подлинной природой» войны и ее «характером»: в то время как последний параметр является весьма изменчивым, первый меняется очень медленно, если меняется вообще [5]. Есть основания предполагать, что зарождение военного киберпотенциала изменило характер войны, однако это не значит, что ее природа также трансформировалась каким-либо образом. Классическое положение реализма о том, что войны возникают из комплекса, в котором смешались страх, честь и личный интерес, не менее верно для современного противостояния в сетевых потоках в киберпространстве [6].

В истории военного искусства было немало прецедентов, когда технологические изменения обуславливали изменения правил ведения войны. Их можно использовать для анализа проблем, стоящих перед руководством России в настоящее время. Прежде всего, анализ исторического контекста позволит многое почерпнуть о значении военного киберпотенциала, рассмотрев его сквозь призму длящейся уже более века дискуссии о преимуществах военно-воздушной мощи (ее идеальное и фактическое тактическое и оперативное использование, оптимальная форма организации, доктрина в отношении других видов вооружений, и, предположительно, независимая стратегическая эффективность).

ВОЕННОЕ ИСКУССТВО И ПРОЦЕСС ПРИНЯТИЯ РЕШЕНИЙ

В 2005 г. американский исследователь Р. Смит в своей книге «*Польза силы*», заявил: «…Война, как она когнитивно известна большинству некомбатантов, война, как сражение на поле боя между сражающимися и военной техникой, война, как массовый решающий момент в споре по международным вопросам; такая война уже более не существует. » [7, P.1]. Однако основной тезис о «пользы силы» был изложен другим зарубежным ученым Н. Эйнджеллом в книге «*Великая иллюзия*»: «Человек … подходит к тому, чтобы реже использовать физическую силу, поскольку собранные им доказательства все больше и больше подталкивают его к выводу о том, что он может проще достичь того, к чему он стремится, используя другие средства» [8, P. 222].

Две мировые войны показали, что вера Эйнджелла в рациональность человечества перед лицом очевидной экономической бессмысленности войны в то время оказалась несвоевременной. Тем не менее, уверенность в том, что «большая война» устарела, оказалась чрезвычайно живучей. Сегодняшние дискуссии показывают, что многим западным и российским либеральным исследователям глобальные конфликты XX века показались аберрацией, а не нормой [9, P. 22]. Действительно, Х. Стрэчан, один из ведущих историков первой мировой войны, утверждает, что «центром, вокруг которого организуются наши идеи кластера войны, уже больше не будет большая война, которая и сама является теоретическим конструктом, выведенным из второй мировой войны, и едва ли с тех пор реализованным на практике» [10, P. 23]. Кроме того, появление термоядерного оружия у сверхдержав в 1950-е годы и его последующее распространение среди государств меньшего масштаба, увеличило разрушительный потенциал большой войны на много порядков больше того, что мог себе представить Эйнджелл, и этого было достаточно для того, чтобы удержать лидеров от ее использования в качестве рационального инструмента политики. Ни в коем случае это не означает, что войны исчезли. Они по-прежнему проявляются в различных формах во всем мире. События на Украине показывают, что концепции «выжженной земли» и воздушно-бомбовых ударов по мирным городам никуда не исчезли и могут быть полноценно реализованы в любое время в любой точке земного шара.

Очевиден и другой тезис. Если в прошлом войны могли приносить существенную материальную прибыль, ресурсы и технологии, то в настоящее время выгоды от победы, являются, в лучшем случае, сомнительными [11]. Для вооруженных сил существует возможность увязнуть в длительной истощающей ресурсы

DOI: 10.7256/1812–8696.2015.3.14566

войне. Можно утверждать, что одновременно с тем, что самое главное в современных войнах, как и было всегда, это нанесение ударов и уничтожение вооруженных сил противника, за пределами этой максимы военные должны следовать военному эквиваленту Клятвы Гиппократа: «Не нанеси ущерб, не вызванный необходимостью».

Насколько это похоже на призыв упоминавшегося Эйнджелла к тому, чтобы «этика, которая была разработана в соответствии с потребностями в западном обществе индивидуумов, также была применена и к сообществу наций, так как это общество становится в силу нашего развития более взаимозависимым» [8, P. 298]. При внимательном анализе можно отметить поразительное сходство между началом двадцатого века и современным периодом. Сегодня наблюдается разброс мнений относительно будущего характера ведения боевых действий, которые были далеко не решены в ходе событий первой и второй мировой войн. Хотя широко распространенная до первой мировой войны убежденность в том, что наземная война в XX столетии будет молниеносной, была опровергнута четырехлетним окопным «сидением», впоследствии сохранились существенные противоречия в штабах ведущих вооруженных сил относительно того, каким образом организовать, подготовить и оснастить сухопутные и военно-морских силы с учетом новых технологических разработок в авиации, системах связи и бронетехнике, появившихся в ходе войны.

Аналогично этому, в настоящее время идет бурное обсуждение вероятного характера будущей войны, которое вращается вокруг «правильных» уроков, извлекаемых из текущих конфликтов: в частности, в какой степени вооруженные силы должны быть подготовлены для ведения противоповстанческих действий, нетрадиционных войн, или для того, что обозначается еще более неуклюжим (но используемым западными штабистами) термином «Операции, Проводимые Вне Условий Войны». «Крестоносцы» настаивают, что вооруженные силы Запада должны адаптироваться, чтобы побеждать в войне, которую они ведут, либо они будут обречены на поражение, на потери личного состава и материально-технических средств, на существование в менее безопасном мире, в котором вредное влияние «глобальных мятежных действий» будет расти в недееспособных и теряющих дееспособность государствах. С другой стороны, «консерваторы» утверждают, что Ирак и Афганистан представляют собой девиации, и что адаптация сил Запада для ведения противоповстанческих действий является проявлением трусости, заменой первоклассной армии, готовой к ведению боевых действий, на второсортную машину, пригодную лишь для ведения борьбы с партизанскими движениями [12]. Политики в Великобритании и США, как представляется, сошлись в своих мнениях о композитной или «гибридной войне», согласно которой «будущее не предполагает наличие набора явно выраженных вызовов с альтернативными или различающимися методами, а их конвергенцию в мультимодальные или Гибридные Войны … Они могут вестись государствами, которые сочетают высокотехнологичные возможности, например противоспутниковое оружие, с терроризмом и средствами кибервойны» [13].

В январе 2010 года в своей речи в Международном институте стратегических исследований начальник генерального штаба ВС Великобритании, генерал Д. Ричардс использовал почти аналогичные термины для описания видения будущих войн: «конфликт в настоящее время, особенно потому, что его бóльшая часть эффективно ведется с использованием средств, созданных в ходе Революции в области телекоммуникаций, в основном идет за людей и вокруг них — за их сердца и умы в массовом масштабе. Это гораздо больше, чем просто кибератаки и кибероборона, хотя и это тоже важно … Войны между государствами происходят, и будут происходить, но некоторые не понимают, как эти войны будут вестись. Эти войны не будут вестись методом маневрирования обычных регулярных сил, готовых к отпору со стороны бронетанковых соединений или военно-морских флотов, но это будет, скорее, комбинация экономических действий, кибердействий и действий с использованием сил союзников» [14].

DOI: 10.7256/1812–8696.2015.3.14566

В отношении первой мысли, умышленно или по какой-либо иной причине, Ричардс повторил выводы социолога Мануэля Кастелльса о том, что партизанская война на не определенной некими границами территории представляет собой парадигматической тип конфликта информационно-виртуальной постмодернистской эпохи: «Конфликты нашего времени ведутся объединенными в сети социальными акторами, которые стремятся достичь своих контрагентов и свои целевые аудитории, решительно перейдя в мультимедийные коммуникационные сети» [15]. Но, что наиболее важно, генерал Ричардс также напомнил о начале XX века, когда описывал текущие стратегические и доктринальные концепты, которые он охарактеризовал как еще *более* широкие и амбициозные: «Это не то изменение, которое происходит один раз в жизни целого поколения, оно происходит еще реже. И во многих отношениях оно более фундаментальное, чем переход от лошади к танку. В то время как это занимает умы генералов, настоящие трансформации затрагивают все общество и, следовательно, оказывает воздействие на всю инфраструктуру безопасности» [14].

Наши рассуждения о характере современной войны не означают, что мы абстрагируемся от киберпространства. Стратегия не может быть применена к направленности войны и ее ведению, если она базируется на ложных представлениях о характере этой войны. В целом, однако, большая часть дебатов о кибервойне ведется следующим образом: они объединяют кибершпионаж, киберпреступность, взлом и нарушения прав интеллектуальной собственности, которые в большей или меньшей степени являются угрожающими или раздражающими для общества и поднимают их до уровня боевых действий, традиционно рассматриваемых западным обществом как юридически, морально и стратегически исключительными. Это проблематично во многих отношениях, и не в последнюю очередь с аналитической точки зрения, но это также и вопрос практики.

При этом масштабные дискуссии о кибервойне отвлекают нас от фактического стратегического контекста, который, образно говоря, является «миром конфронтации и конфликтов, а не миром войны и мира». Мы имеем дело с состоянием продолжающейся перманентной враждебности, существующей между различными государственными и негосударственными акторами, которая ведется, в основном, невоенными средствами (ключевые — пропаганда, политическая агитация и манипулирование общественным мнением), с использованием саботажа и пропаганды действием, невиданного уровня шпионажа, как коммерческого, так и политического, и киберпреступности. Все это проводится в рамках киберпространства, через него или в сочетании с ним. Коротко говоря, дискуссии о кибервойне обнажают тенденцию к «секьюритизации» проблемы, на которую традиционные силовые инструменты, в действительности, имеют сравнительно мало рычагов воздействия. Суть остается неизменной: «большая война», наиболее грубое проявление национальной мощи — как представляется, по ряду причин утратила свое место решающего арбитра событий в мире. Это тревожит западных стратегов, как всегда озабоченных увязкой военных средств с желаемыми политическими целями, и приводит их в замешательство.

Сторонники так называемой «виртуальной революции» декларируют тезис о том, что «она предоставляет новые возможности, но заново изобретает войну» [17]. Аналогичные заявления типичны для обсуждений военно-воздушной мощи, особенно популярных в Европе и Соединенных Штатах в межвоенный период. Историк М. Шерри описывает 1920-е годы как золотой век теоретизирования о самолетах. Он пишет: «Так как пророчества всегда предшествуют технологиям, они часто читаются как фантастические или бескровные абстракции, как если бы имели целью, как научная фантастика, менее изображать угрозы в будущем, чем выражать текущие тревоги» [15].

Параллели с современной эпохой весьма многообразны. Одна из наиболее очевидных — это используемые язык и стиль описания. В 1923 году английский стратег Дж. Ф. С. Фуллер назвал свою книгу о формах буду-

DOI: 10.7256/1812–8696.2015.3.14566

щих войн «*Реформирование войны*», заголовок которой отражает его веру в огромное преобразующее влияние новых технологий на способы ведения боевых действий [18]. Сторонники «*Виртуальной революции*» в контексте объяснения метода пакетной коммутации — одного из основных элементов цифровой связи с использованием сетей, при которой блоки данных передаются через соединение, которое открыто только в течение срока этой конкретной передачи — отмечают, что «данные пройдут всегда». Это парафраз характерной для 1930-х годов метафоры «бомбардировщик прорвется всегда» [15].

Основными характеристиками воздушной мощи являются: скорость — функция отсутствия препятствий на пути в воздушном пространстве, что делает воздушную мощь высокоманевренной; дальность — функция универсальности атмосферы, что делает средства воздушной мощи высокомобильными; высота — функция глубины воздушного пространства, что предоставляет возможность широко обозревать конфликт, развертывающийся внизу на земле. Кибермощь, как представляется, предлагает аналогичные характеристики, что, по-видимому, и объясняет, почему она была с энтузиазмом поддержана штабами военно-воздушных сил по обе стороны Атлантики. Кроме того, она предлагает и нечто другое, отсутствующее у ВВС — анонимность как функция архитектуры киберпространства [19]. Этот атрибут в одинаковой степени и вызывает тревогу, и привлекает, потому что он предлагает возможности для принятия неуловимых решений; если личность атакующего через киберпространство неизвестна, то нанести удар возмездия сложно, и, возможно, поэтому, эскалация военных действий, которая в основном сдерживала возникновение серьезных войн с 1945 г., может не быть эффективной. Короче говоря, кибермощь — это даже более соблазнительно для планирующих структур, чем воздушная мощь, в силу того, что она представляет возможность достижения цели без необходимости вообще какого-либо физического контакта (не говоря уже об обязательствах) в отношении других акторов.

РОЛЬ И МЕСТО КИБЕРПРОСТРАНСТВА В СОВРЕМЕННОЙ ВОЕННОЙ СТРАТЕГИИ

Констатируем, что военно-воздушная мощь не оправдала мечты ее наиболее активных адептов. Это не отрицает огромный вклад, который она внесла в современные боевые действия. Действительно, практически ничем не сдерживаемое господство в воздухе стало более или менее sine qua non [обязательным условием] западного «способа ведения войны». Эта максима является неоспоримым преимуществом в конвенциональных войнах XX и начала XXI века.

Вполне возможно, что армия двадцать первого века, в попытках воевать без «зонтика» военной кибермощи против противника, располагающего такой возможностью будет страдать, несмотря на тактическую проницательность, высокий дух личного состава и степень сложности других видов используемого оружия. Скорее всего, добиться независимого эффекта победы в войне не представится возможным — выиграть войну в течение 48 часов с нулевыми потерями, как это представлял себе Фуллер, не удастся.

Однако излишне напоминать здесь о «больших дебатах по поводу воздушной мощи», которые убедительно велись в других конфликтах Европы [20]. Скорее, полезней извлечь из дебатов то, что пока военная кибермощь, скорее всего, будет результативной, она не будет таковой сама по себе. Утверждения, сделанные в 1994 г. американской комиссией по защите национальной инфраструктуры», что «эта технология позволяет определять исход геополитических кризисов без единого выстрела» [21], следует рассматривать со скепсисом. Рассуждения о военно-воздушном превосходстве являются лишь примером более общей надежды западных политикоформирующих и планирующих структур на то, что, невзирая на уроки истории, передовые технологии могут преодолеть непредсказуемость и неопределенность природы войны. Однако подобные надежды, связанные с модными и популярными не так давно теориями сетецентрической войны, операций базовых эффектов, революции в военном деле и т.д.,

DOI: 10.7256/1812–8696.2015.3.14566

не выдержали испытания в реальных условиях конфликтов, протекавших после 2001 г. [22]. Можно постулировать, что технология не может компенсировать все недостатки стратегии; часто то, что она дает одной рукой, она забирает другой.

Литература, посвященная киберстратегии, далека от невосприимчивости к обоюдоострому характеру информационной технологии. Состояние методов и способов ведения войны сегодня является источником беспокойства для институтов, ведущих, планирующих и разрабатывающих политику, поскольку она является гораздо более сложной и запутанной, чем это предполагалось в первое время после окончания «холодной войны», когда многие наивно считали, что наступило постоянное торжество либеральной демократии и рыночного капитализма (на фундаменте чего западные вооруженные силы с триумфом легко разгромят менее технологически оснащенных противников) [23]. Для крупных армий мира, сформированных в соответствии с правилами индустриальной эпохи, конфликт двадцать первого столетия кажется непостижимо сложным. Использование «кибервойны», таким образом, еще более усложняет ситуацию. Возможно, наиболее стойкая обеспокоенность, выраженная теми исследователями, кто пишет о кибервойне, состоит в том, что кибервойна усиливает диспропорции между сильными и слабыми государствами и между всеми государствами и некоторыми «слишком укрепившимися» негосударственными акторами [24]. Дж. Адамс пришел к заключению в своей книге «*Следующая мировая война*»: «Давид, борясь с Голиафом, доказал, что силу можно победить. Америка сегодня выглядит неловко, как Голиаф, самонадеянная в своей власти, вооруженная до зубов, не понимающая свои слабости» [25, P. 313]. Затем Адамс переходит к сути вопроса: страх стран, играющих «Голиафа», обусловлен тем, что они уязвимы для изматывающих, изнуряющих атак слабее вооруженного противника, так как они, безусловно, не могут отвечать на эти атаки на своих собственных условиях. Подрывной потенциал киберпространства в определенной степени изменяет баланс сил между США и их ближайшими оппонентами (а также негосударственными акторами): «Одной из причин для неизбежной и широкой природы вызова, бросаемого киберпространством, является низкая стоимость входа по сравнению с намного более сложным и дорогостоящим оборудованием, необходимым для воздушного и космического оружия, а также с ростом возможностей существующих и будущих противников «лилипутских» размеров генерировать то, что названо «катастрофическими каскадными эффектами» в результате проведения асимметричных операций против Американского Голиафа» [15].

Данная идея, несомненно, является эффективным риторическим трюком, как повторяющиеся ссылки на надвигающийся «электронный Перл-Харбор». Адамс описал гипотетическую «кибервойну» между Китаем и США, которая велась с помощью инструментов, названных им «войной с помощью других средств». Сценарий основан на уже знакомых тезисах, что компьютеры, управляющие китайскими промышленными и телекоммуникационными сетями и коммунальным хозяйством («нервной системой» страны) были заражены западными производителями в ходе их установки вирусами, включая программы-трояны, которые эффективно перевели функцию дистанционного управления ими на американцев [25, P. 16].

«Война другими средствами» в этом футурологическом сценарии является почти полностью электронной, бескровной и решительной, приближаясь к «непрямому подходу» Лиддел-Гарта, или даже к знаменитому афоризму Сунь Цзы, который говорит о максимальном уровне военного искусства, когда противник сдается без боя [26]. Другой апокалиптический сценарий, сформулированный Ричардом Кларком, рисует немного иную картину гипотетической «кибервойны» между США и неизвестным противником: в течение четверти часа 157 крупных мегаполисов страны ввергнуты в хаос в результате отключения электроэнергии. Облака отравляющего газа надвигаются на Уилмингтон и Хьюстон. В нескольких городах горят запасы нефти на нефтеперерабатывающих заводах. Произошли аварии в метро в Нью-Йор-

DOI: 10.7256/1812–8696.2015.3.14566

ке, Окленде, Вашингтоне, и Лос-Анджелесе. Грузовые поезда сошли с рельсов на подходах к основным железнодорожным узлам и сортировочным станциям. По всей стране самолеты буквально падают с неба в результате воздушных столкновений. Взрываются газопроводы, в результате чего миллионы людей оказались под угрозой замерзания. Финансовая система также оказалась полностью блокированной из-за того, что терабайты информации в центрах обработки данных были стерты. Метеорологические, навигационные и телекоммуникационные спутники сошли со своих орбит. Вооруженные силы США превратились в набор изолированных частей и подразделений, стремящихся наладить связь друг с другом ... И во всех войнах, которые вела Америка, ни одна страна раньше не наносила такого рода ущерб американским городам. Современная кибератака со стороны одного из государств может нанести такой ущерб сегодня за пятнадцать минут, без появления на территории страны чужих военнослужащих или террористов [27, P. 67–68].

Западных экспертов наиболее беспокоит развитие второго из приведенных сценариев. По ряду параметров видение Кларка представляется им более достоверным. С одной стороны, оно далеко не бескровно и имеет большое значение с учетом доминирования Китая в настоящее время в производстве компьютерного оборудования; с другой стороны, западные общества, по мнению некоторых специалистов, бездумно подключили свои сетевые системы таким образом, что их трудно отключить от Интернета, повысив степень собственной уязвимости [27, P. 148]. Данный контекст, по нашему мнению, абсолютно применим и к российским реалиям, ибо наше киберпространство довольно прозрачно для проведения кибератак извне.

В обоих приведенных сценариях кибератаки являются стратегически решающими: такие атаки фактически разоружают государства, являющиеся их объектами. Тем не менее, ряд экспертов предупреждает, что возможности «враждебного завоевания» в киберпространстве «могут быть менее значимым, чем это кажется» [15]. Может ли «кибервойна» без фактического насилия или угрозы применения насилия быть войной? Клаузевиц, считавший деятелей, стремившихся найти «некий хитроумный способ разоружить противника или нанести ему поражение без кровопролития», фантазерами, опроверг бы этот тезис [28, С. 83]. По Клаузевицу, боевые действия является фундаментальным фактором войны: «Боевые действия — это единственная эффективная сила в войне; их цель заключается в уничтожении вражеских сил в качестве средства для достижения дальнейших целей. Это остается верным, даже при отсутствии фактических боевых действий, так как результаты основываются на предположении, что, если дело дойдет до боевых действий, противник будет уничтожен. Отсюда следует, что уничтожение сил противника лежит в основе всех военных действий; все планы, в конечном итоге, основаны на этом» [28, С. 111].

Тактически армии должны осуществлять некоторые базовые вещи — перемещать войска, вести огонь и обеспечивать взаимодействие, для чего связь предоставляет средства управления и координации; вероятно, что кибератаки могут привести к снижению координирующей роли телекоммуникаций до такой степени, что основные функции не могут быть исполнены адекватным образом. Стратегически, с учетом все возрастающих масштабов и последствий киберпространства для повседневной жизни, было бы разумно предположить, что атаки на цифровые системы могут быть весьма болезненными. Даже в этом случае, однако, по-прежнему остается проблема признания их независимого стратегического эффекта. Уже упоминавшийся Кларк указывает: «в кибервойне мы можем даже и не знать, кто нанес удар» [27, P. 149].

С точки зрения стратегии, проблема анонимности существует не только для объекта атаки, который должен выяснить, на кого направить оружие возмездия; в равной степени существует проблема и для атакующего, который должен задаться вопросом: «как я смогу навязывать свою волю объекту атаки, если я не раскрою ни себя, ни сообщу, какова моя воля?» Это нисколько не умаляет «проблему установления авторства», которая совершенно очевидно используется хакерами и киберпреступниками, в соответствии с доктриной

DOI: 10.7256/1812–8696.2015.3.14566

Вооруженных Сил США по операциям в киберпространстве, постоянно «поражающими специалистов глобальной системы правопорядка той скоростью, с которой они всегда идут на один шаг впереди в технологической гонке» [19, P. 10]. Можно предположить, что проблема установления авторства — это действительно то, что в основном относится к области шпионажа и преступности, когда цели могут быть достигнуты анонимно и значительно меньше относятся к области военной стратегии, которая, с тем чтобы являться рациональным инструментом политики, в конечном счете, должна быть ясной в понимании, что есть эта политика.

Ложная привлекательность концепции кибервойны заключается в том, что она обеспечивает способ для возвращения стратегам «большой войны» решимости, которой им не хватало на протяжении последних лет. Но, когда государства используют военную кибермощь против других государств в целях заставить их исполнить навязываемую волю, они по-прежнему должны декларировать свои цели и намерения (даже в том случае, если это произойдет уже после неких событий). Однако если США (или в некоторых сценариях, Китай) собираются уничтожить несколько тысяч китайцев (или наоборот) и значительно повлиять на жизни миллионов других, прибегнув к кибератаке для того, чтобы принудить правительство противника исполнить свою волю, тогда префикс «кибер» становится излишним для характеристики отношений, существующих между странами. Таким образом, «кибервойна» как вариант «чистой игры» для государств является нереалистичной моделью в силу обширности и многообразия их интересов и возможностей.

Дискуссия о противостоянии в киберпространстве началась после публикации статьи «Грядет кибервойна!», опубликованной в 1993 г. [29]. По сути, это было авторское видение передислокации подразделений и ведения огня, проводимых более изощренно, чем это делает оппонент, за счет использования более совершенных информационных систем. Она была о знании, использованном в качестве силы в буквальном и непосредственном значении. Что интересно, в качестве источника вдохновения для прогнозирования войны авторами использовалась не высокоточная технология ведения боевых действий 1991 г. в Персидском Заливе, а тактики, использованные империей монголов в XIII столетии. Снова напомним о том, что то, что здесь представляет интерес — это не технология как таковая; скорее, это тот результат, который можно достичь с помощью технологии. В этом случае киберпространство позволяет вооруженным силам перемещать информацию таким образом, что, при прочих равных условиях, может дать им значительные боевые преимущества. Военная кибермощь — это реальное и важное дополнение к другим военным возможностям. При этом кибермощь, как и военно-воздушная мощь, не устраняет эти возможности и не изменяет объективную природу войны.

ЗАКЛЮЧЕНИЕ

Можно сделать вывод, что военная кибермощь не обладает настолько стратегически мощным потенциалом, как его рисовали в последние годы. Есть все основания полагать, что, подобно военно-воздушной мощи, она будет представлять собой важный элемент в будущих совместных операциях сухопутных, воздушных и морских сил; но концепция кибервойны как стратегически решающая форма межгосударственного противостояния представляет собой вводящее в заблуждение и бессмысленное отвлечение сил и средств на негодный объект. Западные правительства, возможно, в большей степени в Великобритании, нежели в США, по-видимому, понимают это. В западном экспертном сообществе ширится подозрение, что киберугроза была переоценена (экспертами и компаниями, заинтересованными в продаже соответствующих услуг), на что следует обратить внимание, поскольку угроза должна быть тщательно скоррелирована с конкретной обстановкой. Клаузевиц выразил это следующим образом: «Первый, высший, и имеющий наиболее далеко идущие последствия акт принятия решения, который должен осуществить государственный деятель или командующий — это установить, какого рода будет война, в которую они вступают; ни принимая ошибочно ее за что-то иное, ни пытаясь превратить ее

DOI: 10.7256/1812–8696.2015.3.14566

в что-то, противное ее природе. Это — первый из всех стратегических вопросов и наиболее всеобъемлющий» [28, С. 100].

Возможно, наиболее адекватное решение в данном контексте — это понять, что оптимальной системой координат для оценки конфликта в информационно-виртуальную эпоху является не современнейшая кибервойна в «чистом виде», в которой государственные цели могут быть достигнуты с помощью собственно кибердара. Правильной системой координат будут короткие киберстычки, более или менее постоянный информационный шум с низким уровнем активности на широком «виртуальном ландшафте», часто проводимые нерегулярными акторами, возможно, с небольшим количеством столкновений, которые будут иметь стратегические последствия или вообще без них. В этом случае, действительно, ставки в их совокупности, то есть, с точки зрения бесперебойного функционирования всеобъемлющих систем национальной, региональной и международной безопасности — будут значительными.

БИБЛИОГРАФИЯ

1. Cowen T. The Age of the Infovore. London: Penguin,— 2011.— 315 p.
2. Poe M. A History of Communications. Cambridge: Cambridge University Press,— 2010.— 273 p.
3. Liang Qiao, Xiangsui Wang. Unresticted Warfare. Beijing: PLA Literature and Arts Publishing House,— February 1999.— 285 p.
4. Halliday F. The World at 2000: Perils and Promises. London: Palgrave,— 2000.— 139 p.
5. Strachan H. On War, A Biography. London,— 2007.— 263 p.
6. Lebow R. N. A Cultural Theory of International Relations. Cambridge: Cambridge University Press,— 2008.— 317 p.
7. Smith R. The Utility of Force. London,— 2005.— 267 p.
8. Angell N. The Great Illusion. London,— 1910.— 437 p.
9. Holsti K. The State, War and the State of War. Cambridge: Cambridge University Press,— 1996.— 237 p.
10. Strachan H. One War, Joint Warfare // RUSI Journal.— 2009.— vol. 154.— № . 4.— P. 22–35.
11. Kaldor M. New and Old Wars. Cambridge: Polity,— 2006.— 316 p.
12. Nagl J. Let's Win the Wars We're In // Joint Force Quarterly. 1st quarter 2009.— no. 52.— P. 20–26.
13. Hoffman Frank G. Conflict in the 21st Century: The Rise of Hybrid Wars. Washington DC: Potomac Institute,— 2007.— 341 p.
14. General Sir David Richards. Future Conflict and Its Prevention: People and the Information Age», International Institute for Strategic Studies, 18 January 2010. URL: http://www.iiss.org/recent-key-addresses/general-sir-david-richards-address/. (дата обращения 12.11.2014).
15. Betz D. J., Stevens T. Cyberspace and War // Adelphi Series.— 2011.— V. 51:424.— P. 75–98.
16. Buzan B., Waever O., Wilde Jaap de. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner,— 1998.— 267 p.
17. BBC, The Virtual Revolution, Episode 2 «The Enemy of the State?», aired on BBC2, 6 February 2010. URL: http://www.bbc.co.uk/programmes/b00n4j0r (дата обращения 12.11.2014).
18. Fuller J. F.C. The Reformation of War. London: Hutchinson,— 1923. URL: http://www.archive.org/stream/reformationofwar00fulluoft /reformationofwar00fulluoft_djvu.txt (дата обращения 12.11.2014).
19. Cyberspace Operations. United States Air Force Doctrine Document 3–12.— 15 July 2010.— P. 10. URL: http://www.e-publishing.af.mil/shared/media/epubs/afdd3–12.pdf (дата обращения 12.11.2014).
20. Byman D., Waxman M. Kosovo and the Great Air Power Debate // International Security.— Spring 2000.— vol. 24.— no. 4.— P. 5–38.
21. Information Systems Security / Joint Security Commission, Redefining Security. Washington DC, 28 February 1994. URL: http://www.fas.org/sgp/library/jsc/chap8.html (дата обращения 12.11.2014).

DOI: 10.7256/1812–8696.2015.3.14566

22. McMaster H. R. Learning from Contemporary Conflicts to Prepare for Future War // Orbis.— 2008.— vol. 52.— no. 4.— P. 564–584.
23. Фукуяма Ф. Конец истории. М.,— 2005.— 316 с. Fukuyama F. Konets istorii. M.,— 2005.— 316 c.
24. Robb J. Brave New War. Hoboken, NJ: John Wiley and Sons,— 2007.— 146 p.
25. Adams J. The Next World War. New York,— 1998.— 317 p.
26. Лиддел Гарт Б. Стратегия непрямых действий. М.,— 2014.— 265 с. Liddel Gart B. Strategiya nepryamykh deystviy. M.,— 2014.— 265 c.
27. Clarke R. Cyber War. New York, HarperCollins,— 2010.— 253 p.
28. Клаузевиц К. О войне. В 3-х т. М.,— 2009.— Т. 1.— 295 с. Klauzevits K. O voyne. V 3-kh t. M.,— 2009.— T.1.— 295 s.
29. Arquila J., Ronfeldt D. Cyberwar is Coming / in Arquila and Ronfeldt (eds), In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA: RAND,— 1997.
30. В. Н. Конышев, А. А. Сергунин Ремилитаризация Арктики и безопасность России // Национальная безопасность / nota bene.— 2011.— 3.— С. 55–67.
31. Сергунин А. А. КОНЦЕПТ «ВОЕННАЯ БЕЗОПАСНОСТЬ» И ЭВОЛЮЦИЯ ВОЕННО-ПОЛИТИЧЕСКОГО МЫШЛЕНИЯ ПОСТСОВЕТСКОЙ РОССИИ // Вопросы безопасности.— 2012.— 2.— С. 119–140. URL: http://www.e-notabene.ru/nb/article_183.html
32. Щупленков О. В. Методологические аспекты национальной безопасности России // Вопросы безопасности.— 2014.— 2.— С. 60–110. DOI: 10.7256/2409–7543.2014.2.11662. URL: http://www.e-notabene.ru/nb/article_11662.html

REFERENCES (TRANSLITERATED)

1. Cowen T. The Age of the Infovore. London: Penguin,— 2011.— 315 p.
2. Poe M. A History of Communications. Cambridge: Cambridge University Press,— 2010.— 273 p.
3. Liang Qiao, Xiangsui Wang. Unresticted Warfare. Beijing: PLA Literature and Arts Publishing House,— February 1999.— 285 p.
4. Halliday F. The World at 2000: Perils and Promises. London: Palgrave,— 2000.— 139 p.
5. Strachan H. On War, A Biography. London,— 2007.— 263 p.
6. Lebow R. N. A Cultural Theory of International Relations. Cambridge: Cambridge University Press,— 2008.— 317 p.
7. Smith R. The Utility of Force. London,— 2005.— 267 p.
8. Angell N. The Great Illusion. London,— 1910.— 437 p.
9. Holsti K. The State, War and the State of War. Cambridge: Cambridge University Press,— 1996.— 237 p.
10. Strachan H. One War, Joint Warfare // RUSI Journal.— 2009.— vol. 154.— № . 4.— R. 22–35.
11. Kaldor M. New and Old Wars. Cambridge: Polity,— 2006.— 316 p.
12. Nagl J. Let's Win the Wars We're In // Joint Force Quarterly. 1st quarter 2009.— no. 52.— R. 20–26.
13. Hoffman Frank G. Conflict in the 21st Century: The Rise of Hybrid Wars. Washington DC: Potomac Institute,— 2007.— 341 p.
14. General Sir David Richards. Future Conflict and Its Prevention: People and the Information Age', International Institute for Strategic Studies, 18 January 2010. URL: http://www.iiss.org/recent-key-addresses/general-sir-david-richards-address/. (data obrashcheniya 12.11.2014).
15. Betz D. J., Stevens T. Cyberspace and War // Adelphi Series.— 2011.— V. 51:424.— R. 75–98.
16. Buzan B., Waever O., Wilde Jaap de. Security: A New Framework for Analysis. Boulder, CO: Lynne Rienner,— 1998.— 267 p.
17. BBC, The Virtual Revolution, Episode 2 'The Enemy of the State?', aired on BBC2, 6 February 2010. URL: http://www.bbc.co.uk/programmes/b00n4j0r (data obrashcheniya 12.11.2014).
18. Fuller J. F.C. The Reformation of War. London: Hutchinson,— 1923. URL: http://www.archive.org/stream/reformationofwar00fulluoft /reformationofwar00fulluoft_djvu.txt (data obrashcheniya 12.11.2014).

DOI: 10.7256/1812–8696.2015.3.14566

19. Cyberspace Operations. United States Air Force Doctrine Document 3–12.— 15 July 2010.— R. 10. URL: http://www.e-publishing.af.mil/shared/media/epubs/afdd3–12.pdf (data obrashcheniya 12.11.2014).
20. Byman D., Waxman M. Kosovo and the Great Air Power Debate // International Security.— Spring 2000.— vol. 24.— no. 4.— R. 5–38.
21. Information Systems Security / Joint Security Commission, Redefining Security. Washington DC, 28 February 1994. URL: http://www.fas.org/sgp/library/jsc/chap8.html (data obrashcheniya 12.11.2014).
22. McMaster H. R. Learning from Contemporary Conflicts to Prepare for Future War // Orbis.— 2008.— vol. 52.— no. 4.— R. 564–584.
23. Fukuyama F. Konets istorii. M.,— 2005.— 316 c. Fukuyama F. Konets istorii. M.,— 2005.— 316 c.
24. Robb J. Brave New War. Hoboken, NJ: John Wiley and Sons,— 2007.— 146 p.
25. Adams J. The Next World War. New York,— 1998.— 317 p.
26. Liddel Gart B. Strategiya nepryamykh deistvii. M.,— 2014.— 265 c. Liddel Gart B. Strategiya nepryamykh deystviy. M.,— 2014.— 265 c.
27. Clarke R. Cyber War. New York, HarperCollins,— 2010.— 253 p.
28. Klauzevits K. O voine. V 3-kh t. M.,— 2009.— T.1.— 295 s. Klauzevits K. O voyne. V 3-kh t. M.,— 2009.— T.1.— 295 s.
29. Arquila J., Ronfeldt D. Cyberwar is Coming / in Arquila and Ronfeldt (eds), In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica, CA: RAND,— 1997.
30. V. N. Konyshev, A. A. Sergunin Remilitarizatsiya Arktiki i bezopasnost' Rossii // Natsional'naya bezopasnost' / nota bene.— 2011.— 3.— C. 55–67.
31. Sergunin A. A. KONTsEPT 'VOENNAYa BEZOPASNOST>>' I EVOLYuTsIYa VOENNO-POLITIChESKOGO MYShLENIYa POSTSOVETSKOI ROSSII // Voprosy bezopasnosti.— 2012.— 2.— C. 119–140. URL: http://www.e-notabene.ru/nb/article_183.html
32. Shchuplenkov O. V. Metodologicheskie aspekty natsional'noi bezopasnosti Rossii // Voprosy bezopasnosti.— 2014.— 2.— C. 60–110. DOI: 10.7256/2409–7543.2014.2.11662. URL: http://www.e-notabene.ru/nb/article_11662.html

DOI: 10.7256/1812–8696.2015.3.14566