УДК 004.056.5
ББК 32.973.202

Себекин Сергей Александрович*, аспирант кафедры мировой истории и международных отношений исторического факультета Иркутского государственного университета.

Необходимость совершенствования доктрины сдерживания в условиях роста киберугроз (экспертные подходы)

Формализация проблемы

Доктрина сдерживания всегда была неотъемлемой составляющей обеспечения национальной безопасности сначала в СССР, а затем и в современной России[1]. До сегодняшнего дня важнейшим гарантом безопасности служило ядерное сдерживание. Однако опыт показывает, что этих сил уже недостаточно. Как говорит академик РАН Андрей Афанасьевич Кокошин: "Ядерное сдерживание при всей его значимости – это не панацея в обеспечении национальной безопасности России. За счёт него невозможно (и даже опасно) пытаться парировать, нейтрализовать весь спектр политико-военных угроз безопасности нашей страны… Так что в числе прочих мер ядерное сдерживание должно быть дополнено эффективным неядерным („предъядерным“) сдерживанием"[2]. А генерал-майор В. М. Буренок и полковник О. Б. Ачасов утверждают: "…в последние годы стала очевидной неэффективность подобного вида сдерживания при предотвращении военных конфликтов… Это говорит о целесообразности его сочетания со сдерживанием потенциального агрессора неядерными средствами в соотношении, адекватном характеру и масштабам угроз безопасности страны"[3].

Действительно, ещё в 1990-х гг. стали вестись активные обсуждения относительно неядерного, или конвенционального, сдерживания, одним из инициаторов которых был А. А. Кокошин[4]. С этого момента и по сегодняшний день в отечественном военном мышлении ядерное и неядерное сдерживания сосуществуют бок о бок, дополняя и балансируя относительно друг друга. В зависимости от развития неядерного сдерживания ядерное играло бóльшую или меньшую роль.

* sebserg37@gmail.com

[1] *Костров А.В.* Геополитика. Иркутск: Изд-во ИГУ, 2015. С. 60.

[2] *Кокошин А.А.* Политико-военные и военно-стратегические проблемы национальной и международной безопасности. М.: Высш. шк. экономики, 2013. С. 223.

[3] *Буренок В.М., Ачасов О.Б.* Неядерное сдерживание // Военная мысль. 2007. № 12. С. 12–15. URL: http://militaryarticle.ru/voennaya-mysl/2007-vm/10005-nejadernoe-sderzhivanie (дата обращения: 14.01.2018).

[4] *Кокошин А.А.* Указ. соч. С. 208.

Следствием развития неядерного сдерживания, в котором доминируют традиционные высокоточные вооружения, и увеличение его эффективности является повышение порога применения ядерного оружия[5]. Однако мир уже относительно давно вступил в цифровую эпоху, которая не только продуцирует новые возможности, но и порождает новые угрозы – кибератаки.

Интересно, что кибероружие по возможным масштабам и последствиям уже приравнивается к оружию массового поражения, причём как зарубежными, так и отечественными экспертами в области безопасности. Например, в докладе, разработанном комиссией по кибербезопасности Центра стратегических и международных исследований (Center for Strategic and International Stadies, CSIS) в декабре 2008 г. для 44-й администрации нового тогда президента США Барака Обамы под названием "Защита киберпространства для 44-го президента", делалось следующее революционное заявление: "Соединённые Штаты должны рассматривать кибербезопасность в качестве одного из наиболее важных вызовов, с которыми они сталкиваются… Это стратегический вопрос, приравниваемый к применению оружия массового поражения…"[6]

Джон Келли и Лаури Альманн вообще утверждают, что кибероружие необходимо классифицировать как электронное оружие массового поражения вследствие того, что оно может наносить "неописуемый ущерб"[7]. Аналогичного мнения придерживаются и российские эксперты[8]. Так, директор Института проблем информационной безопасности МГУ им. М. В. Ломоносова генерал-полковник В. П. Шерстюк говорит, что война в киберпространстве приближается по своим разрушительным последствиям к оружию массового поражения[9].

Если это так, тогда кибероружие уже сегодня является феноменом, который (*а*) нужно сдерживать и (*б*) может одновременно оказывать сдерживающий эффект. Таким образом, под киберсдерживанием логично понимать следующее: 1) использование кибервозможностей для сдерживания традиционных угроз в реальном мире; 2) использование кибервозможностей для сдерживания угроз в киберпространстве.

---

[5] *Хряпин А.Л., Афанасьев В.А.* Концептуальные основы стратегического сдерживания // Военная мысль. 2005. № 1. URL: http://militaryarticle.ru/voennaya-mysl/2005-vm/9554-konceptualnye-osnovy-strategicheskogo (дата обращения: 15.01.2018).

[6] Securing Cyberspace for the 44th Presidency [A Report of the CSIS Commission on Cybersecurity for the 44th Presidency] // Center for Strategic and International Studies. 2008. December. P. 15. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf (дата обращения: 15.01.2018).

[7] *Kelly J.J., Almann L.* eWMDs // Hoover Institution. 2008. 3 December. URL: https://www.hoover.org/research/ewmds (дата обращения: 15.01.2018).

[8] См. подробнее: *Стрельцов А.А.* Основные направления развития международного права вооружённых конфликтов применительно к киберпространству // Digital Report. 2015. 2 сентября. URL: https://digital.report/pravo-cyber-konfliktov/ (дата обращения: 15.01.2018); *Он же.* Применение международного гуманитарного права к вооружённым конфликтам в киберпространстве // Digital Report. 2016. 25 апреля. URL: https://digital.report/konflikt-v-kiberprostranstve/ (дата обращения: 15.01.2018).

[9] *Тюрин Д.* Кибероружие становится опаснее ядерного: Россия и Запад расширяют диалог о безопасности в киберпространстве // Известия. 2016. 29 апреля. URL: https://iz.ru/news/611996 (дата обращения: 15.01.2018).

Действительно, что касается пункта (*a*), в статье "Сдерживание в эпоху ядерного распространения" коллективом авторов, среди которых 56-й и 60-й госсекретари США Г. Киссинджер и Дж. Шульц соответственно, отмечается, что "необходимо признать существование нового сложного спектра угроз глобальной безопасности", которые включают в себя и кибервойну[10].

В отношении потенциальной сдерживающей способности кибероружия президент Академии военных наук М. А. Гареев справедливо отмечает: "В наше время… с целью достижения большей рациональности действий мы должны отвечать на возникающие угрозы более гибко и по возможности не прямыми, а асимметричными мерами… С этой целью предлагается ввести понятие „стратегическое сдерживание“. Практически оно уже употребляется, но не всегда одинаково понимается или сводится лишь к стратегическому ядерному сдерживанию", что в условиях современного мира неверно[11]. И хотя М. А. Гареев в данном тексте не делает прямой отсылки к кибероружию, становится понятно: в цифровую эпоху необходимо сделать вывод, что кибервозможности превосходно соответствуют понятию асимметричных мер, так как позволяют компенсировать дисбаланс традиционных средств противостояния из-за своей дешевизны и растущей мощности.

Исходя из сказанного, как мы полагаем, назрела необходимость рассмотреть, что же в России делается для того, чтобы актуализировать подходы к доктрине сдерживания в условиях киберпространства, и в каком направлении развивается отечественная доктрина киберсдерживания. Однако нужно учитывать один момент – российская понятийно-терминологическая база в области кибербезопасности очень несовершенна. Например, в России существует серьёзнейшая путаница между терминами "кибер-" и "информационный". Дело в том, что "кибер-" подразумевает под собой технологические аспекты, а именно связанные с ИКТ, сетями, компьютерами и т.д. А термин "информационный" обозначает прежде всего всё то, что связано с информацией – её хранением, передачей, использованием, манипулированием, воздействием, искажением, воспроизведением, независимо от того, на каком носителе она находится.

Как можно видеть, в термине "информационный" ключевым является психологический компонент. Например, термин "информационная война" подразумевает в первую очередь психологическое воздействие посредством манипуляции информацией, а вот уже какими средствами – с использованием ИКТ-технологий и сетей или же методом сбрасывания пропагандистских листовок с самолёта над нужной территорией – это уже второй вопрос. Не всегда информационная безопасность или война осуществляются с помощью ИКТ-технологий, но всегда связаны с манипулированием / защитой информации, психологическим воздействием или просто кражей данных. Кибербезопасность и кибервойны, напротив,

---

[10] Deterrence in the Age of Nuclear Proliferation / G.P. Shultz, W.J. Perry, H.A. Kissinger, S. Nunn // Hoover Institution. 2011. 7 March. URL: https://www.hoover.org/research/deterrence-age-nuclear-proliferation (дата обращения: 15.01.2018).

[11] *Гареев М.А.* Стратегическое сдерживание: проблемы и решения // Красная звезда. 2008. 8 октября. URL: http://old.redstar.ru/2008/10/08_10/2_04.html (дата обращения: 16.01.2018).

не всегда направлены на защиту или манипулирование информацией, но предполагают обязательное использование исключительно ИКТ-технологий.

Это именно те значения, которые следует вкладывать в эти понятия. Отметим также, что информационные войны успешно ведутся уже несколько веков, даже когда о существовании киберпространства не могло быть и речи, вследствие чего уравнивание терминов "информационный" и "кибер-" не совсем уместно.

Однако в России термин "кибер-" встречает сильное сопротивление, а в официальных документах он вообще отсутствует, даже когда фактически речь идёт о кибербезопасности, кибервойне или киберсдерживании. Вместо них употребляется термин "информационный", в значение которого в России вкладываются как технологические, так и информационно-психологические аспекты. Очень часто в значение этого понятия включают чисто технологические аспекты, и тогда путаницы становится ещё больше.

Чтобы избежать наложения понятий, нужно учитывать различия между ними, однако будем иметь в виду, что даже если в изучаемой работе употребляется термин "информационный", но в нужном нам контексте – контексте технологических аспектов, то мы говорим о киберсдерживании, а не информационном сдерживании.

Киберсдерживание в отечественной военно-теоретической мысли

Надо подчеркнуть, что в отечественной военно-теоретической мысли потенциалу киберсдерживания уделяется очень мало внимания, несмотря на его исключительную важность. В 2007 г. в журнале "Военная мысль" была опубликована статья В. М. Буренка и О. Б. Ачасова под названием "Неядерное сдерживание". В ней авторы утверждают, что к нелетальному оружию, обладающему высоким потенциалом сдерживания, среди прочего относятся компьютерные вирусы, т.е. кибероружие[12]. Однако о данном факте упоминается вскользь и пристального внимания кибероружию не уделяется.

Первым важнейшим документом, составляющим ядро доктрины отечественного киберсдерживания и определяющим её принципы для вооружённых сил, являются "Концептуальные взгляды на деятельность Вооружённых Сил Российской Федерации в информационном пространстве", выпущенные Министерством обороны РФ в 2011 г. Более того, это первый документ, в котором отражён *официальный взгляд правительства и Министерства обороны РФ* на сдерживание в киберпространстве.

Помимо того что в документе киберпространство отчасти признаётся пятым театром военных действий, в нём целый раздел посвящён тому, как к нему может быть адаптировано сдерживание. В "Концептуальных взглядах" сформулированы следующие принципы доктрины сдерживания ВС РФ в киберпространстве: 1) развитие системы обеспечения кибербезопасности; 2) развитие международного сотрудничества; 3) стремление

[12] *Буренок В.М., Ачасов О.Б.* Указ соч.

к заключению под эгидой ООН договора об обеспечении международной кибербезопасности; 4) принятие мер по выявлению потенциальных военных конфликтов в киберпространстве и установлению организатора киберконфликта; 5) определение факторов возникновения и эскалации конфликта и установление контроля над ними; 6) принятие мер по противодействию развитию конфликта и его переходу в такое состояние, которое значительно увеличивает цену урегулирования; 7) принятие мер по недопущению распространения конфликта на смежные сферы межгосударственных отношений, на нейтрализацию последствий которого потребуются дополнительные усилия и затраты; 8) принятие мер по нейтрализации причин конфликта; 9) разъяснение мировой общественности причин и истоков конфликта и формирование необходимого общественного мнения, что позволит создать в глобальном информационном пространстве атмосферу, способствующую ограничению возможности совершения организаторами конфликта его дальнейшей эскалации[13].

В завершение же говорится, что обороноспособность России существенно зависит от эффективности деятельности ВС в киберпространстве и во многом определяется их возможностями по сдерживанию, предотвращению и разрешению киберконфликтов[14].

В 2012 г. была опубликована статья "Сменщики „Сатаны“ и „Минитмена“ заступают на боевой пост" Евгения Мясникова. В ней он также включает кибероружие в список типов вооружений, которые можно рассматривать в качестве стратегических неядерных[15].

В апреле 2015 г. на 11-й научной конференции Международного исследовательского консорциума информационной безопасности в рамках международного форума "Партнёрство государства, бизнеса и гражданского общества при обеспечении международной информационной безопасности" в г. Гармиш-Партенкирхен (Германия) генерал-майор Игорь Николаевич Дылевский и полковник Сергей Анатольевич Комов представили интереснейший с точки зрения взгляда официальных представителей Министерства обороны РФ доклад "Правила поведения в информационном пространстве – альтернатива гонке информационных вооружений".

Самое любопытное в докладе то, что авторы фактически отказываются от стратегии киберсдерживания в традиционном её понимании как стратегии устрашения, утверждая, что такой подход к сдерживанию дестабилизирует военно-политическую обстановку в мире, ведёт к милитаризации киберпространства и провоцирует гонку кибервооружений, так как "основывается на создании и демонстрации мощного военного информационного потенциала"[16]. На фоне этого авторы видят решение проблемы

---

[13] Концептуальные взгляды на деятельность Вооружённых Сил Российской Федерации в информационном пространстве // Министерство обороны РФ. Офиц. сайт. 2011. URL: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (дата обращения: 20.01.2018).

[14] Там же.

[15] *Мясников Е.В.* "Сменщики "Сатаны" и "Минитмена" заступают на боевой пост" // Независимое военное обозрение. 2012. 28 сентября. URL: http://nvo.ng.ru/armament/2012-09-28/11_satan.html (дата обращения: 20.01.2018).

[16] О предотвращении военных конфликтов в информационную эру / И.Н. Дылевский, О.В. Запивахин, С.А. Комов, А.А. Кривченко // Digital Report. 2017. 4 марта. URL: https://digital.report/o-predotvrashhenii-voennyih-konfliktov-v-informatsionnuyu-eru/ (дата обращения: 21.01.2018).

киберсдерживания в принятии Правил поведения в области обеспечения международной информационной безопасности, последний проект которых был представлен Шанхайской организацией сотрудничества на 69-й сессии Генеральной ассамблеи ООН в 2015 г.

Как считают авторы, для предотвращения киберконфликтов необходимо принятие правил поведения в киберпространстве всеми государствами – членами ООН, а также развитие широкого международного сотрудничества. Они утверждают, что, в отличие от стратегии устрашения, такой подход основывается не на страхе возмездия, а на добровольном принятии универсальных правил поведения государств в информационном киберпространстве[17].

В 2016 г. вышел второй документ, отражающий официальный взгляд правительства и Министерства обороны РФ на киберсдерживание, – Доктрина информационной безопасности Российской Федерации. Одним из основных направлений обеспечения информационной безопасности в области обороны государства является "стратегическое сдерживание… военных конфликтов, которые могут возникнуть в результате применения информационных технологий"[18]. Однако не уточняется, о каких именно военных конфликтах идёт речь – традиционных или в киберпространстве. Кроме того, остаётся не до конца ясным, какими методами сама Россия будет осуществлять сдерживание – традиционными, информационными или киберметодами. Как говорит руководитель Центра прикладных исследований Института США и Канады РАН П. А. Шариков: "С одной стороны, это может означать использование информации в качестве сдерживающего фактора для предотвращения конфликтов в киберпространстве. С другой стороны, это может означать сдерживание обычных стратегических угроз с использованием военных кибервозможностей"[19].

В 2017 г. вышли сразу несколько статей отечественных авторов, которые так или иначе были посвящены сдерживанию в киберпространстве. 25 февраля 2017 г. в своём блоге на сайте Совета при Президенте РФ по развитию гражданского общества и правам человека Сергей Александрович Караганов отметил: "Следует начать… важный трёхсторонний диалог (между Россией, Китаем и США. – *Прим. авт.*) о том, как можно повысить международную стратегическую стабильность. Все элементы безопасности, начиная с ядерного оружия и заканчивая вопросами кибербезопасности и политики, следует рассматривать с точки зрения конечной цели – укрепление взаимного, многостороннего сдерживания"[20].

---

[17] О предотвращении военных конфликтов в информационную эру.

[18] Доктрина информационной безопасности Российской Федерации [утв. указом Президента РФ от 5 декабря 2016 г. № 646] // Совет Безопасности РФ. Офиц. сайт. 2016. 5 декабря. URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения: 20.01.2018).

[19] *Sharkiov P.* What is behind Russia's new information security doctrine? // Russia Direct. 2016. 13 December. URL: http://www.russia-direct.org/opinion/what-behind-new-russias-information-security-doctrine (дата обращения: 20.01.2018).

[20] *Караганов С.А.* Взаимное гарантированное сдерживание // Совет при Президенте РФ по развитию гражданского общества и правам человека. Офиц. сайт. 2017. 25 февраля. URL: http://president-sovet.ru/members/blogs/post/2902/ (дата обращения: 21.01.2018).

Таким образом, С. Караганов считает, что вопросы кибербезопасности также должны быть рассмотрены с точки зрения укрепления взаимного сдерживания. Такое упоминание кибербезопасности в общем контексте с ядерным оружием (ЯО) свидетельствует о том, что киберсдерживание в восприятии его государственными деятелями поднимается до уровня ядерного сдерживания.

4 марта 2017 г. был опубликован текст выступления "О предотвращении военных конфликтов в информационную эру", подготовленного коллективом авторов, среди которых вышеупомянутые И. Н. Дылевский и С. А. Комов. В нём они вновь выразили приверженность своему тезису о том, что "реагирование военной силой на какие-либо реальные или мнимые информационные угрозы может серьёзно дестабилизировать ситуацию во всём мире"[21]. И снова авторы предлагают государствам заменить стратегию сдерживания в киберпространстве международным сотрудничеством и укреплением доверия между государствами по вопросу кибербезопасности, приняв вышеупомянутые Правила поведения[22]. Возможно, по их мнению, именно строгая международная ответственность за развязывание конфликтов с использованием ИКТ должна служить сдерживающим фактором.

Итак, в последние годы киберсдерживание начинает занимать определённое место в отечественном военно-теоретическом мышлении. Хотя ядерное сдерживание и выглядит более эффективным и преобладающим, стоит учитывать, что ядерные комплексы в информационную эпоху всё больше зависят от киберуправляемых систем, а значит, с помощью кибероружия можно повлиять на процесс принятия решений о нанесении ядерного удара, нарушить командные цепочки, "обмануть" систему предупреждения о ракетном нападении и тем самым привести к некорректному восприятию намерений потенциального противника о запуске баллистических ракет (БР) с ядерным оружием[23]. Таким образом, безопасность самого ЯО и создаваемого им стратегического баланса зависит от эффективного обеспечения кибербезопасности и киберсдерживания, что, несомненно, возвышает роль последнего.

Более того, в своих статьях от 2017 г. эксперт Российского совета по международным делам Д. Стефанович и руководитель Группы проблем информационной безопасности ЦМБ ИМЭМО РАН Н. Ромашкина поднимают вопрос о том, способно ли ядерное оружие сдержать кибервойну. И хотя аналитики отмечают, что вопрос носит сугубо теоретический характер, на наш взгляд, это революционный переворот в осознании роли киберсдерживания – ядерное и киберсдерживание в цифровую эпоху неожиданно поменялись ролями[24].

---

[21] О предотвращении военных конфликтов в информационную эру.

[22] Там же.

[23] См.: *Стефанович Д.* Ядерно-кибернетические комплексы // Российский совет по международным делам. Офиц. сайт. 2017. 6 июля. URL: http://russiancouncil.ru/analytics-and-comments/analytics/yaderno-kiberneticheskie-kompleksy/ (дата обращения: 22.01.2018); *Ромашкина Н.* Стратегическая стабильность: новые вызовы инфосферы // Российский совет по международным делам. Офиц. сайт. 2017. 23 ноября. URL: http://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-stabilnost-novye-vyzovy-infosfery/ (дата обращения: 22.01.2018).

[24] Там же.

Проблемы и перспективы киберсдерживания

Несмотря на то что перспективы киберсдерживания для России всё ещё обсуждаются в отечественных академических кругах, определённые общие тенденции относительно его формирования среди российских исследователей уже наблюдаются. Так, многие из них сходятся во мнении, что кибероружие – новый мощнейший фактор стратегической стабильности. Например, директор Института ООН по исследованию проблем разоружения (ЮНИДИР) Ярмо Сарева и Павел Шариков отмечают, что кибероружие способно существенно подорвать сложившуюся стратегическую стабильность, обеспечиваемую ядерным и неядерным сдерживанием[25]. А Наталья Ромашкина вообще утверждает, что не только кибероружие, но и "все факторы, дестабилизирующие современную систему стратегической стабильности, сегодня связаны с развитием ИКТ…"[26]

При этом исследователи указывают на одни и те же причины подрыва стратегической стабильности.

1. Дестабилизация стратегического баланса может произойти в силу того, что доступ к мощнейшему кибероружию (из-за его дешевизны и доступности) могут получить и негосударственные акторы – от крупных компаний до террористов и хакеров-одиночек. Таким образом, государства могут потерять незыблемое право на применение силы и ведение войны. Например, в США частные IT-компании и компании в сфере обеспечения безопасности уже пытаются добиться права на осуществление контркибератак[27].

2. Проблема атрибуции. Чрезвычайно сложно установить реального организатора кибератаки – он может перенаправить трафик через территорию другого государства и его сети, используя его как подставное лицо.

3. Кибероружие порождает вопросы о применимости международного права к киберконфликтам. Так, если Россия настаивает на разработке новой международно-правовой базы, учитывающей специфику киберпространства, то западные страны утверждают, что существующее международное право полностью применимо к киберконфликтам, ссылаясь на ст. 51 Устава ООН и ст. 5 Вашингтонского договора (о коллективном реагировании на агрессию в отношении государства – члена НАТО). Невозможность прийти к консенсусу в отношении этих подходов подрывает стратегическую стабильность.

4. Высокая степень мировой информатизации с всеобъемлющим киберпространством, отрицающим наличие национальных границ, делает кибероружие "идеальным глобальным оружием", способным поразить

---

[25] *Сарева Я.* Вызовы технологий XXI в. для стратегической стабильности и глобальной безопасности // Индекс безопасности. 2016. № 118–199. С. 101. URL: http://pircenter.org/media/content/files/13/14875351040.pdf (дата обращения: 23.01.2018); *Шариков П.* Информационное сдерживание: трансформация парадигмы стратегической стабильности // Российский совет по международным делам. Офиц. сайт. 2013. 5 сентября. URL: http://russiancouncil.ru/analytics-and-comments/analytics/informatsionnoe-sderzhivanie-transformatsiya-paradigmy-strat/?sphrase_id=421955 (дата обращения: 23.01.2018).

[26] *Ромашкина Н.* Указ. соч.

[27] См. подробнее: *Харрис Ш.* Кибервойн@: пятый театр военных действий. М.: Альпина Нон-фикшн, 2016. С. 172–173.

абсолютно любой объект, в том числе критически важный, с мгновенной скоростью, и при этом нанести колоссальный ущерб – начиная с самих объектов и заканчивая экономикой и национальной безопасностью.

5. Развитие кибероружия провоцирует стремительную гонку кибервооружений. Как утверждает П. Шариков: "Речь идёт о постоянной инновационной деятельности для поддержания стратегического преимущества. Разработка информационного оружия может предоставить стратегическое преимущество лишь на время – до тех пор, пока противник не обнаружит уязвимость в собственных информационных системах или не создаст более изощрённую наступательную технологию"[28]. Аналогичного мнения придерживаются И. Н. Дылевский и С. А. Комов, которые говорят, что в случае с кибероружием "достичь убедительного превосходства над соперниками чрезвычайно трудно"[29].

6. Распространение технологий кибероружия практически не поддаётся контролю.

7. Проблема с получением доступа к ядерному арсеналу и манипулированием как им самим, так и информацией о его применении, мнением кадрового состава, введением в заблуждение (якобы противником запущена БР с ЯО, хотя на самом деле нападения не было) может привести к ядерной эскалации. Так, спецпредставитель Президента по вопросам международного сотрудничества в области информационной безопасности А. Крутских отмечает, что "никому не хочется погибнуть от ядерного оружия из-за киберпровокаций"[30].

8. Киберсдерживание носит двухсторонний и противоречивый характер, балансируя между необходимостью скрывать свой максимальный уровень кибервозможностей, с одной стороны, и сделать общеизвестным факт наличия мощных киберсил для сдерживания неприятеля – с другой[31]. И то и другое подрывает стратегический баланс.

В этом смысле противоречие киберсдерживания проявляется в том, что, как отмечает П. Шариков, "скрытая разработка и применение технологии военного назначения, позволяющей добиться превосходства над противником, могли стать фактором, дестабилизирующим стратегическую стабильность", а "официальная демонстрация кибероружия тождественна потере преимущества, так как противник моментально начнёт искать способы и средства противодействия данной технологии"[32]. И снова его мнение совпадает с мнением И. Н. Дылевского и А. С. Комова, которые говорят, что "с одной стороны, публикация сведений о разработке новых

---

[28] *Шариков П.* Указ. соч.

[29] *Дылевский И.Н., Комов С.А.* Правила поведения в информационном пространстве – альтернатива гонке информационных вооружений // Digital Report. 2016. 5 марта. URL: https://digital.report/pravila-povedeniya-v-informatsionnom-prostranstve/ (дата обращения: 20.01.2018).

[30] Полномочный посол РФ в сфере ИБ: "Никому не хочется погибнуть от ядерного удара из-за киберпровокаций" // Digital Report. 2017. 25 апреля. URL: https://digital.report/polnomochnyiy-posol-rf-v-sfere-ib-nikomu-ne-hochetsya-pogibnut-ot-yadernogo-udara-iz-za-kiberprovokatsiy/ (дата обращения: 25.01.2018).

[31] *Hjortdal M.* China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence // Journal of Strategic Security. 2011. No. 2. P. 4. URL: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss (дата обращения: 24.01.2018).

[32] *Шариков П.* Указ. соч.

систем вооружения немедленно приведёт к разработке средств и способов противодействия им, т.е. к нарушению баланса. С другой стороны, любая неконтролируемая скрытая разработка таких систем также будет нарушать искомый баланс и дестабилизировать военно-политическую обстановку"[33].

9. Дестабилизация стратегической стабильности может произойти также вследствие того, что некоторые страны объявили о готовности в ответ на кибератаки применять обычные вооружённые силы. Так, бывший первый заместитель министра обороны США Уильям Линн заявил, что "США оставляют за собой право по законам вооружённого конфликта отвечать на серьёзные кибератаки уместными, пропорциональными и оправданными военными средствами"[34]. Об этом говорится и в документе Объединённого центра передового опыта по кибероборонe НАТО (Cooperative Cyber Defense Center of Excellence, CCD COE) – "Таллинском руководстве", составленном под контролем профессора международного права Военно-морского колледжа ВМФ США Майкла Шмитта: "Если применение силы достигает уровня вооружённого нападения, государство имеет право отвечать, используя силы самообороны"[35]. Однако И. Н. Дылевский и С. А. Комов заявляют, что "реагирование военной силой на какие-либо реальные или мнимые информационные угрозы может серьёзно дестабилизировать ситуацию во всём мире"[36].

Так или иначе, большинство российских исследователей сходятся в том, что "информационное устрашение… приведёт лишь к новому витку гонки вооружений и милитаризации информационного пространства"[37]. Таким образом, кибероружие может подрывать саму существующую систему сдерживания, что в свою очередь делает уже киберсдерживание довольно противоречивым, в том числе в плане своего осуществления.

В этом свете развитие международного сотрудничества по вопросам кибербезопасности, предлагаемое (как мы могли видеть) в рассмотренных официальных документах и большинством отечественных исследователей в качестве основного инструмента сдерживания киберконфликтов, выглядит весьма логичным. Например, сотрудник Института проблем информационной безопасности МГУ им. М. В. Ломоносова Д. И. Григорьев делает развитие международного сотрудничества по вопросам кибербезопасности центральной темой своей статьи "Российские приоритеты и шаги к кибербезопасности", опубликованной в тематическом сборнике "Глобальное киберсдерживание" Институтом Восток – Запад. Согласно автору, перед Россией стоят следующие задачи: 1) участие в создании международной системы управления интернетом; 2) принятие универсального

---

[33] *Дылевский И.Н., Комов С.А.* Правила поведения в информационном пространстве…

[34] *Lynn W.J.* The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack // Foreign Affairs. 2011. 28 September. URL: https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later (дата обращения: 24.01.2018).

[35] Tallin Manual On The International Law Applicable To Cyber Warfare / Ed. M.N. Schmitt. N.Y.: Cambridge University Press, 2013. P. 55. URL: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (дата обращения: 24.01.2018).

[36] О предотвращении военных конфликтов в информационную эру.

[37] *Дылевский И.Н., Комов С.А.* Правила поведения в информационном пространстве…

международного политико-правового договора, в котором осуждается использование интернета в военно-политических целях; 3) создание региональных систем информационной безопасности и т.д.[38]

Международное сотрудничество как самый эффективный способ киберсдерживания рассматривают большинство отечественных исследователей. Таковой является и официальная позиция РФ. Россия делает основную ставку на сотрудничество, создание единых правил поведения и установление доверия в киберпространстве как эффективные инструменты сдерживания, а не на устрашение как сдерживание. Однако этот подход к сдерживанию киберконфликтов также испытывает некоторые трудности из-за различных подходов и понимания самого обеспечения кибербезопасности между различными договаривающимися сторонами[39]. Например, в мировом сообществе отсутствует единая понятийно-терминологическая база в области кибербезопасности и наблюдается разное понимание ключевых терминов, таких как "кибербезопасность" и "информационная безопасность", "информационные угрозы", "киберугрозы" и т.д.

Мы уже отмечали, что в России существует серьёзнейшая путаница между терминами "кибер-" и "информационный". Между тем в странах Запада данные понятия чётко разграничиваются. В этом кроется основной корень зла – западные страны используют на международном уровне термин "кибер-", имея в виду технологические аспекты (сюда же относятся и "технологические" операции с информацией). Мы же, вынося вопрос об обеспечении кибербезопасности на международную арену, используем термин "информационный", утверждая, что имеем в виду технический аспект защиты информации, а не защиту от её контентного содержания, под которым в данном случае понимается неугодная диссидентская информация, подрывающая престиж государства, дискредитирующая существующий политический строй. При этом акцент делается на том, что борьба с контентной составляющей – это внутренние дела государства, а то, о чём говорит МИД на международной арене, – это борьба с кибератаками. Таким образом, МИД утверждает, что на самом деле Россия обеспокоена именно традиционными киберугрозами, а не борьбой с инакомыслием в интернете[40].

Но другие страны, традиционно используя термин "кибербезопасность", в формулировке "международная информационная безопасность" усматривают именно борьбу с инакомыслием, упрекая в этом Россию. Из-за этого и создаются проблемы на уровне понимания, одна из которых – сопротивление со стороны доктринального противника России – США – использованию в некоторых международных документах на уровне ООН

---

[38] *Grigoriev D.I.* Russian Priorities and Steps Towards Cybersecurity // Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway. 2010. April. P. 6. URL: https://www.files.ethz.ch/isn/115239/2010-04_GlobalCyberDeterrence.pdf (дата обращения: 24.01.2018).

[39] См. подробнее: *Бедрицкий А.В.* Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. № 4. С. 136.

[40] *Лукацкий А.В.* Кибербезопасность или информационная безопасность? // Бизнес без опасности. 2013. 1 августа. URL: http://lukatsky.blogspot.ru/2013/08/blog-post.html (дата обращения: 26.01.2018).

термина "международная информационная безопасность" и противодействие всем российским инициативам в сфере обеспечения международной кибербезопасности.

Исходя из сказанного, уместен вопрос – чего мы хотим? Если мы действительно хотим защититься от кибератак, тогда необходимо не вкладывать в понятие "информационный" тот смысл, который по существу к нему не применим, и использовать более удобный термин – "кибер-". Таким образом, государствам действительно следует разработать единую понятийно-терминологическую базу, связанную с киберпространством, необходимую для достижения реальных результатов взаимодействия. Помимо этого, *у международного сотрудничества как способа сдерживания существует ещё одна серьёзнейшая проблема* – оно по-настоящему эффективно только в случае с государствами, но не в случае с другими акторами – террористами, группами хакеров, хакерами-одиночками и т.д.[41]

* *
*

Несмотря на то что пока государства не могут прийти к консенсусу, России всё же необходимо развивать доктрину киберсдерживания. "Настало время говорить о разработке теории ведения боевых действий в информационной сфере, которые становятся решающей составляющей вооружённой борьбы"[42].

Потенциалу киберсдерживания в отечественной военно-теоретической мысли несправедливо уделяется ничтожно мало внимания – оно видится в качестве одного из незначительных компонентов системы неядерного сдерживания. В свою очередь рассмотрение системы отечественного неядерного сдерживания фокусируется лишь на традиционном неядерном оружии, не доходя до киберсдерживания.

Таким образом, возвращаясь к разговору о влиянии неядерного сдерживания на теоретический уровень порога применения ядерного оружия, необходимо отметить, что, будучи дестабилизирующим фактором глобальной стратегической стабильности, параллельно с этим именно кибероружие способно повышать порог применения ядерного оружия на национальном уровне. При этом киберсдерживание может являться полноценным самодостаточным сдерживанием, по эффективности, масштабам и последствиям сравнимым с ядерным, пусть и не способным заменить его полностью. Чтобы сдерживать противника, не нужно непосредственно демонстрировать свой киберпотенциал, необходимо лишь разработать эффективную доктрину киберсдерживания, в которой будут прописаны пропорциональные ответные меры на кибератаки. Кроме того, такая доктрина будет призвана убедить общественность

[41] *Jasper S.* Strategic Cyber Deterrence: The Active Cyber Defense Option. N.Y.: Rowman & Littlefield, 2017. P. 10.

[42] *Киселев В.А.* К каким войнам необходимо готовить Вооружённые Силы России // Военная мысль. 2017. № 3. С. 40. URL: http://sc.mil.ru/files/morf/military/archive/v_mysl_2017_march.pdf (дата обращения: 26.01.2018).

в необходимости тех или иных мер. Возможно также создание системы кибернетического щита, или, по аналогии с ядерным зонтом, системы кибернетического зонта.

Ключевые слова: *киберсдерживание – киберпространство – кибербезопасность – стратегическая стабильность – ядерное сдерживание – кибероружие – Россия.*

Keywords: *cyber deterrence – cyber space – cyber security – strategic stability – nuclear deterrence – cyber weapons – Russia.*

СПИСОК ЛИТЕРАТУРЫ

1. *Бедрицкий А.В.* Международные договорённости по киберпространству: возможен ли консенсус? // Проблемы национальной стратегии. 2012. № 4. С. 119–136.

2. *Буренок В.М., Ачасов О.Б.* Неядерное сдерживание // Военная мысль. 2007. № 12. URL: http://militaryarticle.ru/voennaya-mysl/2007-vm/10005-nejadernoe-sderzhivanie (дата обращения: 14.01.2018).

3. *Гареев М.А.* Стратегическое сдерживание: проблемы и решения // Красная звезда. 2008. 8 октября. URL: http://old.redstar.ru/2008/10/08_10/2_04.html (дата обращения: 16.01.2018).

4. Доктрина информационной безопасности Российской Федерации [утв. указом Президента РФ от 5 декабря 2016 г. № 646] // Совет Безопасности РФ. Офиц. сайт. 2016. 5 декабря. URL: http://www.scrf.gov.ru/security/information/document5/ (дата обращения: 20.01.2018).

5. *Дылевский И.Н., Комов С.А.* Правила поведения в информационном пространстве – альтернатива гонке информационных вооружений // Digital Report. 2016. 5 марта. URL: https://digital.report/pravila-povedeniya-v-informatsionnom-prostranstve/ (дата обращения: 20.01.2018).

6. *Караганов С.А.* Взаимное гарантированное сдерживание // Совет при Президенте РФ по развитию гражданского общества и правам человека. Офиц. сайт. 2017. 25 февраля. URL: http://president-sovet.ru/members/blogs/post/2902/ (дата обращения: 21.01.2018).

7. *Киселев В.А.* К каким войнам необходимо готовить Вооружённые Силы России // Военная мысль. 2017. № 3. С. 37–46. URL: http://sc.mil.ru/files/morf/military/archive/v_mysl_2017_march.pdf (дата обращения: 26.01.2018).

8. *Кокошин А.А.* Политико-военные и военно-стратегические проблемы национальной и международной безопасности. М.: Высш. шк. экономики, 2013. 261 с.

9. Концептуальные взгляды на деятельность Вооружённых Сил Российской Федерации в информационном пространстве // Министерство обороны РФ. Офиц. сайт. 2011. URL: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (дата обращения: 20.01.2018).

10. *Костров А.В.* Геополитика. Иркутск: Изд-во ИГУ, 2015. 119 с.

11. *Лукацкий А.В.* Кибербезопасность или информационная безопасность? // Бизнес без опасности. 2013. 1 августа. URL: http://lukatsky.blogspot.ru/2013/08/blog-post.html (дата обращения: 26.01.2018).

12. *Мясников Е.В.* "Сменщики „Сатаны“ и „Минитмена“ заступают на боевой пост" // Независимое военное обозрение. 2012. 28 сентября. URL: http://nvo.ng.ru/armament/2012-09-28/11_satan.html (дата обращения: 20.01.2018).

13. О предотвращении военных конфликтов в информационную эру / И.Н. Дылевский, О.В. Запивахин, С.А. Комов, А.А. Кривченко // Digital Report. 2017. 4 марта. URL: https://digital.report/o-predotvrashhenii-voennyih-konfliktov-v-informatsionnuyu-eru/ (дата обращения: 21.01.2018).

14. Полномочный посол РФ в сфере ИБ: "Никому не хочется погибнуть от ядерного удара из-за киберпровокаций" // Digital Report. 2017. 25 апреля. URL: https://digital.report/polnomochnyiy-posol-rf-v-sfere-ib-nikomu-ne-hochetsya-pogibnut-ot-yadernogo-udara-iz-za-kiberprovokatsiy/ (дата обращения: 25.01.2018).

15. *Ромашкина Н.* Стратегическая стабильность: новые вызовы инфосферы // Российский совет по международным делам. Офиц. сайт. 2017. 23 ноября. URL: http://russiancouncil.ru/analytics-and-comments/analytics/strategicheskaya-stabilnost-novye-vyzovy-infosfery/ (дата обращения: 22.01.2018).

16. *Сарева Я.* Вызовы технологий XXI в. для стратегической стабильности и глобальной безопасности // Индекс безопасности. 2016. № 118–199. С. 97–102. URL: http://pircenter.org/media/content/files/13/14875351040.pdf (дата обращения: 23.01.2018).

17. *Стефанович Д.* Ядерно-кибернетические комплексы // Российский совет по международным делам. Офиц. сайт. 2017. 6 июля. URL: http://russiancouncil.ru/analytics-and-comments/analytics/yaderno-kiberneticheskie-kompleksy/ (дата обращения: 22.01.2018).

18. *Стрельцов А.А.* Основные направления развития международного права вооружённых конфликтов применительно к киберпространству // Digital Report. 2015. 2 сентября. URL: https://digital.report/pravo-cyber-konfliktov/ (дата обращения: 15.01.2018).

19. *Стрельцов А.А.* Применение международного гуманитарного права к вооружённым конфликтам в киберпространстве // Digital Report. 2016. 25 апреля. URL: https://digital.report/konflikt-v-kiberprostranstve/ (дата обращения: 15.01.2018).

20. *Тюрин Д.* Кибероружие становится опаснее ядерного: Россия и Запад расширяют диалог о безопасности в киберпространстве // Известия. 2016. 29 апреля. URL: https://iz.ru/news/611996 (дата обращения: 15.01.2018).

21. *Харрис Ш.* Кибервойн@: пятый театр военных действий. М.: Альпина Нонфикшн, 2016. 390 с.

22. *Хряпин А.Л., Афанасьев В.А.* Концептуальные основы стратегического сдерживания // Военная мысль. 2005. № 1. URL: http://militaryarticle.ru/voennaya-mysl/2005-vm/9554-konceptualnye-osnovy-strategicheskogo (дата обращения: 15.01.2018).

23. *Шариков П.* Информационное сдерживание: трансформация парадигмы стратегической стабильности // Российский совет по международным делам. Офиц. сайт. 2013. 5 сентября. URL: http://russiancouncil.ru/analytics-and-comments/analytics/informatsionnoe-sderzhivanie-transformatsiya-paradigmy-strat/?sphrase_id=421955 (дата обращения: 23.01.2018).

24. Deterrence in the Age of Nuclear Proliferation / G.P. Shultz, W.J. Perry, H.A. Kissinger, S. Nunn // Hoover Institution. 2011. 7 March. URL: https://www.hoover.org/research/deterrence-age-nuclear-proliferation (дата обращения: 15.01.2018).

25. *Grigoriev D.I.* Russian Priorities and Steps Towards Cybersecurity // Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway. 2010. April. URL: https://www.files.ethz.ch/isn/115239/2010-04_GlobalCyberDeterrence.pdf (дата обращения: 24.01.2018).

26. *Hjortdal M.* China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence // Journal of Strategic Security. 2011. No. 2. P. 1–24. URL: http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1101&context=jss (дата обращения: 24.01.2018).

27. *Jasper S.* Strategic Cyber Deterrence: The Active Cyber Defense Option. N.Y.: Rowman & Littlefield, 2017. 270 p.

28. *Kelly J.J., Almann L.* eWMDs // Hoover Institution. 2008. 3 December. URL: https://www.hoover.org/research/ewmds (дата обращения: 15.01.2018).

29. *Lynn W.J.* The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack // Foreign Affairs. 2011. 28 September. URL: https://www.foreignaffairs.com/articles/2011-09-28/pentagons-cyberstrategy-one-year-later (дата обращения: 24.01.2018).

30. Securing Cyberspace for the 44th Presidency [A Report of the CSIS Commission on Cybersecurity for the 44th Presidency] // Center for Strategic and International Studies. 2008. December. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/081208_securingcyberspace_44.pdf (дата обращения: 15.01.2018).

31. *Sharkiov P.* What is behind Russia's new information security doctrine? // Russia Direct. 2016. 13 December. URL: http://www.russia-direct.org/opinion/what-behind-new-russias-information-security-doctrine (дата обращения: 20.01.2018).

32. Tallin Manual On The International Law Applicable To Cyber Warfare / Ed. M.N. Schmitt. N.Y.: Cambridge University Press, 2013. 302 p. URL: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf (дата обращения: 24.01.2018).