Международные процессы, Том 17, № 3 (58), сс. 51–65
DOI 10.17994/IT.2019.17.3.58.4

АНАЛИТИЧЕСКИЕ ПРИЗМЫ
Обзоры зарубежных публикаций

КИБЕРСДЕРЖИВАНИЕ И ЦИФРОВАЯ ДИЛЕММА БЕЗОПАСНОСТИ В АМЕРИКАНСКОМ ЭКСПЕРТНОМ ДИСКУРСЕ

ЕЛЕНА ЗИНОВЬЕВА
МГИМО МИД России, Москва, Россия

Резюме

В условиях нарастания конфликтности в цифровой среде в современной научной литературе проявляется склонность анализировать данную сферу международных отношений с позиций политического реализма и с опорой на представления и концепции, сложившиеся в данной школе ещё в эпоху биполярного ядерного противостояния. Одним из наиболее проработанных и популярных теоретических направлений реализма является теория сдерживания. Авторитетные американские исследователи, такие как Дж. Най и М. Либики, а также ряд других авторов утверждают, что стратегия сдерживания по аналогии с ядерным сдерживанием, но с некоторыми модификациями, может быть использована и в отношении кибервооружений. В этой связи академическим сообществом был предложен и активно используется новый термин «киберсдерживание» (cyber-deterrence). Эти концептуальные построения находят своё отражение на уровне практической политики. В частности, согласно Стратегии национальной безопасности от 2017 года, США стремятся к сдерживанию конкурентов и противников в киберпространстве. Цель статьи заключается в научной критике американской концепции «киберсдерживания» путём рассмотрения её в контексте особенностей цифровой «дилеммы безопасности». Доказывается, что эти особенности настолько фундаментальны, что сдерживание в киберпространстве принципиально отличается от сдерживания в любой другой сфере международных отношений. При этом ни авторы концепции «киберсдерживания», ни политики, реализующие её на практике, этих особенностей не учитывают. Современные информационно-коммуникационные технологии принципиально отличаются от всех предыдущих технологий, что необходимо учитывать при их военном использовании. Аналитические категории, разработанные в период ядерного сдерживания, не могут применяться к цифровой среде без существенной модификации. В этой связи особенно востребованными становятся нормы ответственного поведения государств в глобальном информационном пространстве. Их выработка рассматривается в качестве одного из инструментов снижения конфликтности в данной области.

Ключевые слова:

информационно-коммуникационные технологии; международная информационная безопасность; цифровая дилемма безопасности; киберсдерживание; США.

Исследование выполнено при финансовой поддержке РФФИ и АНО ЭИСИ в рамках научного проекта № 19-011-31053 «Мегатренды мировой политики в XXI веке: сферы проявления и развития».

Дата поступления рукописи в редакцию: 13.05.2019
Дата принятия к публикации: 29.10.2019

Для связи с автором / Corresponding author:
Email: zinovjeva@mail.ru

В условиях нарастания конфликтности в цифровой среде усиливается тенденция анализировать протекающие в ней процессы в терминах исследований безопасности. Это неизбежно порождает соблазн заимствовать устоявшиеся подходы и категории, перенося их впрямую для описания, изучения и предписания отношений в кибернетическом пространстве. Зачастую такой импорт производится из области ядерных исследований. С одной стороны, они имеют дело, так же как и анализ взаимодействия в кибернетическом пространстве, с продуктами внедрения высоких технологий. С другой – сегодня последствия хорошо подготовленного кибердудара оцениваются как сопоставимые с использованием ядерного оружия[1]. Цель настоящей статьи – продемонстрировать принципиальные ограничения по заимствованию концепций и подходов для изучения проблем информационной и кибербезопасности из любых других областей исследования. Реализуется она на примере критического анализа современных американских концепций «киберсдерживания». В силу того что сложившиеся в академическом сообществе подходы, разделяемые значительным числом авторитетных специалистов, оказывают значительное влияние на выработку внешнеполитического курса США [Истомин 2012], данное исследование имеет не только теоретическую, но и прикладную значимость. В статье доказывается, что снизить конфликтность в киберсреде традиционными силовыми методами, основанными на взаимном страхе и балансе сил, невозможно. Решение лежит в плоскости сотрудничества, а не конфронтации и предполагает выработку норм ответственного поведения государств в глобальном информационном пространстве.

Центральное место в традиционных исследованиях безопасности занимает понятие «дилемма безопасности». В самом общем смысле она подразумевает ситуацию, в которой действия государств, направленные на повышение собственной защищённости, вызывают опасения у контрагентов, провоцируя возрастание конфликтности [Herz 1950]. Её возникновение обусловлено пребыванием международных отношений в состоянии анархии и, как следствие, взаимным недоверием государств, каждое из которых стремится обеспечить собственную национальную безопасность. Важный вклад в осмысление дилеммы безопасности внёс американский специалист Роберт Джервис. Он доказывал, что большинство способов повышения защищённости одного государства негативно влияет на других игроков [Jervis 1989: 169]. Особенно высоки потенциальные риски в ситуации балансирования на грани войны: такое положение подталкивает каждого из контрагентов к нанесению первого удара.

Дилемма безопасности не всегда воспринимается сторонами одинаково. Интенсивность опасений государств относительно угроз своего выживания варьирует. Ключевую роль приобретают характеристики военных технологий, к которым государства прибегают для обеспечения своей защиты. Некоторые из технологий делают более эффективной наступательную стратегию, а другие – оборонительную. Соответственно, больше опасений у соседей будет вызывать внедрение первых. При этом не всегда между наступательными и оборонительными вооружениями можно провести однозначное разграничение. В спорных случаях государства будут исходить из наихудшего возможного сценария. [Jervis 1978: 160, 187]. Оборонительной считается такая технология, которая способствует повышению безопасности государства без создания угроз соседям.

Это довольно оптимистический взгляд на природу конфликта в международных отношениях. Если он справедлив, тогда доминирование оборонительных вооружений над наступательными в мире будет озна-

[1] См., например: *Madrigal A.* Stuxnet Is the Hiroshima of Cyber War // The Atlantic. March, 4, 2011. URL: https://www.theatlantic.com/technology/archive/2011/03/stuxnet-is-the-hiroshima-of-cyber-war/72033/

чать конец войны. С одной стороны, ядерное оружие в некоторой степени подтверждает такие оптимистичные ожидания. По крайней мере, в период «холодной войны» оно рассматривалось государствами исключительно как оружие возмездия, а не нападения. С другой стороны, есть вполне убедительные исследования, доказывающие справедливость наступательного реализма, рассматривающего любые виды потенциалов как гипотетически способные содействовать экспансии. В частности, Кир Либер показывает на обширном историческом материале, что начало войн всё же лучше объясняется изменениями общего баланса сил между государствами, нежели изменением соотношения между наступательными и оборонительными вооружениями [Lieber 2005].

Выводы Р. Джервиса созвучны управленческой теории социальных возможностей и ограничений технологий (Technology Affordances and Constraints Theory). Согласно ей, любая технология, с одной стороны, позволяет индивиду или организации реализовывать в какой-то мере свои цели, с другой стороны, одновременно ограничивает их в этом процессе. Финальная конфигурация использования технологии – это всегда результат конкретных отношений между человеком и технологией. Такой подход позволяет объяснить два распространенных эмпирических наблюдения. *Во-первых*, люди и организации не всегда используют весь возможный потенциал технологии. *Во-вторых*, люди и организации часто используют технологии способами, не предусмотренными их разработчиками. Поэтому определение наступательной или оборонительной природы той или иной военной инновации есть всегда результат двусторонних отношений между технологией и обществом. Нельзя исключать, что оборонительная технология в итоге может быть использована как наступательная, и наоборот. Современные информационно-коммуникационные технологии также обладают набором качеств, порождающих соответствующие возможности и ограничения, в том числе и при их использовании в военных целях [Majchrzak, Markus 2012; Morozov 2012].

В рамках настоящей статьи были поставлены следующие вопросы: (1) в каких целях – наступательных или оборонительных – более эффективно военное использование информационно-коммуникационных технологий; (2) как характеристики технологий влияют на межгосударственные отношения и восприятие угроз информационной безопасности, исходящих от других государству (цифровую дилемму безопасности); (3) насколько, исходя из этих характеристик, концепция «киберсдерживания» применима к глобальному информационному пространству? Для того чтобы ответить на эти вопросы, необходимо рассмотреть основные направления использования современных информационно-коммуникационных технологий (ИКТ) в военных целях.

1

Военные теоретики рассматривают информационное пространство в качестве «пятого поля боя» наряду с наземным, морским, воздушным и космическим пространствами [Lewis, Timlin 2011; Manjikian 2010]. Схожим образом глобальное информационное пространство и киберпространство[2] концептуализируются в документах стратегического

[2] В настоящей работе оба термина «глобальное информационное пространство» и «киберпространство» используются как синонимы. Вместе с тем данная терминология является предметом политической и академической дискуссии. Так, российская точка зрения на информационную безопасность делает акцент на всеобъемлющем характере информации, где киберпространство является только одним из элементов системы. Информация рассматривается как естественная и искусственная. Киберпространство является искусственной средой и рассматривается как техническое измерение информации [Rausher, Yashenko 2011: 8]. В официальных документах США, а также в исследовательской литературе американских авторов, как правило, используется термин «киберпространство», которое понимается как электронная среда, в (посредством) которой информация создаётся, обрабатывается и уничтожается [Rausher, Yashenko 2011: 11].

планирования ведущих государств и международных организаций[3].

Несмотря на то что в ранних работах по информационной и кибербезопасности возможность существования кибероружия ставилась под вопрос [Lewis 2002], современные исследователи утверждают, что оно возможно [Reich 2010; Kugler 2009]. Между отдельными государствами сохраняются различия в определении информационного оружия и кибероружия. В силу того что в фокусе внимания настоящей работы находится политика США и теоретические построения американских авторов, мы будем исходить из узкого понимания, в соответствии с которым акцентируется воздействие на данные, информационные системы и процессы, а не политико-идеологическая сфера или принятие решений противников[4].

В большинстве стран мира наметился рост затрат на сферу информационной безопасности и противодействие связанным с ней угрозам[5]. Соответствующие стратегии принимаются в странах Северной Америки, Европы, в России, Китае и других частях мира. В вооружённых силах создаются специальные подразделения, которые декларируют своей целью не только защиту государственных и коммерческих компьютерных сетей и систем, но и возможность проведения атак на информационные объекты недружественных государств. В соответствии с Кибериндексом, подготовленным Институтом ООН по вопросам разоружения (ЮНИДИР), более 47 государств разрабатывают программы использования ИКТ в военных целях, при этом 15 из них обладают возможностью использовать ИКТ-потенциал как наступательное оружие[6]. По оценкам британского эксперта Э. Крейга, на 2017 г. в 63 странах были созданы специальные подразделения вооружённых сил, нацеленные на работу в киберпространстве[7].

Постоянно совершенствуется вредоносное программное обеспечение, появляются новые виды вирусных атак. Как отмечают эксперты, современные супервирусы настолько сложны, что их создание под силу только высококвалифицированным командам специалистов, для чего необходимы существенные временные и финансовые ресурсы [Демидов, Симоненко 2013: 229]. Поэтому наиболее влиятельными игроками в области военного использования ИКТ являются государства, однако и негосударственные субъекты обладают некоторым потенциалом (как иронично отметил Дж. Най, «в киберпространстве все собаки кусаются, но большие собаки кусают больнее» [Nye 2011: 195]).

По мнению экспертов, в мире набирает темпы гонка вооружений в сфере ИКТ

[3] См., например: Доктрина информационной безопасности Российской Федерации. Утв. Указом Президента Российской Федерации от 05.12.2016 г. № 646. URL: http://kremlin.ru/acts/bank/41460 (дата обращения: 01.10.2019); USA Department of Defense Cyber Strategy. Summary. 2018. URL: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF (дата обращения: 30.11.2019); EU Cyber Defence Policy Framework (2018 update) Brussels, 19 November 2018. URL: https://www.consilium.europa.eu/media/37024/st14413-en18.pdf; NATO Brussels Summit Declaration. Brussels, 2018. URL: https://www.nato.int/cps/en/natohq/official_texts_156624.htm#20 (дата обращения: 30.11.2019).

[4] Российские авторы используют термин «информационное оружие», что, помимо технологических аспектов, включает в себя политико-идеологическое и/или информационно-психологическое измерения [Панарин 2006]; показательно, что в последние годы подобная терминология всё чаще используется и в исследовательских трудах учёных из США, в том числе «РЭНД Корпорейшн» [The Emerging Risk of … 2019].

[5] Киберстабильность: подходы, перспективы, вызовы: Материалы международной конференции // Международная жизнь (онлайн-версия журнала), 2018. URL: https://interaffairs.ru/jauthor/material/2010

[6] The Cyber Index International Security Trends and Realities. UNIDIR, 2013. URL: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf (дата обращения: 01.10.2019).

[7] Craig A. Understanding the Proliferation of Cyber Capabilities. Council on Foreign Relations. Blog Post by Guest Blogger for Net Politics. October 18, 2018. URL: https://www.cfr.org/blog/understanding-proliferation-cyber-capabilities (дата обращения: 01.10.2019).

Таблица 1
Особенности конвенциональных и кибервооружений

Конвенциональное	Информационное
• основано на использовании энергии (электромагнитной, кинетической или ядерной), химических и биологических реакций; • цель – материальная; • инструменты специально разработаны для вооружённого конфликта; • доступ к наиболее опасным образцам ограничен; • даже базовые образцы стоят дорого. Примеры традиционного вооружения, доработанного с помощью ИКТ: GPS, сетевые подразделения и т.д.	• основано на использовании информации и логики; • цель – контроль или получение информации; • имеют преимущественно гражданское предназначение; • низкая стоимость (продолжает снижаться). Примеры: «черви», «вирусы», удалённый контроль, кража паролей и др.

Источник: [Коротков, Зиновьева 2011: 158].

[Craig, Valeriano 2017: 155], которая идёт по таким приоритетным направлениям, как кибершпионаж и разработка программного обеспечения, направленного против критических информационных инфраструктур [Deibert 2015: 532]. Как правило, гонка вооружений становится ответной реакцией на дилемму безопасности. Вместе с тем можно выделить ряд особенностей кибервооружений, которые кардинальным образом отличают их от традиционных видов оружия, а также существенно влияют на восприятие государствами дилеммы безопасности в данной области, а следовательно, и на их внешнюю политику, и на возможность реализации стратегии сдерживания в данной области (табл. 1).

В кибернетическом пространстве невозможно разграничить военное и гражданское использование технологий. Это порождает асимметричные угрозы для государств-лидеров, в наибольшей степени зависящих от гражданского использования ИКТ, и поощряет наступательное использование данных технологий как возможность снижения асимметрии в других видах потенциалов между государствами-лидерами в области развития ИКТ (прежде всего, к таковым относят страны Запада, в особенности США) и остальными субъектами.

Особенностью информационных видов оружия оказывается также отложенный характер последствий их использования, которые в большинстве случаев являются косвенными [Brantly 2018: 40]. Вредоносная манипуляция объектами киберпространства направлена на сбор информации или изменение режима функционирования критической инфраструктуры, но не на полное разрушение (как это было в случае с супервирусом Stuxnet, выведшем из строя центрифуги АЭС в Иране, Натанз, но не разрушившим их полностью, подобно кинетическому оружию) [Zetter 2014].

При этом, как отмечают Р. Мэннес и Б. Валериано, несмотря на то что количество кибератак и актов использования кибероружия возрастает, уровень насилия остаётся минимальным [Mannes, Valeriano 2016: 302]. В этой связи они попадают в «серую зону» и не могут быть расценены как акт агрессии [Libicky 2018: 49]. Более того, определение источника кибератаки в большинстве случаев оказывается достаточно сложным и требует существенных временных затрат [Glaser 2011:3]. Хотя по мере развития технологий возрастает уровень достоверности выявления источников атак, проблема атрибуции в киберпространстве не решена полностью [Rid, Buchanan 2015: 4]. Применимость традиционных теорий сдерживания к киберпространству осложняется тем фактом, что значительная часть кибератак не имеет аналогов в реальном мире и среди кинетического оружия [Cooper 2012: 105]

Авторитетный американский военный теоретик М. Либики, сотрудник «РЭНД Корпорейшн» (RAND Corporation), ставший одним из пионеров исследований в

данной области, ещё в 2009 г. утверждал, что информационное оружие может быть эффективно использовано для нападения, в то время как его оборонительное использование малоэффективно [Libicki 2009]. Таким образом, технологические особенности информационных видов оружия лишь обостряют дилемму безопасности. Особенности информационно-коммуникационных технологий способствуют гонке информационных и кибервооружений, создавая искушение использовать возможность первого удара в условиях, когда оборона представляется малоэффективной. Кроме того, многие государства и негосударственные субъекты, совершая кибератаки, используют посредников («прокси») для того, чтобы иметь возможность правдоподобно отрицать использование кибероружия в политических целях [Borghard, Lonergan 2016: 395].

Вместе с тем именно асимметричный характер использования информационных технологий порождает в США интерес к возможности применения концепции сдерживания к киберпространству с тем, чтобы, сохранив преимущества лидера, обеспечить национальную безопасность. В самом общем смысле сдерживание определяется как создание у противников чувства страха перед последствиями возможных атак [Mearsheimer 1985]. Таким образом, сдерживание предполагает как наличие материальных возможностей (в области обороны или нанесения ответного удара), так и формирование разделяемых всеми убеждений о возможных последствиях агрессивных действий. Именно такая трактовка сдерживания применяется западными авторами, когда речь идёт о киберсдерживании.

2

Информатизация формирует новые угрозы даже для государств-лидеров, что порождает «цифровой парадокс мощи» [Lindsay 2013]. ИКТ, усиливая прежде всего крупные и технологически развитые государства, делают их же более уязвимыми по отношению к угрозам информационной безопасности со стороны малых государств и негосударственных игроков [Brenner 2014]. В академических кругах асимметричный характер кибероружия признаётся уже с 1990-х годов, когда исследователи начали обсуждать риски «кибер-Перл-Харбора», однако и на современном этапе политические деятели также обращают внимание на эту проблему [Kello 2017]. Как доказывает Р.В. Болгов, военная мощь США в сфере ИКТ и развитие информационного оружия лишь провоцируют глобальную конфликтность, в том числе за счёт попыток противников США создавать собственные системы информационного оружия или давать асимметричный ответ США иным способом, в том числе путём развития ядерных программ [Болгов 2010: 12].

В последние годы Соединённые Штаты весьма озабочены последствиями кибератак для своей национальной безопасности. Полным ходом идёт формирование внешнеполитической стратегии в данной области, и, как следствие, активизировалась научная дискуссия о военном использовании информационных технологий. В частности, среди американских исследователей растёт интерес к применимости практики сдерживания в информационной сфере. Возможно, это связано с более широкой тенденцией во внешней политике США, которая проявляется в усилении политики сдерживания потенциальных конкурентов [Шаклеина 2018: 40].

Для ранних работ в области военного использования ИКТ было характерно отрицание применимости политики сдерживания к киберпространству [Lukasik 2010]. В частности, авторы отмечали следующие особенности угроз в кибернетическом пространстве, которые делают классическую теорию сдерживания неприменимой:

– сложность атрибуции кибератак и выявления их источников, инициировавших их субъектов;

– доступность кибервооружений и лёгкость в осуществлении актов киберагрессии;

– широкий спектр государственных и негосударственных субъектов, участвующих в кибератаках, мишенями которых становятся также и государства, и негосударственные участники;

– короткий жизненный цикл новых технологий, в том числе кибервооружений;

– сложность определения «пороговых уровней» эскалации и «красных линий» при киберагрессии;

– сложность выработки и имплементации международных норм, регламентирующих поведение в информационном пространстве и киберпространстве;

– сложность предотвращения эскалации конфликтов в киберпространстве.

Американские авторы Р. Кларк и Р. Кнейк утверждают, что из всех элементов стратегического планирования и соответствующих теоретических концептов теория сдерживания наименее применима к реалиям кибервойны. Они полагают, что высокая зависимость Соединённых Штатов от стабильного функционирования ИКТ-инфраструктуры делает их чрезвычайно уязвимыми для ответных асимметричных кибератак: «В реальности США следует воздерживаться от масштабного применения кибервооружений, опасаясь асимметричных последствий, которые могут повлечь за собой акты возмездия, направленные на американские ИКТ-сети» [Clarke, Knake 2014: 6].

Несмотря на эти соображения, ряд авторов все же предлагает использовать стратегию сдерживания, дополнив её по ряду характеристик, чтобы обойти описанные выше ограничения. В частности, предлагается использовать комплексную стратегию сдерживания, которая включает в себя военные и невоенные инструменты ответных мер, а также комбинирует возможности различных областей – киберпространства и реального «офлайн-мира» (так называемое широкое, или межсекторальное, сдерживание (broad deterrence, cross-domain deterrence) [Brantly 2016: 34]). Предлагается также использовать расширительную трактовку сдерживания, которая подразумевает противодействие не только актам военной агрессии в киберпространстве, но и иным злонамеренным действиям, находящимся в «серой зоне», то есть тем, которые не подпадают под определение «международной агрессии», но создают издержки для объекта атаки (например, сдерживание киберпреступлений) и зачастую выступают результатом деятельности негосударственных игроков [Tor 2017].

Авторитетный американский исследователь Дж. Най исходит из расширительной трактовки сдерживания в кибернетическом пространстве [Nye 2017: 45]. В его понимании оно включает в себя кибероборону: повышение устойчивости и безопасности информационных сетей с целью минимизации преимуществ, которые может получить инициатор атаки; возмездие, в том числе необходимость публично озвучить угрозу неизбежного ответа на успешную атаку; вовлечение – включение партнёров и потенциальных врагов в отношения взаимозависимости для повышения издержек от возможной атаки для её инициатора; международное нормотворчество и выработку нормативных «табу» – прежде всего, развитие международного сотрудничества, направленного на выработку социальных норм на международном уровне [Finnemore, Hollis 2016: 425] и анализ их применимости к киберпространству (например, вопросы применимости гуманитарного права к ограничению возможных целей наступательных кибератак [Talinn Manual 2013, Talinn Manual 2.0 2017]). По мнению Дж. Ная, развитие международных норм как инструмента сдерживания необходимо ввиду того, что в киберпространстве в условиях сложности верификации источника атаки и инспекций невозможно ограничение вооружений, но возможно ограничение вероятных целей кибератак, закреплённое в нормах международного права. Запретными целями могут быть объекты гражданской инфраструктуры и гражданские лица. Таким образом, предполагается распространить нормы международного гуманитарного права на киберпространство без их адаптации к особенностям данной сферы. Подобное табу может быть усилено за счёт выработки мер укрепления доверия в киберпространстве – таких, как международная помощь в сборе улик, необходимых для атрибуции кибератаки, а также невмешательство в работу групп реагирования на компьютерные инциденты (Computer

Emergence Response Teams, CERT). Дж. Най опирается на работы Марты Финнемор, которая полагает, что в киберпространстве уже существует определённый набор норм, причём они зачастую носят неформальный характер и не всегда закреплены в документах международного права [Finnemore, Holis 2016: 428].

Американский эксперт также настаивает, что ответ на кибератаку не должен ограничиваться кибернетическим пространством, возмездие должно включать в себя также использование обычных вооружений и несиловых мер (например, экономические санкции) [Nye 2017: 45]. С ним солидарен М. Либики, который в статье от 2018 г. показывает, что использование кибератак в качестве инструмента сдерживания – в том числе в информационном пространстве – малоэффективно, но применение иных, «кинетических» угроз может быть эффективным средством предотвращения агрессивных действий государств в цифровой сфере [Libicki 2018: 44].

Выводы Дж. Ная развивает Аарон Брентли. Он полагает, что традиционные модели сдерживания, сложившиеся в годы «холодной войны» применительно к ядерному оружию и основанные на угрозе возмездия (которая предполагает увеличение *ex-post* издержек для атакующей стороны) и обороне (которая предполагает создание *ex-ante* издержек для возможного инициатора атаки), неприменимы к киберпространству ввиду асимметрии ресурсов государств, проблемы атрибуции источника кибератаки и множественности субъектов в киберпространстве, обладающих наступательным потенциалом. В этих условиях наиболее эффективной моделью сдерживания является сдерживание путём вовлечения, что предполагает смещение фокуса от обороны и возмездия к поощрению среди потенциальных противников стратегии избегания рисков [Brantly 2018]. Последняя направлена на управление восприятием и предполагает увеличение возможной «тени будущего». Реализация сдерживания путём вовлечения предполагает создание центров обмена информацией об угрозах критической информационной инфраструктуре (например, в финансовом секторе), укрепление торговых связей в области программного и аппаратного обеспечения, формирование глобальных цепочек поставок. Таким образом, потенциальные противники оказываются вовлечёнными в союзнические отношения. По мнению Брентли, именно стратегия вовлечения со стороны США по отношению к Китаю стала причиной того, что КНР воздерживается от кибератак в отношении Соединённых Штатов или стран ЕС [Brantly 2018].

В исследованиях киберсдерживания преобладают работы американских авторов, которые находятся под влиянием теоретических представлений, сложившихся ещё в период «холодной войны» [Valeriano, Maness 2018: 270]. Согласно версии американских исследователей, сдерживание сформировалось в годы биполярного противостояния и носит «абсолютный характер», то есть ориентировано на полный отказ противников США от использования отдельных видов вооружения [Jervis 1989]. На ценностном уровне данная концепция исходит из признания великодержавности Соединённых Штатов, которые ставили задачу максимизации выгод от обладания ядерными оружием, при этом не используя его для предотвращения или снижения количества конфликтов с использованием обычных вооружений. Схожие цели ставятся в отношении ИКТ [Роговский 2014: 80]. Сторонники политики сдерживания в США концептуализировали её как использование угрозы с целью влияния на выработку курса противников. Это стратегия психологического воздействия, а не принуждения силой [Schelling 1966]. Согласно данному подходу, сдерживание предполагает психологическое влияние с тем, чтобы предотвратить нежелательные действия, опираясь исключительно на угрозу насилия.

Идея сдерживания находит отражение и в официальных документах, в том числе принятых администрацией Д. Трампа. В Стратегии национальной безопасности США от 2017 г. признаётся необходимость сдерживания в киберпространстве в целях

обеспечения национальной безопасности[8]. В Национальной киберстратегии Соединённых Штатов от 2018 г. отмечается, что сдерживание в киберпространстве является одним из основных приоритетов внешней политики страны[9]. Реализация политики сдерживания в киберпространстве порождает угрозы международной безопасности, связанные, с одной стороны, с ограничениями самой этой политики, разработанной в годы «холодной войны», а с другой – со спецификой информационной сферы, которая не полностью учитывается даже в рамках модифицированной стратегии «киберсдерживания».

Таким образом, среди американских исследователей в настоящее время преобладает расширительный подход к реализации политики сдерживания в киберпространстве. В то же время её неудачи приводят к всплескам насилия на международной арене. Последние сегодня рассматриваются как неотъемлемая часть международного взаимодействия, так как государствам требуется определить «красные линии» неприемлемого поведения по отношению друг к другу [Stevens 2012]. Более того, в отличие от ядерных вооружений, кибероружие значительно более доступно, и его использование потенциально предоставляет значительно большие политические преимущества, обостряя дилемму безопасности. Современные исследования киберсдерживания не в полной мере учитывают эти особенности. В кибернетическом пространстве исследователи исходят из возможности ограничения уровня агрессии с опорой на угрозы и, возможно, ответные меры (зачастую они могут носить асимметричный характер, чтобы подкрепить значимость угроз) [Lupovici 2011: 49].

Вместе с тем подобный подход характеризуется существенными недостатками, которые связаны с особенностями цифровой дилеммы безопасности [Buchanan 2016]. Главной опасностью выступает возможность эскалации межгосударственных конфликтов вследствие применения подобной широкой трактовки киберсдерживания. Как представляется, эта угроза – следствие неверной трактовки особенностей цифровой дилеммы безопасности американскими авторами, а также недостаточного учёта специфики информационных видов оружия, применение которых в наступательных операциях предоставляет асимметричные преимущества.

3

Исследователи признают, что дилемма безопасности в кибернетическом пространстве носит более острый характер, чем в традиционных средах межгосударственной конкуренции. Для обозначения нового качества был предложен термин «цифровая дилемма безопасности». Её острота обусловлена асимметрией оборонительного и наступательного потенциала кибер- и информационного оружия, ростом влияния невоенных аспектов, в особенности экономических интересов крупного бизнеса, а также практикой глубокого проникновения государств в информационную инфраструктуру союзников и противников посредством программных средств, как правило, осуществляемого при посредничестве бизнеса [Buchanan 2016: 6].

Асимметрия наступательного и оборонительного потенциалов кибероружия рассматривается как фактор, обостряющий дилемму безопасности. Она усиливает напряжённость, способствует гонке вооружений и создаёт искушение использовать

[8] National Security Strategy of the USA. White House, December, 2017. URL: https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf (дата обращения: 01.10.2019).

[9] US Department of Homeland Security Cybersecurity Strategy. Department of Homeland Security, May, 2018. URL: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (дата обращения: 01.10.2019); National Cyber Strategy of the USA. White House, September, 2018. URL: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (дата обращения: 01.10.2019).

ИКТ в качестве «первого удара». Низкая стоимость кибервооружений поощряет средние или развивающиеся страны приобретать их как самый дешёвый способ восполнить пробелы в области обычных вооружений.

Вместе с тем ключевая особенность цифровой дилеммы безопасности связана с высокой зависимостью развитых в сфере ИКТ стран от стабильной работы ИКТ-инфраструктуры, которая, в свою очередь, находится в собственности бизнеса (более 90% всей инфраструктуры находится в собственности бизнеса [Finnemore 2019: 8]). При этом ещё одна особенность информационной сферы заключается в том, что и для обороны, и для агрессии в кибернетическом пространстве необходимо глубокое проникновение в инфраструктуру предполагаемого противника. Обычно оно осуществляется с помощью компаний, которые предоставляют на иностранной территории услуги, связанные с её функционированием. В этой связи страны Запада стараются воспрепятствовать стремлению китайской *Huawei* поставлять на свои рынки сетевое оборудование для перехода на 5G. Оно лучше и дешевле западных аналогов, но может потенциально создавать плацдарм для кибератаки. Таким образом, дилемма безопасности в информационной сфере обостряется в связи с экономической (невоенной) активностью сторон, которая приводит к инфраструктурному проникновению этого на территорию другого государства в гражданской сфере.

В результате секьюритизация иностранных ИКТ-технологий и инфраструктуры может привести к регионализации в сфере производства и поставок сетевого оборудования и вычислительной техники, а также к экономическим потерям в целом [Buchanan 2016: 52]. По мере того как всё большее количество стран осуществляет глубокое внедрение в зарубежную информационную инфраструктуру, возрастает риск неправильной интерпретации подобных действий или же нежелательных последствий неправильного функционирования внедрённого программного обеспечения, что способно привести к эскалации конфликтов в данной области [Buchanan 2016].

Американская политика киберсдерживания ориентирована на государства и не учитывает самостоятельной роли бизнеса, рассматривая его исключительно как проводника государственной политики, что не всегда справедливо [Cavelty 2014: 701]. В то же время такой подход чреват дополнительными вызовами для международной безопасности: в результате действий компаний под угрозой могут оказаться межгосударственные отношения. Более того, с учётом возможности использования кинетического оружия как инструмента стратегии киберсдерживания, эти противоречия могут создать серьёзную угрозу миру.

Кибернетическое пространство характеризуется высокой степенью взаимозависимости между государством и бизнесом. Значительная часть критической информационной инфраструктуры находится в собственности или под управлением компаний, либо отдельные её компоненты не могут функционировать без предоставляемых частным сектором решений. Таким образом, в отличие от других критически важных сфер, национальные правительства вынуждены в большей степени полагаться на взаимодействие с негосударственными участниками.

В этих условиях выработка международных норм, регламентирующих действия государств в глобальном информационном пространстве, выступает наиболее эффективным способом предотвращения конфликтов. Реализация стратегии киберсдерживания, основанной на устрашении, – малоэффективный инструмент в силу, с одной стороны, особенностей кибервооружений, обладающих большим наступательным потенциалом, чем оборонительными возможностями, а с другой – специфики «цифровой дилеммы безопасности», в которой существенную роль играет деятельность негосударственных субъектов, в особенности бизнес-структур. В этом контексте большое значение приобретает сформированный в 2018 г. по инициативе России переговорный механизм ООН по вопросам информационной безопасности, а именно Рабочая группа

открытого состава (РГОС)[10]. Он предусматривает возможность не только участия всех государств–членов ООН, но и межсессионных консультаций с представителями бизнеса и академического сообщества. Приоритетное внимание он должен уделить дальнейшей работе над нормами, правилами и принципами ответственного поведения в информационном пространстве, вопросам применимости в нём международного права и наращиванию цифрового потенциала развивающихся стран. РГОС — это полноценный орган Генеральной Ассамблеи ООН, который может вырабатывать и рекомендовать государствам-членам любые документы вплоть до проектов международных договоров[11]. Предотвращение киберконфликтов и их эскалации возможно лишь путём международного нормотворчества, а не через политику сдерживания.

* * *

Анализ концепции «киберсдерживания», сложившейся в американском академическом дискурсе, показал, что большая часть работ, постулирующая её необходимость, лишь усугубляет цифровую дилемму безопасности и не учитывает высокую роль в кибернетическом пространстве негосударственных игроков, прежде всего бизнеса. Вместе с тем предложения о необходимости выработки международных норм как элемента сдерживания конфликтности в глобальном информационном пространстве представляются рациональными и соответствующими особенностям современного этапа развития информационно-коммуникационных технологий. Также представляется важным, чтобы такие правила вырабатывались не узким кругом государств или заинтересованных структур (как предлагают американские авторы [Finnemore, Holis 2016] и американские дипломаты[12]), а представителями всего международного сообщества при участии негосударственных субъектов, в особенности компаний, специализирующихся на инфраструктурных и программных решениях в сфере ИКТ.

Список литературы

Болгов Р.В. Информационные технологии в современных вооруженных конфликтах и военных стратегиях (политические аспекты): Автореф. дис... канд. полит. наук. СПб.: СПбГУ, 2010. 38 с.

Демидов О., Симоненко М. Пожар в киберпространстве // Индекс безопасности. 2013. № 1. С. 229–232.

Истомин И.А. Научное обеспечение внешней политики США: Автореф. дис. ... канд. полит. наук. М.: МГИМО, 2012. 27 с.

Коротков А.В., Зиновьева Е.С. Безопасность критических информационных инфраструктур в международном гуманитарном праве // Вестник МГИМО-Университета. 2011. № 4. С. 154–162.

Панарин И.Н. Информационная война и геополитика. М.: Поколение, 2006. 560 с.

Роговский Е.А. Кибер-Вашингтон: глобальные амбиции. М.: Международные отношения, 2014. 848 с.

Шаклеина Т.А. Лидерство и современный мировой порядок // Международные процессы. 2015. № 4. С. 6–19.

A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Ed. by J. Healey Cyber Conflict Studies Association, 2013. 356 p.

Borghard E.D., Lonergan S.W. Can States Calculate the Risks of Using Cyber Proxies? // Orbis. 2016. No. 3. P. 395–416.

Brenner J. America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare. NY: Penguin Press, 2014. 320 p.

Brantly A.F. The Cyber Deterrence Problem // 2018 10th International Conference on Cyber Conflict (CyCon). IEEE, 2018. P. 31–54.

[10] Резолюция ГА ООН A/RES/73/27 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 05.12.2018.

[11] *Чернухин Э.* Международная информационная безопасность: успехи России в ООН. Российский совет по международным делам. 2018. URL: https://russiancouncil.ru/analytics-and-comments/analytics/mezhdunarodnaya-informatsionnaya-bezopasnost-uspekhi-rossii-v-oon/?sphrase_id=31433326 (дата обращения: 01.10.2019).

[12] Там же.

Brantly A.F. Conceptualizing Cyber Deterrence by Entanglement (April 05, 2018). URL: http://dx.doi.org/10.2139/ssrn.2624926

Buchanan B. The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations. Oxford University Press, 2016. 304 p.

Cavelty M.D. Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities // Science and Engineering Ethics. 2014. No. 3. P. 701–715.

Clarke R.A., Knake R.K. Cyber War. Tantor Media, Incorporated, 2014. 136 p.

Cooper J.R. A New Framework for Cyber Deterrence // Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World. Ed. by D.S. Reveron. Washington: Georgetown University Press, 2012. P. 105–120.

Craig A., Valeriano B. Conceptualising Cyber Arms Races // 2016 8th International Conference on Cyber Conflict (CyCon). IEEE, 2016. P. 141–158. URL: https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

Deibert R. Trajectories for Future Cybersecurity Research. In The Oxford Handbook of International Security. Ed. by A. Gheciu and W. C. Wohlforth. Oxford: Oxford University Perss, 2015. P. 531–556.

Finnemore M. Talking Past Each Other: Government, Business and Civil Society Discussing Cyber Security // Вестник МГИМО-Университета. 2019. Т. 12. №5. С. 7–11.

Finnemore M., Hollis D.B. Constructing Norms for Global Cybersecurity // American Journal of International Law. 2016. Vol. 110. No. 3. P. 425–479.

Gaver W.W. Technology Affordances // Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM, 1991. P. 79–84.

Glaser C.L. Deterrence of Cyber Attacks and US National Security // Developing Cyber Security Synergy. 2011. Vol. 47. URL: http://www.offnews.info/downloads/2011-5CyberDeterrenceGlaser.pdf

Herz J.H. Idealist internationalism and the security dilemma // World politics. 1950. Vol. 2. No. 2. P. 157–180.

Jervis R. Cooperation under the Security Dilemma // World Politics. 1978. Vol. 30. No. 2. P. 167–214.

Jervis R. Rational Deterrence: Theory and Evidence // World Politics. 1989a. Vol. 41. No. 2. P. 183–207.

Jervis R. Some Thoughts on Deterrence in the Cyber Era // Journal of Information Warfare. 2016. Vol. 15. No. 2. P. 66–73.

Jervis R. The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon. Cornell University Press, 1989. 266 p.

Kello L. The Virtual Weapon and International Order. New Heaven and London: Yale University Press, 2017. 319 p.

Kugler R.L. Deterrence of Cyber Attacks and US National Security // Cyberpower and National Security. Ed by F. Kramer, S. Starr, L. Wentz. Washington DC: Potomac Books, 2009. P. 309–342.

Lewis J. Assessing the risks of cyber terrorism, cyber war and other cyber threats. – Washington, DC: Center for Strategic & International Studies, 2002. URL: https://www.steptoe.com/images/content/4/5/v1/4586/231a.pdf

Lewis J., Timlin K. Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR, 2011. URL: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

Libicki M. Cyberdeterrence and Cyberwar. Rand Corporation, 2009. 214 p.

Libicki M. Expectations of Cyber Deterrence // Strategic Studies Quarterly. 2018. No. 4. P.44 –57.

Libicki M. Cyberspace in Peace and War. Naval Institute Press, 2016. 478 p.

Lindsay J. Stuxnet and the Limits of Cyber Warfare // Security Studies. 2013. No. 3. P. 36–404.

Lieber K.A. War and the engineers: The primacy of politics over technology. Cornell University Press, 2005. 226 p.

Lukasik S.J. A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains // Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy. 2010. Vol. 2. P. 99–122.

Maness R., Valeriano B. The Impact of Cyber Conflict on International Interactions // Armed Forces & Society. 2016. Vol. 42. No. 2. P. 301–323.

Majchrzak A., Markus M.L. Technology Affordances and Constraints in Management Information Systems (MIS). In Encyclopedia of Management Theory. Ed. by E. Kessler. London: Sage, 2012.

Manjikian M. From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik // International Studies Quarterly. 2010. No. 2. P. 381–401.

Mearsheimer J.J. Conventional Deterrence. Ithaca: Cornell University Press, 1985. 296 p.

Morozov E. The Net Delusion: The Dark Side of Internet Freedom. Public Affairs, 2012. 429 p.

Nye J.S. Deterrence and Dissuasion in Cyberspace // International Security. 2017. Vol. 41. No. 3. P. 44–71.

Nye J.S. The Future of Power. Public Affairs, 2011. 300 p.

Rauscher K. F., Yaschenko V. Russia-US bilateral on cybersecurity: Critical terminology foundations. New York, USA: EastWest Institute, 2011. 48 p.

Reich P.C. et al. Cyber Warfare: a Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity // European Journal of Law and Technology. 2010. Vol. 1. No. 2. P. 1–58.

Rid T., Buchanan B. Attributing Cyber Attacks // Journal of Strategic Studies. 2015. Vol. 38. No. 1–2. P. 4–37.

Schelling T.C. (1966). Arms and influence. New Haven, CT: Yale University Press.

Stevens T. A Cyberwar of Ideas? Deterrence and Norms in Cyberspace // Contemporary Security Policy. 2012. Vol. 33. No. 1. P. 148–170.

Tallinn Manual on the International Law Applicable to Cyber Warfare. Ed. by M. N. Schmitt. Cambridge University Press, 2013. 281 p.

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Ed. by M. N. Schmitt. Cambridge University Press, 2017. 597 p.

The Emerging Risk of Virtual Societal Warfare / M. Mazarr, R. Bauer, A. Casey, S. Heintz, L. Matthews. Santa Monica, CA: RAND Corporation, 2019. URL: https://www.rand.org/pubs/research_reports/RR2714.html

Tor U. "Cumulative Deterrence" as a New Paradigm for Cyber Deterrence // Journal of Strategic Studies. 2017. Vol. 40. No. 1–2. P. 92–117.

Valeriano B., Maness R. International Relations Theory and Cyber Security: Threats, Conflicts and Ethics in an Emergent Domain // The Oxford Handbook of Political Theory / Ed. by C. Brown, R. Eckersley. Oxford: Oxford University Press, 2018. P. 259–275.

Wilner A. US Cyber Deterrence: Practice Guiding Theory // Journal of Strategic Studies. 2019. P. 1–36. URL: https://www.tandfonline.com/doi/full/10.1080/01402390.2018.1563779#aHR0cHM6Ly93d3cudGFuZGZvbmxpbmUuY29tL2RvaS9wZGYvMTAuMTA4MC8wMTQwMjM5MC4yMDE4LjE1NjM3NzkvbmVlZEFjY2Vzcz10cnVlQEBAMA==

Zetter K. Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. NY: Crown Publishers, 2014. 449 p.

CONCEPTS OF CYBERDETERRENCE AND DIGITAL SECURITY DILEMMA IN THE US ACADEMIC LITERATURE

ELENA ZINOVIEVA

MGIMO University, Moscow, 119454, Russian Federation

Abstract

The global information space is conceptualized as a new battlefield, both in the research literature and in the strategic planning documents of states. In such analytical environment, there is a growing tendency to analyze international processes in the global information space from the standpoint of the theory of political realism, based on the ideas emerged in the "nuclear era".

One of the most developed theoretical concepts of realism is deterrence theory, which is aimed to overcome the limitations of the security dilemma. American political scientist R. Jervis was one of the founders of the both theoretical concepts, which were later revised by contemporary authors in relation to cyberspace. Contemporary researchers, including D. Nye and M. Libicki, as well as a number of other authors, argue that the deterrence strategy, by analogy with nuclear deterrence, is applicable to cyber weapons. In particular, they propose new term "cyber deterrence" (cyber-deterrence). Such conceptual constructions influence practical politics. According to the National Security Strategy of 2017, the United States is seeking implement a deterrence in cyberspace.

The purpose of the article is to analyze the applicability of the cyber-deterrence concept to cyberspace in the US academic discourse based on the characteristics of the digital "security dilemma". The article shows that

cyber deterrence, by analogy with the nuclear one, can only exacerbate the security dilemma in digital space. Digital security dilemma is different from the security dilemma that exists in relation to other types of weapons, due to the specifics of information technologies whose offensive use is more effective rather than defensive, as well as the significant role of non-state actors, especially business. Thus, methodologically, this article proceeds from the fact that modern information and communication technologies are not inherently neutral, but have a certain set of characteristics that determine their military use and, as a result, affect modern international security. Under these conditions, the development of norms of responsible behavior of states in the global information space is considered as one of the tools to deter conflict in cyber space.

Keywords:

information and communication technologies; cyber security; digital security dilemma; cyber-deterrence.

References

Bolgov R.V. (2010). *Informatsionnye tehnologii v sovremennyh vooruzhennyh konfliktah i voennyh strategijah (politicheskie aspekty)*. [Information Technologies in the Contemporary International Armed Conflicts (Political Aspects)]. PhD Dissertation. Saint-Petersburg: Saint-Petersburg State University. 38 p.

Borghard E.D., Lonergan S.W. (2016). Can States Calculate the Risks of Using Cyber Proxies? *Orbis*. No. 3. P. 395–416.

Brantly A. (2018). *Conceptualizing Cyber Deterrence by Entanglement*. URL: http://dx.doi.org/10.2139/ssrn.2624926

Brantly A. F. (2018). *The Cyber Deterrence Problem*. 10th International Conference on Cyber Conflict (CyCon). IEEE. P. 31–54.

Brenner J. (2014). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. NY: Penguin Press. 320 p.

Buchanan B. (2016). *The Cybersecurity Dilemma: Hacking, Trust, and Fear between Nations*. Oxford University Press, 2016. 304 p.

Cavelty M.D. (2014). Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities. *Science and Engineering Ethics*. No. 3. P. 701–715.

Clarke R.A., Knake R.K. (2014). *Cyber War*. Tantor Media, Incorporated. 136 p.

Cooper J. R. (2012). A New Framework for Cyber Deterrence. In Reveron D.S. (ed.) *Cyberspace and National Security Threats, Opportunities, and Power in a Virtual World*. Washington: Georgetown University Press. P. 105–120.

Craig A., Valeriano B. (2016). *Conceptualising Cyber Arms Races*. 8th International Conference on Cyber Conflict (CyCon). IEEE. P. 141-158. URL: https://ccdcoe.org/uploads/2018/10/Art-10-Conceptualising-Cyber-Arms-Races.pdf

Deibert R. (2015). Trajectories for Future Cybersecurity Research. In Gheciu A., Wohlforth W.C. (eds) *The Oxford Handbook of International Security*. Oxford: Oxford University Perss, 2015. P. 531–556.

Demidov O., Simonenko M. (2013). Pozhar v kiberprostranstve [Cyberspace on Fire]. *Indeks bezopasnosti*. No. 1. P. 229–232.

Finnemore M. (2019). Talking Past Each Other: Government, Business and Civil Society Discussing Cyber Security. *Vestnik MGIMO-Universiteta*. Vol. 12. No. 5. P. 7–11.

Finnemore M., Hollis D.B. (2016). Constructing Norms for Global Cybersecurity. *American Journal of International Law*. Vol. 110. No. 3. P. 425–479.

Gaver W.W. (1991). *Technology Affordances*. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM. P. 79–84.

Glaser C.L. (2011). Deterrence of Cyber Attacks and US National Security. *Developing Cyber Security Synergy*. Vol. 47. URL: http://www.offnews.info/downloads/2011-5CyberDeterrenceGlaser.pdf

Healey J. (ed.) (2013). A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. Cyber Conflict Studies Association. 356 p.

Herz J. H. (1950). Idealist internationalism and the security dilemma. *World politics*. Vol. 2. No. 2. P. 157–180.

Istomin I. (2012). *Nauchnoe obespechenie vneshnej politiki SShA*. [Scientific support of the US foreign policy]. PhD Dissertation. Political Sciences.

Jervis R. (1978). Cooperation under the Security Dilemma. *World Politics*. Vol. 30. No. 2. P. 167–214.

Jervis R. (1989a). Rational Deterrence: Theory and Evidence. *World Politics*. Vol. 41. No. 2. P. 183–207.

Jervis R. (2016). Some Thoughts on Deterrence in the Cyber Era. *Journal of Information Warfare*. Vol. 15. No. 2. P. 66–73.

Jervis, R. (1989b). *The meaning of the nuclear revolution: Statecraft and the prospect of Armageddon*. Cornell University Press. 266 p.

Kello L. (2017). *The Virtual Weapon and International Order*. New Heaven and London: Yale University Press. 319 p.

Korotkov A.V., Zinovieva E.S. (2011). Bezopasnost' kriticheskih informacionnyh infrastruktur v mezhdunarodnom gumanitarnom prave [Critical Information Infrastructures Security in the International Humanitarian Law]. *Vestnik MGIMO–Universiteta*. No. 4. P. 154–162.

Kugler R.L. (2009). Deterrence of Cyber Attacks and US National Security. In Kramer F., Starr S., Wentz L. (eds) *Cyberpower and National Security*. Washington DC: Potomac Books. P. 309–342.

Lewis J., Timlin K. (2011). *Cybersecurity and Cyberwarfare: Preliminary Assessment of National Doctrine and Organization, UNIDIR*. URL: http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf

Libicki M. (2009). *Cyberdeterrence and Cyberwar*. Rand Corporation. 214 p.

Libicki M. (2016). *Cyberspace in Peace and War*. Naval Institute Press. 478 p.

Libicki M. (2018). Expectations of Cyber Deterrence. *Strategic Studies Quarterly*. No. 4. P.44–57.

Lieber K.A. (2005). *War and the engineers: The primacy of politics over technology*. Cornell University Press. 226 p.

Lindsay J. 2013. Stuxnet and the Limits of Cyber Warfare. *Security Studies*. No. 3. P. 36–404.

Lukasik S.J. (2010). *A Framework for Thinking About Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains*. Proceedings of a Workshop on Deterring Cyber Attacks: Informing Strategies and Developing Options for US Policy. Vol. 2. P. 99–122.

Majchrzak A., Markus M.L. (2012). Technology Affordances and Constraints in Management Information Systems (MIS). In Kessler E. (ed.) *Encyclopedia of Management Theory*. London: Sage. URL: https://ssrn.com/abstract=2192196

Maness R., Valeriano B. (2016). The Impact of Cyber Conflict on International Interactions. *Armed Forces & Society*. Vol. 42. No. 2. P. 301–323.

Manjikian M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly*. No. 2. P. 381–401.

Mazarr M., Bauer R., Casey A., Heintz S., Matthews L. (2019). *The Emerging Risk of Virtual Societal Warfare*. Santa Monica, CA: RAND Corporation. URL: https://www.rand.org/pubs/research_reports/RR2714.html

Mearsheimer J.J. (1985). *Conventional Deterrence*. Ithaca: Cornell University Press. 296 p.

Morozov E. (2012). *The Net Delusion: The Dark Side of Internet Freedom*. Public Affairs. 429 p.

Nye J.S. (2011). *The Future of Power*. Public Affairs. 300 p.

Nye J.S. (2017). Deterrence and Dissuasion in Cyberspace. *International Security*. Vol. 41. No. 3. P. 44–71.

Panarin I.N. (2006). *Informatsionnaya vojna i geopolitika* [Information Warfare and Geopolititcs]. Moscow: Pokolenie. 560 p.

Rauscher K. F., Yaschenko V. (2011). Russia-US bilateral on cybersecurity: Critical terminology foundations. New York, USA: EastWest Institute. 48 p.

Reich P.C. et al. (2010). Cyber Warfare: a Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity. *European Journal of Law and Technology*. Vol. 1. No. 2. P. 1–58.

Rid T., Buchanan B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*. Vol. 38. No. 1–2. P. 4–37.

Rogovskij E.A. (2014). *Kiber-Vashington: global'nye ambitsii* [Cyber–Washington: Global Ambitions]. Moscow: Mezhdunarodnye otnoshenija. 848 p.

Schelling, T. C. (1966). *Arms and influence*. New Haven, CT: Yale University Press.

Schmitt M.N. (ed.) (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. (2013). Cambridge University Press. 281 p.

Schmitt M.N. (ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. (2017). Cambridge University Press. 597 p.

Shakleina T.A. (2015). Liderstvo i sovremennyj mirovoj porjadok [Leadership in the Contemporary International Order]. *Mezhdunarodnye protsessy*. No. 4. P. 6–19.

Stevens T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*. Vol. 33. No. 1. P. 148–170.

Tor U. (2017). "Cumulative Deterrence" as a New Paradigm for Cyber Deterrence. *Journal of Strategic Studies*. Vol. 40. No. 1-2. P. 92–117.

Valeriano B., Maness R. (2018). International Relations Theory and Cyber Security: Threats, Conflicts and Ethics in an Emergent Domain. In Brown C., Eckersley R. (eds) *The Oxford Handbook of Political Theory*. Oxford: Oxford University Press. P. 259–275.

Wilner A. (2019). US Cyber Deterrence: Practice Guiding Theory. *Journal of Strategic Studies*. P. 1–36.

Zetter K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. NY: Crown Publishers. 449 p.