Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве

Олег Игоревич Шакиров

https://doi.org/10.46272/2587-8476-2020-11-4-147-170

АННОТАЦИЯ

Сложившееся в последние десятилетия понимание киберпространства как среды, в которой государство может сталкиваться с серьёзными угрозами своей безопасности, способствовало поиску путей предотвращения таких угроз в военно-политической сфере. Одним из решений этой задачи стало обращение к концепции сдерживания, которая в период холодной войны заняла центральное место в стратегии держав. Однако прямой перенос привычных подходов в цифровое пространство оказывается проблематичным. С одной стороны, это накладывает ряд концептуальных ограничений, связанных с применением этой концепции. С другой стороны, способствует дискуссии о том, каким образом можно добиться сдерживания в киберпространстве с помощью традиционных и новых механизмов. Несмотря на неопределённости, возникающие при экстраполяции, на практике ведущие государства используют концепцию сдерживания в контексте их деятельности в киберпространстве, хотя и делают это по-разному. В этой связи в статье автор рассматривает не столько проблемы применения концепции сдерживания в киберпространстве, сколько ее интерпретации государствами при формулировании и реализации политики в этой сфере. Такой конструктивистский подход позволяет выявить специфику восприятия, точки пересечения и расхождения взглядов. На примере России и Соединённых Штатов автор на основе анализа официальных документов и практических кейсов показывает, какие расхождения существуют в интерпретации концепции сдерживания в киберпространстве, как это влияет на позиции России и США по данной проблематике.

КЛЮЧЕВЫЕ СЛОВА

Россия, США, киберпространство, сдерживание, информационная безопасность, кибербезопасность

Сдерживание и киберсдерживание

В самом общем виде концепция сдерживания строится на идее о том, что с помощью угрозы одна сторона может убедить другую сторону воздержаться от определённых действий. Угроза заставляет оппонента заново оценить перспективы успеха своих планов и возможные издержки. При этом в англоязычной литературе сдерживание (*deterrence*) отличают от принуждения (*compellence*), подразумевающего использование силы, чтобы заставить другую сторону совершить или не совершить определённые действия.

Необходимо также различать два английских термина, которые часто переводятся на русский как «сдерживание»: *deterrence* и *containment*. Если под первым понимается предотвращение конфликта посредством угрозы, то второй связан с ограничением, удержанием противника в определённых рамках, прежде всего, географических. Понятие *containment* тесно ассоциируется с политикой США во время холодной войны, заключавшейся в ограничении политического влияния социалистического блока в разных регионах мира. В данной статье сдерживание будет рассматриваться в первом значении (*deterrence*).

Сдерживание может пониматься в широком смысле как концепция, применимая в любых конфликтных ситуациях. Но в контексте международной безопасности речь чаще всего идёт о сдерживании от применения военной силы и о военно-политических конфликтах. Энциклопедия РВСН РФ определяет военно-политическое сдерживание как «[систему] мер военно-политического характера, предпринимаемых государством (их коалицией) с целью предотвращения угрозы агрессии или ее эскалации, а также угрозы жизненно важным интересам на основе косвенного, опосредованного использования военной силы в качестве политического средства убеждения противника отказаться от агрессии под угрозой неприемлемых для него последствий в ответных действиях, приводящих к срыву планируемых военно-политических целей»[1].

Идея использования угрозы для предотвращения конфликта имеет долгую историю и, например, отражена в крылатом выражении *Si vis pacem*, *para bellum*. Ю.А. Печатнов выделяет три исторических этапа становления теории сдерживания и соответствующих им парадигм – общепризнанного понимания проблематики сдерживания[2]:

1. Парадигма «стратагемного» сдерживания в неядерном мире (древние времена – начало 1940-х). Сдерживание неотделимо от военного искусства, его политическое значение не рассматривается и больше связывается с приемами, используемыми древними полководцами.

2. Парадигма ядерного сдерживания (1945 г. – конец 1980-х). Основанием этой парадигмы служат концепции и доктрины использования ядерного оружия. По мнению Ю.А. Печатнова, это относится только к США, а в СССР, как он отмечает, формально понятие сдерживания отсутствовало. Однако с такой точкой зрения сложно согласиться. Очевидно, что начиная с ускоренного созда-

1 Сдерживание военно-политическое // Энциклопедия РВСН. Министерство обороны Российской Федерации. [Электронный ресурс]. URL: https://encyclopedia.mil.ru/encyclopedia/dictionary/details_rvsn.htm?id=14205@morfDictionary (дата обращения: 24.02.2021).

2 Печатнов 2016, 26–27.

ния собственной атомной бомбы, руководство СССР осознавало необходимость иметь возможность нанести ответный удар США и тем самым сдержать их от использования ядерного оружия. В дальнейшем взаимное сдерживание играло определяющую роль во взаимоотношениях между двумя великими державами, приводя как к кризисам, так и к периодам снижения напряжённости. Учитывая исключительную роль ядерного оружия, на этом этапе парадигма сдерживания становится основополагающей для формирования военного и внешнеполитического курса всех ядерных держав.

3. Парадигма стратегического сдерживания (начало 1990-х– настоящее время). Согласно Ю.А. Печатнову, после холодной войны парадигма сдерживания меняется под влиянием новых инструментов силового и несилового давления, а также в связи с геополитическими изменениями. Следуя данному подходу, в рамках такой расширенной парадигмы можно рассматривать и проблематику сдерживания в киберпространстве.

Во время холодной войны (второй этап, согласно Ю.А. Печатнову) возрастает академический интерес к проблеме сдерживания[1]. Г. Снайдер предлагает классическую типологию стратегий сдерживания: «сдерживание посредством недопущения» (*deterrence by denial*) и «сдерживание посредством наказания» (*deterrence by punishment*)[2]. Он иллюстрирует это на военных примерах: в первом случае сдерживание достигается за счёт обладания военной силой, которая может не допустить захвата территории противником; во втором – военная сила увеличивает издержки для противника при нападении настолько, что они превышают возможные выгоды. Г. Снайдер пишет, что сдерживание, как и политическая сила в целом, не должно основываться только на военных возможностях, но может обеспечиваться и невоенными средствами, такими как торговые ограничения. Т. Шеллинг рассматривал концепцию ядерного сдерживания как инструмент торга, уделяя внимание проблемам восприятия и убедительности сдерживания[3].

К основным типологиям сдерживания также относятся[4]:

– Прямое сдерживание, если оно направлено на предотвращение нападений на саму защищающуюся сторону, либо расширенное – в этом случае страна предотвращает нападения на третьи страны, прежде всего на своих союзников.

– Общее сдерживание, рассчитанное на предотвращение нежелательных действий в нормальных условиях на протяжении продолжительного времени, и непосредственное, то есть сдерживание в конкретных кризисных ситуациях.

– Сдерживание в узкой трактовке (когда речь идёт исключительно о военных инструментах) и в широком понимании (в эту концепцию могут включаться невоенные вызовы и средства реагирования на них).

Имея в виду периодизацию развития парадигм сдерживания, описанную выше, можно сказать, что на текущем этапе сдерживание чаще понимается в широком смысле. Однако в конечном счёте определение зависит от контек-

1 Huth 1999.
2 Snyder 1960, 163.
3 Schelling 2008, 23.
4 Mazarr 2018.

ста (например, в военном конфликте достаточным может быть узкая концепция сдерживания).

Распространение концепции сдерживания на киберпространство было обусловлено ее популярностью, прежде всего в ядерных странах, где она стала одной из основ стратегического мышления. Также этому способствовало расширение возможностей использования информационно-коммуникационных технологий (ИКТ) в военных целях. В США, в частности, киберпространство ещё с 1990-х гг. начало восприниматься как самостоятельный театр военных действий, которое описывалось с помощью привычных терминов. Продолжающаяся милитаризация киберпространства и всё более широкий спектр связанной с ним военно-политической деятельности государств сделал сдерживание в этой сфере востребованной задачей.

С одной стороны, перенос концепции сдерживания в киберпространство стимулировал попытки переосмыслить сдерживание применительно к новой практике. Так, исследователи выделяют не только классические, но и дополнительные стратегии сдерживания, которые могут предотвратить конфликт с учётом специфики среды. Дж. Най[1] выделяет четыре основных механизма сдерживания в киберпространстве: помимо классического сдерживания посредством наказания и посредством недопущения, было также выделено сдерживание посредством взаимозависимости (*entanglement*) и посредством формирования норм и табу.

Сдерживание посредством взаимозависимости достигается за счёт того, что ущерб в результате возможной атаки будет нанесён не только жертве, но и самому нападающему. Сдерживание посредством норм и табу должно обеспечиваться выработкой общепринятых правил того, какая деятельность считается приемлемой для государств. Так же как человечество постепенно пришло к недопустимости применения некоторых видов оружия, оно, вероятно, сможет прийти к недопустимости некоторых видов кибератак. Н. Райан добавляет к этому перечню ещё одну стратегию: сдерживание посредством ассоциации – установление виновных в кибератаках и публичная атрибуция к ним, что, как предполагается, должно в дальнейшем изменить их поведение[2].

С другой стороны, прямой перенос этой концепции на киберпространство проблематичен. М. Либики, автор одной из первых книг о киберсдерживании, в 2009 г. обозначил некоторые проблемные вопросы, отличающие сдерживание в киберпространстве от ядерного[3]:

– Можно ли знать, кто стоит за атакой (проблема атрибуции)?

– Может ли быть установлен порог для ответных действий?

– Можно ли избежать эскалации?

– Будут ли третьи стороны (в т.ч. негосударственные акторы) воздерживаться от вмешательства в межгосударственный киберконфликт?

В академической литературе был выделен ряд ограничений, возникающих при переносе концепции сдерживания в киберпространство. Так, М. Таддео рассматри-

1 Nye 2017, 54–62.
2 Ryan 2018, 35–36.
3 Libicki 2009, xvi–xvii.

вает процесс сдерживания на основе абстрактной модели из трёх ключевых элементов: атрибуция, сигнализирование и стратегия[1]. Он показывает, что каждый из этих элементов работает при переносе в киберпространство лишь частично. Проблема атрибуции, с одной стороны, делает кибератаки привлекательными для нападающего, с другой стороны, повышает риск ошибок при возмездии. Из-за сложности быстрой и надёжной атрибуции сдерживание сталкивается с большими неопределённостями, что подрывает его эффективность. Ограничения есть и со стратегиями сдерживания: обороной и наказанием. По мнению М. Таддео, оборона в киберпространстве сводится к обеспечению устойчивости системы в случае атак, но не к их отражению, что принципиально отличается от оборонительных стратегий в традиционном сдерживании. Что касается угрозы возмездия, то автор обращает внимание на отличие сдерживания в киберпространстве от ядерного сдерживания, которое часто используется в качестве аналогии. Так, в частности, киберсдерживание является несимметричным, потенциально повторимым, а угрозы не носят экзистенциальный характер. Проблемы сигнализирования связаны со сложностью убедительной демонстрации своих возможностей для обороны или возмездия, что снижает шансы на эффективное сдерживание.

Несмотря на это Россия и США используют концепцию сдерживания в своих подходах к киберпространству, что позволяет проследить, как на практике учитываются ограничения и неопределённости концепции сдерживания в контексте информационного пространства. Выбор России и США как пары для анализа обусловлен, во-первых, их лидирующими ролями в международных дискуссиях о регулировании государственного поведения в киберпространстве и их влиянием на подходы других стран к этой проблеме. Так, усиление конкуренции в подходах США и России усиливает поляризацию позиций других стран, и напротив, когда им удаётся договориться, это благоприятно сказывается на общей атмосфере переговорных процессов на различных международных площадках. Во-вторых, хотя возможности определить баланс сил в киберпространстве ограничены, Россия и США, очевидно, относятся к ведущим державам в этой сфере, имеющим наиболее развитые стратегические взгляды на киберпространство и связанные с ним вопросы сдерживания.

Наконец, выделение этой пары обусловлено давними традициями двустороннего стратегического взаимодействия между Москвой и Вашингтоном, которое оказывало влияние на их взгляды на сдерживание. Как показано в этой статье, и сегодня изменения в подходах к сдерживанию в киберпространстве в обеих странах нередко происходят под влиянием друг друга.

Конструктивитский взгляд на сдерживание

В качестве теоретической основы для рассмотрения интерпретаций сдерживания в киберпространстве в России и США был выбран подход, предложенный А. Луповичи[2]. Основная идея подхода заключается в том, что сложность обеспечения сдерживания в киберпространстве обусловлена не самими техническими

1 Taddeo 2018.
2 Lupovici 2016.

особенностями этой среды, а интерпретацией в социальном контексте. А. Луповичи отмечает, что понимание того, как киберпространство влияет на поведение, является продуктом социального взаимодействия. Ссылаясь на М. Либики, он пишет, что в этой связи правила в киберпространстве являются социально сконструированными: «Эти правила определяют, что осуществимо, уместно и полезно, и это влияет на то, как защищающаяся сторона демонстрирует угрозу и, что более важно, как эти угрозы интерпретируются предполагаемыми соперниками. Именно поэтому конструктивистский подход к киберсдерживанию, акцентирующий внимание на интерсубъективных понятиях, становится весьма актуальным»[1].

Конструктивистский подход, предлагаемый А. Луповичи, позволяет перевести фокус с проблем переноса концепции сдерживания в киберпространство на особенности *интерпретации* этой концепции государствами, что позволяет в ходе их сравнения выявить общие положения, которые могут послужить опорой для дальнейшего развития взглядов на сдерживание в этой сфере.

Дискуссии о терминологии

Одной из проблем международных дискуссий об информационно-коммуникационных технологиях в контексте международной безопасности является отсутствие общепринятой терминологии. Различая в понятийных аппаратах, используемых государствами, отражают особенности их понимания этой сферы и подходов к обеспечению безопасности в ней. Так, между Россией и США на протяжении многих лет сохраняется расхождение в концептуальных подходах к данной теме. В США и других странах Запада предпочтение отдаётся термину «кибербезопасность», под которым понимается защита компьютерных систем, сетей и данных.

В России на официальном уровне используется термин «информационная безопасность»[2]. Информационная безопасность рассматривается в более широком контексте и подразумевает защищённость как от угроз инфраструктуре и информации (аналогично с кибербезопасностью), так и от потенциального воздействия информации на общественное сознание, политическую и социальную ситуацию[3]. Применительно к состоянию глобального информационного пространства используется термин «международная информационная безопасность»[4] (МИБ), прямого аналога которого в западном дискурсе нет.

1 Lupovici 2016, 328.

2 Информационная безопасность Российской Федерации – «состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства». Подробнее см. Доктрина информационной безопасности Российской Федерации (2016) // Российская газета. 2016. [Электронный ресурс]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 24.02.2021).

3 Remington et al. 2016, 1; *Шариков, П.А.* Российско-американские отношения в сфере информационной безопасности // Московский центр Карнеги. 2013. [Электронный ресурс]. URL: https://carnegieendowment.org/files/Article_Sharikov_Russian.pdf.

4 Международная информационная безопасность – «такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на элементы национальной критической информационной инфраструктуры». Подробнее см. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (2013) // Совет Безопасности Российской Федерации. 2013. [Электронный ресурс]. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 02.03.2021).

Помимо различий в подходах между государствами свои терминологии существуют и на уровне профессиональных сообществ, где предпочтение может отдаваться использованию тех или иных понятий, либо же понятия кибербезопасность и информационная безопасность могут использоваться взаимозаменяемо.

Приставка «кибер-» широко используется политиками, журналистами, авторами популярной литературы для образования названий явлений, связанных с цифровой эпохой: «киберпандемия», «кибер- Перл-Харбор», «кибергигиена». С одной стороны, использование этой приставки вызывает узнаваемую ассоциацию с компьютерами и интернетом и может служить удобной отсылкой для смежных областей. С другой стороны, смысл приставки в результате делается все менее конкретным. Некоторые исследователи, например Э. Фаттер, выступают за отказ от повсеместного использования термина «кибер» и за замену соответствующих слов и словосочетаний более точными терминами[1].

В международных организациях для преодоления разногласий вырабатываются громоздкие консенсусные формулировки. Так, в ООН обсуждения правил поведения государств в киберпространстве на протяжении более чем двух десятилетий проводятся в рамках повестки «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», в том числе в форматах Групп правительственных экспертов (ГПЭ) и с 2018 г. – Рабочей группы открытого состава. В ОБСЕ разработка мер доверия для государств в киберпространстве рассматривается в контексте «обеспечения безопасности при всеобъемлющем и многомерном использовании информационных и коммуникационных технологий»[2]. При этом и в рамках ГПЭ, и в ОБСЕ были предприняты шаги по выработке общей терминологии. ГПЭ в докладе 2010 г. рекомендовала найти возможности «для выработки общей терминологии и определений»[3] в связи с обсуждаемыми ей вопросами. В ОБСЕ в аналогичных целях участники договорились в качестве первого шага обменяться перечнями используемых ими терминов[4]. На неправительственном уровне работа ОБСЕ была продолжена, например, фондом «Новая Америка», который при поддержке швейцарского председательства в ОБСЕ запустил проект «Глобальная база данных киберопределений»[5]. Несмотря на все усилия, существенные различия в используемой странами терминологии по-прежнему сохраняются.

В предложенной статье автор опирается на глоссарий «Основы критически важной терминологии» (2-е издание)[6] – российско-американский проект Института проблем информационной безопасности МГУ и Института «Восток-Запад». В глоссарий включены 40 консенсусных определений, выработанных экспертами из Рос-

1 Futter 2018.
2 Решение № 1039 Разработка мер укрепления доверия с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий // ОБСЕ. 2012. [Электронный ресурс]. URL: https://www.osce.org/files/f/documents/6/4/90634.pdf (дата обращения: 24.02.2021).
3 Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. A/70/174 // ООН, Генеральная Ассамблея. 2010. [Электронный ресурс]. URL: https://undocs.org/ru/A/70/174 (дата обращения: 02.03.2021).
4 Решение № 1106 Первоначальный перечень мер укрепления доверия в рамках ОБСЕ с целью сокращения рисков возникновения конфликтов в результате использования информационных и коммуникационных технологий // ОБСЕ. 2013. [Электронный ресурс]. URL: https://www.osce.org/files/f/documents/0/a/109648.pdf (дата обращения: 02.03.2021).
5 "Global Cyber Definitions Database," New America, accessed March 2, 2021, http://cyberdefinitions.newamerica.org/.
6 Godwin et al. 2014.

сии и США. В нём, в частности, даны определения «информационного пространства» («любая среда, в которой информация создается, через которую передается, принимается, в которой хранится, обрабатывается и уничтожается») и «киберпространства» («электронная (включая фотоэлектронные и пр.) среда, в (посредством) которой информация создаётся, передаётся, принимается, хранится, обрабатывается и уничтожается») – следовательно, они соотносятся как общее и частное. Также дано определение «кибербезопасности» (свойство киберпространства (киберсистемы) противостоять намеренным и/или ненамеренным угрозам, а также реагировать на них и восстанавливаться после воздействия этих угроз) и аналогичное определение «информационной безопасности» как свойства информационного пространства. Наконец, в глоссарии определены «средства киберсдерживания» (*cyber deterrent*) (признанный механизм, который считается действенным для препятствования киберконфликту, или угрожающей деятельности в киберпространстве). В качестве средств киберсдерживания могут использоваться, в частности, оборонительные и наступательные возможности в киберпространстве.

Логика, которой придерживались авторы глоссария, полезна для рассмотрения вопросов сдерживания в киберпространстве. В случаях, когда киберпространство не упоминается (например, в российских официальных документах), можно исходить из того, что государственная политика в информационном пространстве распространяется и на киберпространство, оставаясь при этом более широкой по смыслу. В тех же случаях, когда речь идёт прежде всего о киберпространстве, кибербезопасности, логика глоссария позволяет держать в уме их тесную взаимосвязь с информационным пространством, возможное воздействие на неэлектронную среду. Фокус на киберпространстве позволяет сузить рамки исследования и охватить сферу, характеризующуюся новизной и неопределённостью с точки зрения применения концепции сдерживания.

Вопросы сдерживания в киберпространстве в российских стратегических документах

В российских официальных документах киберпространство напрямую не упоминается. Речь идёт об информационном пространстве и, соответственно, (международной) информационной безопасности, информационной сфере. Но, как уже было отмечено, киберпространство относится к информационному как частное к общему, и поэтому изложенные подходы релевантны и для киберпространства.

Сдерживание в контексте информационной безопасности, использования ИКТ, занимает важную роль в российских официальных документах. Формально упоминание сдерживания в данном контексте появилось в Военной доктрине 2014 г.[1] По сравнению с редакцией 2010 г.[2] пункт «Основные задачи Российской Федерации по сдерживанию и предотвращению военных конфликтов» в разделе «Деятельность Российской Федерации по сдерживанию и предотвраще-

1 Военная доктрина Российской Федерации (2014) // Российская газета – Федеральный выпуск № 298(6570). 2014. [Электронный ресурс]. URL: https://rg.ru/2014/12/30/doktrina-dok.html (дата обращения: 24.02.2021).
2 Военная доктрина Российской Федерации (2010) // Сайт Президента России. 2010. [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/461 (дата обращения: 24.02.2021).

нию военных конфликтов» был дополнен семью задачами. Одна из них непосредственно касается сдерживания в киберпространстве: «создание условий, обеспечивающих снижение риска использования информационных и коммуникационных технологий в военно-политических целях для осуществления действий, противоречащих международному праву, направленных против суверенитета, политической независимости, территориальной целостности государств и представляющих угрозу международному миру, безопасности, глобальной и региональной стабильности».

Ещё одно важное нововведение Военной доктрины 2014 г. – понятие «система неядерного сдерживания», под которым понимается «комплекс внешнеполитических, военных и военно-технических мер, направленных на предотвращение агрессии против Российской Федерации неядерными средствами». В тексте Доктрины оно не конкретизировано, но, согласно комментариям составителей документа, неядерное сдерживание должно послужить ответом на разнообразные угрозы и вызовы, которые не могут сдерживаться ядерным оружием[1]. Как отмечает А.А. Кокошин, в контексте развития неядерного сдерживания необходимо учитывать и угрозы в киберпространстве[2].

В более раннем документе, Концептуальных взглядах на деятельность Вооруженных Сил Российской Федерации в информационном пространстве 2011 г.[3] (на основе Доктрины информационной безопасности 2000 г. и Военной доктрины 2010 г.), приведён список из 10 правил «сдерживания и предотвращения военных конфликтов в информационном пространстве», включающих как международные усилия по снижению риска возникновения конфликтов в этой области, так и меры военного характера по выявлению угроз, предотвращению конфликтов и противодействию их развития по пути эскалации.

Наконец, в Доктрине информационной безопасности Российской Федерации 2016 г.[4], «стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий» названо первым в списке направлений обеспечения информационной безопасности в соответствии с российской военной политикой (другие направления: обеспечение информационной безопасности Вооружённых сил; прогнозирование и обнаружение угроз; содействие в защите союзников России; нейтрализация информационно-психологического воздействия).

В предыдущей версии Доктрины от 2000 г.[5] термин «сдерживание» не упоминается. Но среди функций государства по обеспечению информационной безопасности названы меры, направленные на «предотвращение, отражение и нейтрализацию угроз информационной безопасности Российской Федерации», источники которых могут лежать за пределами России.

1 *Набережнов, Г.* В военную доктрину России внесли положение о неядерном сдерживании // РБК. 2014. [Электронный ресурс]. URL: https://www.rbc.ru/politics/13/12/2014/548bf2c22ae59653833655c9 (дата обращения: 24.02.2021).
2 Кокошин 2014, 203.
3 Концептуальные взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве // Министерство обороны Российской Федерации. 2011. [Электронный ресурс]. URL: http://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle (дата обращения: 24.02.2021).
4 Доктрина информационной безопасности Российской Федерации (2016) // Российская газета. 2016. [Электронный ресурс]. URL: https://rg.ru/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 24.02.2021).
5 Доктрина информационной безопасности Российской Федерации (2000) // Гарант. 2000. [Электронный ресурс]. URL: http://base.garant.ru/182535/. (дата обращения: 24.02.2021).

Хотя в этих документах подробно не рассматриваются средства и способы сдерживания в киберпространстве, сдерживание в них описывается, скорее, в оборонительном ключе, то есть в логике «сдерживания посредством недопущения». Прямых указаний на возможность «сдерживания посредством наказания» в документах нет. Это очевидно при сравнении с ядерным сдерживанием: в Военной доктрине чётко оговаривается, в ответ на какие действия Россия может применить ядерное оружие. Однако в целом описание сдерживания в киберпространстве носит в российских официальных документах общий характер.

Концепция сдерживания в киберпространстве (и шире – информационном пространстве) может получить развитие в российских стратегических документах с принятием новой редакции Стратегии национальной безопасности, ожидаемой в 2021 г.[1], и последующим обновлением Военной доктрины. Также изменения могут быть внесены в Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.[2], которые нуждаются в актуализации. В первоначальной редакции документа упоминание сдерживания отсутствовало, но учитывая описанные в этой статье тенденции, появление этой концепции представляется вероятным.

Практическая реализация подходов России к сдерживанию в киберпространстве

Россия избирательно обнародует информацию о развитии военных возможностей для сдерживания в киберпространстве. Так, информация о создании мультисервисной транспортной сети связи – «военного интернета» – освещается достаточно подробно[3]. Планируется, что эта система будет использоваться для военных задач, данные будут храниться на серверах Минобороны, за счёт чего будет обеспечиваться безопасность и защищённость от внешних угроз. С другой стороны, официально почти не публикуется информация о развитии наступательных и других возможностей российских военных в киберпространстве, особенностях сдерживания угроз в этой среде. Большая часть информации в открытом доступе, в частности об операциях, атрибутируемых российским военным или спецслужбам, базируется на журналистских расследованиях, научных публикациях, отчётах компаний по кибербезопасности или специализированных ведомств западных стран[4]. Таким образом, с точки зрения презентации Россией своих усилий в сфере создания возможностей для сдерживания в киберпространстве, акцент делается на усилении обороны, то есть на создание условий для недопущения нанесения ущерба с помощью ИКТ.

«Сдерживание посредством недопущения», очевидно, служит руководящим принципом и для государственной политики в более широком плане.

1 Совбез заявил о готовности новой редакции Стратегии национальной безопасности // ТАСС. 2021. [Электронный ресурс]. URL: https://tass.ru/politika/10676717 (дата обращения: 02.03.2021).

2 Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года (2013) // Совет Безопасности Российской Федерации. 2013. [Электронный ресурс]. URL: http://www.scrf.gov.ru/security/information/document114/ (дата обращения: 02.03.2021).

3 *Рамм, А., Козаченко, А., Степовой, Б.* Военный, красивый, суверенный: армия РФ создает закрытый интернет // Известия. 2019. [Электронный ресурс]. URL: https://iz.ru/854961/aleksei-ramm-aleksei-kozachenko-bogdan-stepovoi/voennyi-krasivyi-suverennyi-armiia-rf-sozdaet-zakrytyi-internet (дата обращения: 24.02.2021).

4 См., например, Lilly 2020.

Показательный пример – «Закон о суверенном Рунете/интернете»[1]. При внесении соответствующего законопроекта его авторы, сенаторы А.А. Клишас, Л.Н. Бокова и депутат Госдумы А.К. Луговой, пояснили, что он «подготовлен с учетом агрессивного характера принятой в сентябре 2018 года Стратегии национальной кибербезопасности США» (имеется в виду Национальная киберстратегия, *National Cyber Strategy* 2018), в которой «Россия впрямую и бездоказательно обвиняется в совершении хакерских атак»[2], что требует дополнительных мер по защите работы интернета в России. Закон, принятый и вступивший в силу в ноябре 2019 г., в частности предписывает операторам связи установку фильтрационного оборудования на точках обмена трафиком, Роскомнадзору – создание системы централизованного управления Рунетом. По закону в России должны регулярно проводиться учения по обеспечению стабильности работы интернета, а также должна быть создана национальная система доменных имён, дублирующая глобальную, на случай отключения России от глобального интернета.

Внешними угрозами обосновывается и импортозамещение иностранного программного обеспечения (ПО). По оценкам Совета Безопасности России, использование на российских объектах критической инфраструктуры зарубежного ПО сопряжено с рисками кибербезопасности, поскольку это может содержать недекларированные уязвимости[3].

Обеспечение суверенитета над национальным сегментом интернета[4] может преследовать разные задачи, а их эффективность – оставаться предметом споров, но с точки зрения сдерживания в киберпространстве они могут быть интерпретированы как шаги по снижению уязвимости России от внешних воздействий в киберпространстве и тем самым обеспечивать «сдерживание посредством недопущения» нежелательного ущерба.

Официальные заявления, касающиеся вопросов информационной безопасности и её международного измерения, также могут интерпретироваться для понимания российских подходов к сдерживанию в киберпространстве. На международном уровне основной посыл представителей России чаще всего заключается в необходимости выработки общих правил и использования дипломатии для предотвращения конфликтов. Главным адресатом таких посланий являются США; так, в сентябре 2020 г. российская позиция была высказана на высшем уровне в предложении президента В.В. Путина восстановить двустороннее сотрудничество в области международной информационной безопасности. Согласно его заявлению: «Одним из основных стратегических вызовов современности является риск возникновения масштабной конфронтации в цифровой сфере. Особая ответственность за её предотвращение ле-

1 Федеральный закон от 1 мая 2019 г. N 90-ФЗ «О внесении изменений в Федеральный закон «О связи» и Федеральный закон «Об информации, информационных технологиях и о защите информации» // Российская газета. 2019. [Электронный ресурс]. URL: https://rg.ru/2019/05/07/fz90-dok.html (дата обращения: 24.02.2021).

2 *Корченкова, Н., Тишина, Ю., Шестоперов, Д.* «Интернет не абонент» // Коммерсантъ. 2018. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3833069 (дата обращения: 24.02.2021).

3 *Петлевой, В., Кантышев, П., Топорков, А.* Зарубежное программное обеспечение – это угроза // Ведомости. 2019. [Электронный ресурс]. URL: https://www.vedomosti.ru/business/articles/2019/01/23/792289-zarubezhnoe-programmnoe-obespechenie (дата обращения: 24.02.2021).

4 Ilona Stadnik, "Sovereign RUnet: What Does it Mean?" Internet Governance Project, Georgia Institute of Technology, 2019, accessed February 24, 2021, https://www.internetgovernance.org/wp-content/uploads/IGPWhitePaper_STADNIK_RUNET-1.pdf.

жит на ключевых игроках в сфере международной информационной безопасности (МИБ)»[1].

Россия не прибегает к практике публичной атрибуции кибератак, в чём проявляется существенное отличие от американского подхода. Более того, российские официальные лица критически оценивают обвинения Вашингтона в адрес конкретных стран в кибератаках и рассматривают такие обвинения как возможный предлог для агрессивных действий. Заместитель секретаря Совета безопасности О.В. Храмов заявил, что участники разведывательного объединения «Пять глаз» (Австралия, Великобритания, Канада, Новая Зеландия, США) «сходятся на том, что виновником компьютерного инцидента можно объявить любое государство и, ссылаясь на закрепленное Уставом ООН право на самооборону, агитируют за возможность предпринимать любые ответные действия»[2]. По его словам, цель обвинения: в одностороннем порядке «легализовать возможность проведения не только информационных, но и военных операций против «неудобных» государств, вплоть до применения ядерных арсеналов»[3].

Если российские представители называют источники тех или иных кибератак, то говорится, как правило, о государстве, с территории которого предположительно осуществлялась вредоносная деятельность. Например, спецпредставитель президента по вопросам международного сотрудничества в области информационной безопасности А.В. Крутских, говоря о нападении на инфраструктуру ЦИК и других российских госорганов в период проведения голосования по поправкам в Конституцию летом 2020 г., заявил: «Источники DDoS-атак мощностью до 240 тыс. запросов в секунду фиксировались с территории США, Великобритании, Украины и ряда стран СНГ»[4].

В российских заявлениях содержатся и намёки на «сдерживание посредством наказания». Так, А.В. Крутских, в 2018 г. комментируя слова Дж. Болтона, на тот момент советника президента США по национальной безопасности, о возможном использовании киберсредств против России, отметил: «А он уверен, что Россия не ответит на подобную провокацию?»[5]. При этом спецпредставитель назвал попытки применить логику сдерживания к киберпространству чудовищной. В июне 2019 г. после публикации *New York Times* о размещении США зловредного ПО (закладок) в российских электросетях, А.В. Крутских процитировал по этому поводу высказывание «кто к нам с кибермечом придет, тот от кибермеча и погибнет»[6]. По его словам, «все политические деятели должны понимать, что за каждым действием будет противодействие. [...] Поэтому желательно этим мечем не размахивать и нас не запугивать»[7].

1 Заявление Владимира Путина о комплексной программе мер по восстановлению российско-американского сотрудничества в области международной информационной безопасности // Сайт Президента России. 2020. [Электронный ресурс]. URL: http://kremlin.ru/events/president/news/64086 (дата обращения: 24.02.2021).

2 *Егоров, И.* Войны виртуальные и реальные // Российская газета. 2019. [Электронный ресурс]. URL: https://rg.ru/2019/08/14/chislo-opasnyh-kiberatak-na-obekty-v-rf-vyroslo-v-11-raz-za-tri-goda.html (дата обращения: 02.03.2021).

3 Там же.

4 При голосовании по конституции в РФ фиксировали DDoS-атаки из США, Великобритании, Украины // ТАСС. 2020. [Электронный ресурс]. URL: https://tass.ru/politika/9391631 (дата обращения: 02.03.2021).

5 *Черненко, Е.В.* Нам не надо бороться за репутацию. Мундир наш и так чист // Коммерсантъ. 2018. [Электронный ресурс]. URL: https://www.kommersant.ru/doc/3611689 (дата обращения: 24.02.2021).

6 Крутских: Москву удивляет, что Трамп назвал статью о кибератаках против РФ госизменой // ТАСС. 2019. [Электронный ресурс]. URL: https://tass.ru/politika/6566204 (дата обращения: 24.02.2021).

7 Крутских о киберугрозах и способах противодействия им // Международная жизнь. 2019. [Электронный ресурс]. URL: https://interaffairs.ru/news/show/22314 (дата обращения: 24.02.2021).

Можно предположить, что противодействием от закладок в российских критических системах могли бы по аналогии быть закладки в критических системах другой стороны, например, США. Действительно, Агентство по кибербезопасности и безопасности инфраструктуры США сообщало о российской правительственной киберактивности, мишенью которой, по их сообщению, были различные организации, относящиеся к критической инфраструктуре[1]. Однако необходимо уточнить, что из этих и подобных сведений сложно выделить мотивацию актора, стоящего за такими действиями (являются ли они действительно инструментом сдерживания или решают иные задачи). Кроме того, российские официальные представители последовательно отрицают причастность России к тем или иным приписываемым ей кибератакам, ссылаясь на отсутствие достаточных доказательств.

Вопросы сдерживания в киберпространстве в американских стратегических документах

В США вопросы безопасности киберпространства появляются в официальных документах с 1990-х гг.[2] Первый полноценный стратегический документ в этой сфере – Национальная стратегия для защиты киберпространства[3] – была принята в 2003 г. администрацией Дж. Буша-мл. Хотя в этой стратегии не содержится самого термина «сдерживание», в ней неоднократно упоминается необходимость сдерживать киберугрозы и злонамеренных акторов, способных нанести ущерб критической инфраструктуре США.

Международная стратегия для киберпространства 2011 г.[4], принятая во время президентства Б. Обамы, включила сдерживание в число основных направлений деятельности США по снижению кибер-рисков наряду с правоохранительными мерами, согласованием норм и правил ответственного поведения государств, мерами укрепления доверия и повышения транспарентности и дипломатией. Сдерживание рассматривается в качестве основы оборонительной части стратегии, причём в документе проводится различие между двумя компонентами такого подхода: убеждением отказаться от атак (*dissuasion*) и угрозой возмездия (*deterrence*). Эти два компонента примерно соответствуют «сдерживанию посредством недопущения» и «сдерживанию посредством наказания». Отмечается, что в рамках сдерживания США оставляют «за собой право использовать все необходимые средства – дипломатические, информационные, военные и экономические – по мере необходимости и в соответствии с применимым международным правом»[5]. Использование военной силы рассматривается как крайний вариант.

Несмотря на то что в документе не прописаны конкретные параметры сдерживания в киберпространстве, в нём отмечены такие особенности, как необхо-

1 "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," CISA, 2018, accessed February 24, 2021, https://us-cert.cisa.gov/ncas/alerts/TA18-074A.
2 Стадник 2018, 159.
3 "National Strategy to Secure Cyberspace (2003)," White House, accessed February 24, 2021, https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf.
4 "International Strategy for Cyberspace (2011)," White House, accessed February 24, 2021, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.
5 Ibid.

димость вовлечения в оборонительные мероприятия всего правительства, частных компаний и граждан, угрозы со стороны преступности и негосударственных акторов, взаимосвязанность безопасности одной страны в киберпространстве с остальным миром. Наконец, в стратегии говорится и о необходимости развития коллективных средств сдерживания в киберпространстве США совместно с партнёрами и союзниками.

При администрации Д. Трампа киберсдерживание ещё более прочно закрепилось в официальных документах по национальной безопасности. Их общей характеристикой стал сдвиг в сторону более решительной и активной политики в киберпространстве на фоне растущих опасений по поводу кибератак и, с другой стороны, желания обеспечить доминирование США в этой среде[1]. В Стратегии национальной безопасности 2017 г.[2] обеспечение безопасности Америки в киберэпоху было выделено в одно из приоритетных направлений в рамках защиты американского народа, страны и образа жизни и включало сдерживание и пресечение деятельности злонамеренных кибераторов. В рамках другого столпа стратегии – «Сохранение мира с помощью силы» – сдерживанию в целом, не только в киберпространстве, отводилась важная роль в возобновившемся «соперничестве великих держав» (стратегическое видение, предложенное администрацией Д. Трампа, предстоящей эпохи как соперничества США с Китаем и Россией). Согласно документу, «сегодня обеспечить сдерживание значительно сложнее, чем во времена холодной войны. Противники изучили американский способ ведения войны и начали развивать возможности, которые нацелены на наши сильные стороны и стремятся использовать наши предполагаемые слабости». К таким возможностям отнесены в том числе киберинструменты. Авторы стратегии делают вывод: «Необходимо распространить сдерживание на все эти области и направить его на все возможные стратегические атаки»[3].

Положения Стратегии национальной безопасности 2017 г. в отношении киберпространства развивались в более специализированных документах: Национальной киберстратегии и Киберстратегии Министерства обороны, принятых в сентябре 2018 г. В первом упомянутом документе сдерживание в киберпространстве вновь рассматривается в контексте сохранения мира с помощью силы. США, с одной стороны, будут продвигать нормы ответственного поведения государств в киберпространстве, а с другой – заниматься атрибуцией и сдерживанием неприемлемого поведения. Это будет обеспечиваться путём идентификации конкретных акторов ответных действий на кибератаки, выстраивания международной коалиции единомышленников для сдерживания в киберпространстве, а также противодействия враждебным информационным операциям[4]. Это отражает меняющееся восприятие угроз в США.

На протяжении многих лет американские представители настаивали на узком понимании кибербезопасности, но в последние годы на фоне скандалов вокруг

1 См. Alexander 2018.
2 "National Security Strategy of the United States of America (2017)," White House, accessed February 24, 2021, https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.
3 Ibid.
4 "National Cyber Strategy of the United States of America (2018)," White House, accessed February 24, 2021. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

российского вмешательства в президентские выборы 2016 г. и различных примеров злонамеренного использования соцсетей на уровне риторики и в отдельных документах киберугрозы все чаще рассматриваются вместе с другими информационными угрозами в более широком контексте.

Наконец, Киберстратегия Пентагона проецирует «соперничество великих держав» на киберпространство: «мы должны обеспечить способность американских вооружённых сил сражаться и побеждать в войнах в любой сфере, включая киберпространство. Это основополагающее требование национальной безопасности США и залог к обеспечению того, чтобы сдерживать агрессию, включая кибератаки, представляющие собой применение силы, против США, наших союзников и наших партнеров»[1]. Непосредственно о сдерживании в стратегии говорится, что США «стремятся использовать все инструменты национальной силы для сдерживания противников от ведения злонамеренной деятельности в киберпространстве, которая угрожала бы национальным интересам США, нашим союзникам или партнёрам». Для Пентагона это в первую очередь предполагает защиту собственных сетей, но также и готовность при необходимости ответить с использованием военной силы. В этом документе вводятся ещё две концепции, которые также должны способствовать сдерживанию: «передовая оборона» (*defend forward*) в киберпространстве, что предполагает пресечение угроз их источника, а также идея «непрерывного» *(persistent*) соперничества, то есть действий против противников в каждодневном режиме, не только в случае конкретных атак.

Важная особенность всех ключевых официальных документов администрации Д. Трампа, касающихся кибербезопасности, заключается в том, что в них обозначены основные противники, которые воспринимаются в США главным объектом сдерживания в киберпространстве: Китай и Россия как два равных соперника *(peer competitors*) и участника «соперничества великих держав». Также это Иран и КНДР, которые проводят враждебную по отношению к США политику и в том числе могут нанести ущерб национальной безопасности с помощью кибератак. Дополнительно к этим странам (которые некоторые американские чиновники окрестили «большой четвёркой»[2]) в числе противников называются негосударственные акторы: террористы и киберпреступники.

Приход Дж. Байдена в Белый дом в 2021 г. открывает новый этап эволюции взглядов на сдерживание в киберпространстве в американских официальных документах. Можно ожидать, что в этой сфере во многом сохранится преемственность: так, ключевые позиции, связанные с кибербезопасностью, в команде нового президента занимают эксперты с большим опытом службы в предыдущих администрациях, в том числе при Д. Трампе[3]. При этом обновлённые стратегические документы будут приниматься под влиянием как последних событий (в том числе таких широко обсуждаемых взломов, как проникновение хакеров в систе-

1 "Department of Defense Cyber Strategy Summary (2018)," U.S. Department of Defense, accessed February 24, 2021, https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF.
2 "Full Transcript of 'Face the Nation' on December 6, 2020," accessed February 24, 2021, https://www.cbsnews.com/news/full-transcript-of-face-the-nation-on-december-6-2020/.
3 Christopher Bing, and Joseph Menn, "After Big Hack of U.S. Government, Biden Enlists 'world Class' Cybersecurity Team," Reuters, January 22, 2021, accessed February 15, 2021, https://www.reuters.com/article/us-usa-biden-cyber-idUSKBN29R18I.

мы федеральных ведомств в США, раскрытое в конце 2020[1]), так и инициатив различных групп влияния внутри США.

Особого внимания заслуживает работа Комиссии по киберпространству (*Cyberspace Solarium Commission*), которая была учреждена Конгрессом в 2019 г. и названа по аналогии с проектом «Солярий», созданным президентом Д. Эйзенхауэром в 1953 г. для определения согласованной стратегии военно-политического сообщества США по противодействию Советскому Союзу. Целью Комиссии по киберпространству было «выработать консенсус в отношении стратегического подхода к защите Соединенных Штатов в киберпространстве от кибератак, чреватых значительными последствиями»[2], а её мандат включал рассмотрение вопросов сдерживания как одного из вариантов защиты США – наряду с продвижением нормативных режимов и срывом враждебных атак. В состав Комиссии вошли члены палаты представителей и сенаторы от обеих партий, высокопоставленные представители Минобороны, ФБР, Министерства внутренней безопасности и других органов. В её основном докладе в марте 2020 г. в качестве нового стратегического подхода к киберпространству было предложено многоуровневое киберсдерживание (*layered cyber deterrence*)[3]. Предполагается, что США будут сдерживать угрозы на трёх уровнях: формирование (ответственного) поведения в киберпространстве (*shape behavior*); недопущение получения противниками выгод с помощью кибератак (*deny benefits*); повышение издержек за счёт поддержания угрозы возмездия (*impose costs*). Эти компоненты уже составляют основу американского подхода к киберсдерживанию, и доклад Комиссии по киберпространству переосмысляет их как часть цельной стратегии.

Доклад Комиссии сам по себе не носил характер стратегического документа, но он содержал более 80 рекомендаций по имплементации предложенного подхода, и 25 из них были включены в закон об ассигнованиях на оборону на 2021 финансовый год[4]. В преддверии инаугурации Дж. Байдена Комиссия, работа которой была продлена до декабря 2021 г., опубликовала «Белую книгу» для новой администрации с предложениями по дальнейшему внедрению основных в области кибербезопасности в политику, в том числе их закрепление в новой редакции Национальной киберстратегии[5].

Практическая реализация подходов США к сдерживанию в киберпространстве

Демонстрация возможностей в киберпространстве является одной из отличительных черт американского подхода к сдерживанию. Несмотря на то что деятельность военных и спецслужб США в этой сфере далеко не является про-

1 Ellen Nakashima, "Biden Administration Preparing to Sanction Russia for SolarWinds Hacks and the Poisoning of an Opposition Leader," Washington Post, February 23, 2021, accessed March 2, 2021, https://www.washingtonpost.com/national-security/biden-russia-sanctions-solarwinds-hacks/2021/02/23/b77039d6-71fa-11eb-85fa-e0ccb3660358_story.html.

2 "H.R.5515 – John S. McCain National Defense Authorization Act for Fiscal Year 2019," § 1652, U.S. Congress, 2018, accessed March 2, 2021, https://www.congress.gov/bill/115th-congress/house-bill/5515/text.

3 "Cyberspace Solarium Commission Report," Cyberspace Solarium Commission, March 2020, accessed March 2, 2021, https://www.solarium.gov/report.

4 "Cyberspace Solarium Commission – NDAA Override Press Release," January 2, 2021, accessed March 2, 2021, https://www.solarium.gov/press-and-news/ndaa-override-press-release.

5 "Transition Book for the Incoming Biden Administration. CSC White Paper #5," Cyberspace Solarium Commission, March 2020, accessed March 2, 2021, https://www.solarium.gov/public-communications/transition-book.

зрачной, о ней известно гораздо больше в сравнении с другими государствами. Официальное и полуофициальное (через санкционированные утечки в СМИ) раскрытие информации может рассматриваться в контексте сдерживания в том смысле, что США повышают таким образом убедительность угрозы ответных действий в ответ на кибератаки. При этом сдерживание вряд ли можно считать единственным поводом для открытости, во многом она мотивирована внутриполитическими соображениями, например, необходимостью показать Конгрессу или налогоплательщикам, что действующая администрация решительно противодействует тем или иным угрозам.

В 2020 г. своё десятилетие отметило Киберкомандование США – главный военный инструмент сдерживания в киберпространстве. По мнению М. Уорнера, с момента своего создания командование выполняло три основные миссии: «(1) защита информационных систем Минобороны, (2) поддержка командующих объединёнными силами с помощью кибероперациий, (3) защита нации от значительных кибератак»[1]. Акцент на сдерживании обозначился в повестке Киберкомандования во второй президентский срок Б. Обамы. Необходимость пересмотра подходов к сдерживанию обсуждалась в контексте растущего внимания к кибератакам против США и ограниченным возможностям военных по их предотвращению.

К 2018 г. Киберкомандование достигло запланированного показателя по численности киберсил (военнослужащих, задействованных в проведении кибероперациий), доведя количество военных хакеров из разных родов сил до 6200, объединённых в 133 команды[2]. В том же году статус Киберкомандования был повышен до самостоятельного объединённого боевого командования – до этого киберсилы были подчинены стратегическому командованию. При этом руководство Киберкомандованием с момента создания по настоящий момент осуществляет глава Агентства национальной безопасности. Изначальным мотивом сдвоенной должности являлось то, что молодое командование, физически базирующееся вместе с Агентством в Форт-Миде, сможет использовать экспертизу и возможности наиболее опытной разведслужбы по радиоэлектронной и технической разведке[3]. Однако на протяжении большей части истории Киберкомандования обсуждается целесообразность разделения роли командующего и главы АНБ.

Помимо создания и развития отдельного командования, специализирующегося на противоборстве в киберпространстве, США демонстрируют свои возможности на примере конкретных операций. Наиболее открыто Киберкомандование делится информацией об операции «Сияющая симфония» против ИГИЛ (запрещенная в России организация)[4], в ходе которой американским военным удалось подорвать работу информационных ресурсов террористической группировки. По мнению исследователя Р. Дебера, раскрытие информации о данной опера-

1 Warner 2020.
2 “Cyber Mission Force Achieves Full Operational Capability,” U.S. Department of Defense, accessed February 24, 2021, https://www.defense.gov/Explore/News/Article/Article/1524747/cyber-mission-force-achieves-full-operational-capability/.
3 Andrew Schoka, “Cyber Command, the NSA, and Operating in Cyberspace: Time to End the Dual Hat,” War on the Rocks, April 3, 2019, accessed February 24, 2021, https://warontherocks.com/2019/04/cyber-command-the-nsa-and-operating-in-cyberspace-time-to-end-the-dual-hat/.
4 Dina Temple-Raston, “How the U.S. Hacked ISIS,” NPR, September 26, 2019, accessed February 24, 2021, https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis.

ции было обосновано соображениями сдерживания: «Ваши кибероперации не смогут реально сдерживать ваших противников, если те не знают, что у вас есть такие возможности»[1]. Официальные лица, включая главу Киберкомандования П. Накасоне, называли операцию «Сияющая симфония» предшественником усилий «по сдерживанию российского вмешательства в выборы 2018 и 2020 гг.»[2].

В 2018 г. во время промежуточных выборов в Конгресс Киберкомандование, согласно репортажам СМИ на основе анонимных источников, нарушило работу Агентства интернет-исследований в Санкт-Петербурге – организации, которую в США рассматривают как один из инструментов российского вмешательства в американскую политику. В статье *Washington Post* ситуация рассматривается в логике сдерживания: «Некоторые американские чиновники утверждали, что "широкомасштабное стратегическое сдерживание" не всегда является целью. [По словам одного военного чиновника], "Мы показали, что возможно в этой сфере. Это больше не старый подход". Эта операция была признана успешной сотрудниками Пентагона, а некоторые сенаторы записали в заслуги Киберкомандованию предотвращение вмешательства России в промежуточные выборы»[3].

В 2019 г. *New York Times* со ссылкой на анонимных чиновников сообщила о размещении США закладок в российских электросистемах. В статье не уточняется, кто за этим стоит, но при описании контекста авторы сообщают, что Киберкомандование, отрабатывая сценарии выборов 2020 г., рассматривало возможность избирательного отключения Россией электроэнергии в ключевых штатах. На этот случай Киберкомандованию необходимо было средство сдерживания[4].

Киберкомандование также реализует расширенное сдерживание, направляя специалистов для проведения совместных операций с союзниками или партнёрами на их территории – например, с сентября до ноября 2020 г. американские военные хакеры посещали Эстонию[5]. Эти так называемые «передовые поисковые операции» (*hunt forward operations*) направлены на поддержку местных киберсил, а также на сбор информации, которая будет полезна для сдерживания угроз.

Подход Киберкомандования администрации Д. Трампа суммирован в статье главы командования и директора АНБ П. Накасоне и старшего советника командования М. Салмейера[6] (впоследствии получившего должность старшего директора по кибербезопасности в Совете национальной безопасности Дж. Байдена[7]). Авторы рассказывают о практической реализации концепций «передовой обо-

1 Dina Temple-Raston, "How the U.S. Hacked ISIS."
2 Dustin Volz, "How a Military Cyber Operation to Disrupt Islamic State Spurred a Debate," Wall Street Journal, January 21, 2020, accessed February 24, 2021, https://www.wsj.com/articles/how-a-military-cyber-operation-to-disrupt-islamic-state-spurred-a-debate-11579604400.
3 Ellen Nakashima, "U.S. Cyber Command Operation Disrupted Internet Access of Russian Troll Factory on Day of 2018 Midterms," Washington Post, 2019, accessed February 24, 2021, https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html.
4 David E. Sanger, and Nicole Perlroth, "U.S. Escalates Online Attacks on Russia's Power Grid," The New York Times, June 15, 2019, accessed February 24, 2021, https://www.nytimes.com/2019/06/15/us/politics/trump-cyber-russia-grid.html.
5 "Hunt Forward Estonia: Estonia, US Strengthen Partnership in Cyber Domain with Joint Operation," U.S. Cyber Command, December 3, 2020, accessed February 24, 2021, https://www.cybercom.mil/Media/News/Article/2433245/hunt-forward-estonia-estonia-us-strengthen-partnership-in-cyber-domain-with-joi/.
6 Paul M. Nakasone, and Michael Sulmeyer, "How to Compete in Cyberspace," Foreign Affairs, January 20, 2021, accessed February 15, 2021, https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.
7 Christopher Bing, and Joseph Menn, "After Big Hack of U.S. Government, Biden Enlists 'world Class' Cybersecurity Team," Reuters, January 22, 2021, accessed February 15, 2021, https://www.reuters.com/article/us-usa-biden-cyber-idUSKBN29R18I. Ellen Nakashima, "Biden Administration Preparing to Sanction Russia for SolarWinds Hacks and the Poisoning of an Opposition Leader."

роны» и «непрерывного воздействия» в киберпространстве: проведении «передовых поисковых операций» в Черногории и других странах, создании специализированной «малой группы» по противодействию российскому вмешательству, онлайн-борьбе с ИГИЛ (запрещенная в России организация) и пр. Резюмируя, они приходят к следующему выводу: консенсус между разными предложениями по защите США в киберпространстве (включая доклад Комиссии по киберпространству) заключается в том, «что для соперничества в этой среде американские киберсилы должны и далее выступать более активно и реализовывать стратегию по борьбе с вредоносной деятельностью противников онлайн»[1]. Уточняется, что действия США при этом должны соответствовать международному праву. Примечательно, что в статье П. Накасоне и М. Салмейера не используется термин «сдерживание», хотя меры, о которых они пишут, в других контекстах представляются именно так.

В качестве инструмента сдерживания в США также рассматривается публичная атрибуция кибератак, также получившая название стратегии «обвинения и пристыжения» (*blaming and shaming*). Так, в 2014 г. первой страной, против граждан которой США выдвинули обвинение за государственное хакерство, был Китай[2]. Публичная атрибуция со стороны американского правительства может осуществляться в нескольких формах: преимущественно технических отчётах Агентства по кибербезопасности и безопасности инфраструктуры, обвинительных заключениях Министерства юстиции, заявлениях спецслужб, политических заявлениях Госдепартамента и других высокопоставленных чиновников.

Публичная атрибуция позволяет сигнализировать противникам, стоящим за кибератаками, что их действия не остаются скрытыми, и за счёт «пристыжения» создаёт стимул для них воздерживаться от аналогичных действий в будущем, чтобы избежать репутационных и иных издержек. Несмотря на критику эффективности такого подхода, американская практика публичной атрибуции кибератак распространяется и на некоторых их союзников, прежде всего участников объединения «Пять глаз» и Нидерланды.

Публичная атрибуция может сопровождаться введением санкций против лиц и организаций, причастных к кибератакам. Так, в октябре 2020 г. Министерство финансов США ввело санкции по закону *CAATSA* против российской научно-исследовательской организации ЦНИИХМ, которая, по оценке Минфина, участвовала в кибератаке против нефтехимического завода на Ближнем Востоке[3].

Уникальным для киберпространства инструментом сдерживания в США стала так же загрузка образцов зловредного программного обеспечения, используемого противниками, на сайт *VirusTotal*. *VirusTotal* даёт возможность специалистам по кибербезопасности делиться вредоносным кодом, что позволят быстрее проводить анализ подозрительных файлов. Но США, загружая на сайт инструменты, используемые враждебными хакерами или другими странами для кибератак, помогает

1 Paul M. Nakasone, and Michael Sulmeyer, "How to Compete in Cyberspace."
2 "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," U.S. Justice Department, May 19, 2014, accessed February 24, 2021, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.
3 "Treasury Sanctions Russian Government Research Institution Connected to the Triton Malware," U.S. Department of the Treasury, 2020, accessed February 24, 2021, https://home.treasury.gov/news/press-releases/sm1162.

компаниям по кибербезопасности учитывать их при разработке своих решений и при проведении расследований.

Таким образом, Киберкомандование подрывает наступательные возможности оппонентов, выводя из строя их кибероружие. На *VirusTotal* благодаря американским военным попали образцы кода, предположительно используемого северокорейскими[1], иранскими[2] и российскими хакерами[3].

Защита собственной инфраструктуры также интерпретируется в США как часть сдерживания в широком понимании. Это стало особенно заметно в контексте обеспечения безопасности электоральных процессов, что можно рассматривать как «сдерживание посредством недопущения». Так, после президентских выборов 2020 г. руководитель Агентства по кибербезопасности и безопасности инфраструктуры США заявил об отсутствии свидетельств о внешнем вмешательстве, причиной чего стала хорошая подготовка властей на разных уровнях и привлечение к защите выборов частного сектора.

Дипломатия также рассматривается в США как средство сдерживания угроз в киберпространстве. Вашингтон вместе с союзниками активно продвигает необходимость выработки и соблюдения правил ответственного поведения государств в киберпространстве. Во время президентства Б. Обамы США заключили двусторонние договорённости по безопасности в киберпространстве с Россией в 2013 г.[4] и Китаем в 2015 г.[5] Однако сегодня опыт этих соглашений для предотвращения киберугроз в США оценивается неоднозначно. Так называемая «горячая линия» по вопросам, связанным с киберугрозами, между Россией и США сохраняется, но в Вашингтоне считают, что созданные механизмы не предотвратили вмешательство в выборы 2016 г.[6] Американо-китайское соглашение о том, что стороны не будут проводить друг против друга кибероперации с целью кражи интеллектуальной собственности, согласно оценкам американских фирм по кибербезопасности, в течение первого года после заключения привело к резкому снижению китайских кибератак против американских компаний. Однако к началу президентства Д. Трампа атаки возобновились[7]. Представитель АНБ Р. Джойс в 2018 г. заявлял, что, по мнению США, Китай не соблюдал договорённости[8].

1 Shannon Vavra, "Cyber Command's Biggest VirusTotal Upload Looks to Expose North Korean-Linked Malware," CyberScoop, September 8, 2019, accessed February 24, 2021, https://www.cyberscoop.com/cyber-command-virus-total-north-korean-malware/.

2 Shanon Vavra, "Why Cyber Command's Latest Warning Is a Win for the Government's Information Sharing Efforts," CyberScoop, July 10, 2019, accessed February 24, 2021, https://www.cyberscoop.com/cyber-command-information-sharing-virustotal-iran-russia/.

3 Catalin Cimpanu, "US Cyber Command Exposes New Russian Malware," ZDNet, November 1, 2020, accessed February 24, 2021, https://www.zdnet.com/article/us-cyber-command-exposes-new-russian-malware/.

4 Совместное заявление президентов Российской Федерации и Соединенных Штатов Америки о новой области сотрудничества в укреплении доверия // Сайт Президента России. 2013. [Электронный ресурс]. URL: http://www.kremlin.ru/supplement/1479 (дата обращения: 24.02.2021).

5 "Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference," White House, September 25, 2015, accessed February 24, 2021, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

6 Erin Banco, and Kevin Poulsen, "This Hotline Could Keep the U.S. and Russia From Cyberwar," The Daily Beast, February 23, 2019, accessed February 24, 2021, https://www.thedailybeast.com/this-hotline-could-keep-the-us-and-russia-from-cyber-war.

7 Laskai et al. 2018.

8 "U.S. Accuses China of Violating Bilateral Anti-Hacking Deal," Reuters, November 9, 2018, accessed February 24, 2021, https://www.reuters.com/article/us-usa-china-cyber-idUSKCN1NE02E.

Выводы

Теоретические подходы к сдерживанию в киберпространстве развиваются в тесной связке с их практическим использованием для обеспечения странами своих интересов в этой сфере. Как показано в статье, классические и новые способы сдерживания находят применение в арсенале России и США. Однако, учитывая ограниченность эмпирических знаний, говорить об эффективности тех или иных подходов преждевременно.

Важно учитывать процесс конструирования странами практики сдерживания в киберпространстве. Попытка интерпретации российских и американских взглядов на сдерживание в киберпространстве, предпринятая в этой статье, позволяет сопоставить их и обратить внимание на характерные для каждой страны особенности. Как в США, так и в России, сдерживание в киберпространстве закреплено в официальных документах. В России эта концепция понимается в более широком контексте обеспечения информационной безопасности. При этом параметры сдерживания представлены в стратегических документах в общих чертах и не конкретизированы. В США развитие концепции киберсдерживания в официальных документах имеет более долгую историю, а её описание более детализировано. И в России, и в США сдерживание в киберпространстве понимается прежде всего в военно-политическом смысле, но не исключительно. Американский подход предполагает использование для сдерживания разных инструментов; в России подчеркивается роль дипломатии и международных договорённостей как средства предотвращения конфликтов.

Наиболее заметное различие во взглядах, вероятно, заключается в том, что и на уровне документов, и на практике США делают ставку на «сдерживание посредством возмездия». Это проявляется, в частности, в готовности демонстрировать возможности по сдерживанию в киберпространстве. США за счёт относительно открытого строительства Киберкомандования, раскрытия деталей некоторых кибероперациий стремятся сделать угрозу возмездия в киберпространстве более убедительной. Российская демонстрация возможностей «сдерживания посредством возмездия» на официальном уровне отсутствует. Но принимая во внимание высказывания российских официальных представителей, а также сообщения о приписываемых России атаках, справедливо полагать, что и в Москве рассматривают «сдерживание посредством возмездия» как возможную стратегию.

Россия, в свою очередь, на практике делает акцент на оборонительных мерах, что можно трактовать как предпочтение «сдерживанию посредством недопущения». Несмотря на различие используемых мер, у России и США схожее понимание необходимости защиты критической инфраструктуры как части сдерживания в более широкой трактовке, однако в США практика «возмездия» превалирует над практикой «недопущения».

Две страны придерживаются противоположных взглядов на проблему публичной атрибуции кибератак. В Вашингтоне публичную атрибуцию считают одним из способов сдерживания киберугроз. И хотя её эффективность остаётся дискуссионным вопросом, США продолжают использовать этот инструмент и призывают к коллективной атрибуции союзников. В Москве же обвинение

в адрес конкретных государств считают не только нелегитимными из-за недостаточной доказанности, но и потенциально опасными, поскольку они могут использоваться для оправдания агрессивных действий против предполагаемых виновников. Соответственно, Россия не рассматривает атрибуцию как средство сдерживания.

Подходы к сдерживанию в киберпространстве в обеих странах эволюционируют, причём некоторые изменения связаны с поведением другой стороны. Так, в России обоснованием «Закона о суверенном Рунете/интернете» стало принятие новой Национальной киберстратегии США, в которой Россия обозначалась в качестве угрозы. В этом документе сдерживание не только распространяется на киберпространство, но и захватывает информационные угрозы – то, против чего США многие годы выступали на международных площадках.

Это наблюдение подводит к выводу о том, что подходы к сдерживанию в двух странах формируются по мере взаимных попыток истолковать намерения и поведение друг друга. Этот процесс носит долгосрочный характер и тесно связан с проблемой выработки общих глобальных подходов к киберпространству.

СПИСОК ЛИТЕРАТУРЫ / REFERENCES

Кокошин, А.А. Стратегическое ядерное и неядерное сдерживание: приоритеты современной эпохи // Вестник Российской академии наук. – 2014– Т. 84 (3). – С. 195–205. https://doi.org/10.7868/S0869587314030086. [Kokoshin, A. A. "Strategic Nuclear and Non-nuclear Deterrence: Priorities of the Modern Era." [Strategicheskoe yadernoe i neyadernoe sderzhivanie: prioritety sovremennoi ehpokhi] *Bulletin of the Russian Academy of Sciences* 84, no. 3 (2014): 195–205] [In Russian].

Печатнов, Ю.А. Теория сдерживания: генезис // Вооружение и экономика. – 2016. – №2 (35). – С. 26–27. [Pechatnov, Yu. A. "Theory of Deterrence: Genesis." [Teoriya sderzhivaniya: genezis] *Armament and Economics*, no. 2 (2016): 26–27] [In Russian].

Стадник, И.Т., Цветкова, Н.А. Политика кибербезопасности США эволюция восприятия угроз // Международные процессы. – 2018. – Т. 16 (3). – С. 157–169. https://doi.org/10.17994/IT.2018.16.3.54.9. [Stadnik, Ilona, and Natalia Tsvetkova. "United States Cybersecurity Policy." [Politika kiberbezopasnosti SSHA ehvolyutsiya vospriyatiya ugroz] *International Trends / Mezhdunarodnye Protsessy* 16, no. 3 (February 1, 2019): 157–169] [In Russian].

Alexander, Keith B., and Jamil N. Jaffer. "Ensuring US Dominance in Cyberspace in a World of Significant Peer and Near-Peer Competition." *Georgetown Journal of International Affairs* 19 (2018): 51–66.

Futter, Andrew. "'Cyber' Semantics: Why We Should Retire the Latest Buzzword in Security Studies." *Journal of Cyber Policy* 3, no. 2 (May 4, 2018): 201–16. https://doi.org/10.1080/23738871.2018.1514417.

Godwin III, J. B., Andrey Kulpin, Karl F. Rauscher, and Valery Yaschenko. *Critical Terminology Foundations 2, Russia-US Bilateral on Cybersecurity.* East-West Institute, Policy Report 2, 2014. http://www.ipib.msu.ru/UserFiles/File/Terminology%20IISI%20EWI/Russia-U%20S%20%20bilateral%20on%20terminology%202.pdf.

Huth, Paul K. "Deterrence and International Conflict: Empirical Findings and Theoretical Debates." *Annual Review of Political Science* 2, no. 1 (June 1999): 25–48. https://doi.org/10.1146/annurev.polisci.2.1.25.

Laskai, Lorand, and Segal, Adam. *A New Old Threat: Countering the Return of Chinese Industrial Cyber Espionage*. Council on Foreign Relations, 2018. https://www.cfr.org/report/threat-chinese-espionage.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. RAND Corporation, 2009. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf.

Lilly, Bilyana, and Joe Cheravitch. "The Past, Present, and Future of Russia's Cyber Strategy and Forces." In *2020 12th International Conference on Cyber Conflict (CyCon),* 129–55. Estonia: IEEE, 2020. https://doi.org/10.23919/CyCon49761.2020.9131723.

Lupovici, Amir. "The 'Attribution Problem' and the Social Construction of 'Violence': Taking Cyber Deterrence Literature a Step Forward." *International Studies Perspectives* 17, no. 3 (August 1, 2016): 322–42. https://doi.org/10.1111/insp.12082.

Mazarr, Michael J. *Understanding Deterrence.* RAND Corporation, 2018. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE295/RAND_PE295.pdf.

Nye, Joseph S. "Deterrence and Dissuasion in Cyberspace." *International Security* 41, no. 3 (January 2017): 44–71.

Remington, T., Chris Spirito, Elena Chernenko, Oleg Demidov, and Vitaly Kabernik. *Toward U.S.-Russia Bilateral Cooperation in the Sphere of Cybersecurity*. Working Group on the Future of U.S.-Russia Relations Paper 7, 2016. https://us-russiafuture.org/publications/working-group-papers/toward-u-s-russia-bilateral-cooperation-in-the-sphere-of-cybersecurity/.

Ryan, N. J. "Five Kinds of Cyber Deterrence." *Philosophy & Technology* 31, no. 3 (September 27, 2018): 331–38. https://doi.org/10.1007/s13347-016-0251-1.

Schelling, Thomas C. *Arms and Influence.* Yale University Press, 2008.

Snyder, Glenn H. "Deterrence and Power." *The Journal of Conflict Resolution* 4, no. 2 (June 1960): 163–78.

Taddeo, Mariarosaria. "The Limits of Deterrence Theory in Cyberspace." *Philosophy & Technology* 31, no. 3 (September 16, 2018): 339–55. https://doi.org/10.1007/s13347-017-0290-2.

Warner, Michael. "US Cyber Command's First Decade." *A Hoover Institution Essay. Aegis Series Paper,* no. 2008 (2020). https://www.hoover.org/sites/default/files/research/docs/warner_webready.pdf.

Сведения об авторе

Шакиров Олег Игоревич,
консультант ПИР-Центра, Россия, 119019, Москва, а/я 147.
e-mail: shakirov@pircenter.org

Дополнительная информация

Поступила в редакцию: 1 декабря 2020. Принята к публикации: 31 января 2021.

Конфликт интересов

Автор заявляет об отсутствии потенциального конфликта интересов.

Цитирование

Шакиров, О.И. Кто придёт с кибермечом: подходы России и США к сдерживанию в киберпространстве // Международная аналитика. – 2020. – Том 11 (4). – С. 147–170. https://doi.org/10.46272/2587-8476-2020-11-4-147-170

Whoever Comes to Us With a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace

ABSTRACT

Developed in recent decades, the understanding of cyberspace as an environment in which a state can face serious threats to its security has contributed to a search for ways to prevent such threats. In the military and political spheres, the concept of deterrence has become one of the ways to solve this problem. During the Cold war, the policy of deterrence became central to the strategic thought in the leading countries, but the direct transfer of conventional approaches to a new reality turns out to be problematic. On the one hand, this opens up a debate about the ways to attain deterrence in cyberspace via traditional and new mechanisms. However, theoretical discussions on cyberspace deterrence highlight the limitations of this concept. At the same time, despite some uncertainties that stem from such a transfer, in practice, the leading states use the concept of deterrence in the context of their activities related to cyberspace, although they implement it differently. In this regard, the article suggests focusing on states' interpretation of deterrence when designing and implementing their policies in this area, rather than on the problems of applying the concept of deterrence. Such a constructivist approach allows to reveal the peculiarities of the understanding of deterrence without considering them predetermined and identify common aspects of views. Using Russia and the United States as examples, we studied specific features of the application of the deterrence concept in respect to cyberspace in official documents and in the course of the practical implementation of their provisions. The analysis shows that countries interpret the concept of cyberspace deterrence in different ways, with an emphasis on specific deterrence strategies. At the same time, Russia and the United States influenced each other while developing views on deterrence.

KEYWORDS

Russia, United States, cyberspace, deterrence, information security, cyber security

Author

Oleg I. Shakirov,
Consultant of the PIR Center, Russia, 119019, Moscow, po / po 147.
e-mail: shakirov@pircenter.org

Additional Information

Received: December 1, 2020. Accepted: January 31, 2021.

Disclosure statement

No potential conflict of interest was reported by the author.

For citation

Shakirov, Oleg I. "Whoever Comes to Us With a Cyber Sword: Russian and U.S. Approaches to Deterrence in Cyberspace." *Journal of International Analytics* 11, no. 4 (2020): 147–170. https://doi.org/10.46272/2587-8476-2020-11-4-147-170