Connections: The Quarterly Journal
ISSN 1812-1101, e-ISSN 1812-2973

Мануэль Фишер, *Connections QJ* 18, № 1-2 (2019): 81-109
https://doi.org/10.11610/Connections.rus.18.1-2.05

Рецензированная статья

Концепция сдерживания и ее применимость в кибер домене

Мануэль Фишер

Европейский центр исследований по вопросам безопасности им. Джорджа К. Маршалла, http://www.marshallcenter.org

Резюме: Киберпространство, как пятый домен, вездесуще, и все развитые государства все больше осознают, что международные отношения и типичные области, охватываемые государством, меняются перед лицом глобальной дигитализации. С появлением технологий, меняющих правила игры, традиционные инструменты государственности, такие как сдерживание, кажутся устаревшими в процессе построения стратегии национальной безопасности. В частности, развитые государства сильно зависят от открытого и безопасного киберпространства, но в то же время страдают от множества уязвимостей. Недавнее прошлое показало, что изощренные кибератаки могут серьезно подорвать деятельность правительств, экономик и обществ и, следовательно, создать угрозу основным интересам безопасности. Как классический инструмент международных отношений, сдерживание может способствовать усилению защите интересов национальной безопасности, даже если киберпространство требует некоторых особых соображений. Поэтому в статье объясняются основные механизмы сдерживания в ядерном веке и при современных международных отношениях, правовые основы киберпространства и возможные способы применения сдерживания в киберпространстве. Статья призвана побудить мировых лидеров внимательно рассматривать сдерживание в киберпространстве как мощный актив, и предоставить политикам варианты действий.

Ключевые слова: кибербезопасность, кибероперации, сдерживание, правовая база.

Введение

Говорить о сдерживании в 21 веке – все равно что раскапывать остатки ушедшей эпохи. С появлением ядерных технологий и, главным образом, во времена Холодной войны, сдерживание было темой не только для политиков и академических кругов, но и влияло на повседневную жизнь миллионов людей, независимо от того, к какому «блоку» они принадлежали. С тех пор сдерживание уменьшило вес в общественном восприятии вместе с ядерными арсеналами великих держав. То, что осталось, по-прежнему имеет огромный потенциал, но как инструмент государственности, а не как основополагающий момент.

В частности, государства сталкиваются с постепенным изменением традиционно ориентированной на государство структуры международной системы, особенно в таких привычных областях государственных функций, как безопасность. Классическое понимание войны и конфликта размывается, а традиционные государственные структуры, кажется, не успевают реагировать с помощью классических инструментов, поскольку конфликт нового типа является многослойным (политическим, военным и экономическим, среди прочего), осуществляемым в основном невоенными средствами, такие как пропаганда и политическая агитация, и среди различных государственных и негосударственных субъектов.[1,2]

Перед лицом ежедневных и непрекращающихся атак на государства и их органы,[3] встает вопрос: что мешает игроку в киберпространстве снова и снова проводить одни и те же атаки или даже подниматься по лестнице эскалации и причинять необратимый ущерб, если это служит его интересам.

---

1 David J. Betz, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (London and New York: Routledge, 2017), 80.

2 Joseph S. Nye, Jr., “Deterrence and Dissuasion in Cyberspace,” *International Security* 41, no. 3 (Winter 2016/2017): 44–71, цитата на с. 48, https://doi.org/10.1162/ISEC_a_00266.

3 Как это произошло в Германии в 2015 году, когда российская хакерская группа под названием «Fancy Bear» атаковала парламент Германии, шпионила по крайней мере за 16 его членами (включая Ангелу Меркель) и извлекла несколько частично конфиденциальных документов. К тому времени Федеральная канцелярия впервые за несколько десятилетий заговорила о (гибридной) войне и потенциальных ответных ударах. Смотри: Patrick Beuth, Kai Biermann, Martin Klingst, and Holger Stark, “Bundestags-Hack – Merkel und der schicke Bär,” *Zeit Online*, May 10, 2017, http://www.zeit.de/2017/20/cyberangriff-bundestag-fancy-bear-angela-merkel-hacker-russland. И тем не менее, то же самое произошло снова в конце 2017 года, когда сотрудники службы безопасности обнаружили предположительно российскую «устойчивую серьезную угрозу», нацеленную на министерство иностранных дел, которая скомпрометировала сеть на срок до года. Смотри: Thorsten Severin and Andrea Shalal, “German Government under Cyber Attack, Shores up Defenses,” *Reuters*, March 1, 2018, www.reuters.com/article/us-germany-cyber/german-government-under-cyber-attack-shores-up-defenses-idUSKCN1GD4C8.

Кажется, что в киберпространстве нет ни уважения, ни страха перед возмездием, ни серьезных технических барьеров – или, другими словами, нет никакого сдерживания.

В этой статье будет рассмотрен вопрос, эффективна ли концепция сдерживания только в том случае, если она связана с ядерным оружием, и становится ли она бесполезной в международной системе, которая больше не является доминируемой (чисто) ядерным оружием, а киберпреступлениями. Автор утверждает, что это не так! Даже в киберпространстве сдерживание может быть мощным инструментом государственности, способствовать защите интересов национальной безопасности государства. Чтобы доказать эту гипотезу, в этой статье будет тщательно исследована концепция сдерживания, заглянув в прошлое, которое дает разнообразные примеры по этой теме, чтобы, наконец, спроецировать результаты на настоящее. Поэтому будут изучены существующие концепции сдерживания и особые последствия для киберпространства вместе с правовой базой все более дигитализированной международной системы, чтобы в итоге найти эффективные способы применения сдерживания в киберпространстве.

Данное исследование проводится при следующих общих предположениях и исключениях:

- Появляющиеся мобильные технологии пятого поколения (5G) и облачные технологии будут стимулировать распространение Интернета вещей. Критические процессы будут постепенно перенесены на эти технологии, и кибер риски будут расти в геометрической прогрессии, поскольку новые устройства создают больше возможностей для потенциальных проникновений. Кроме того, контролируя физические активы, можно нанести даже физический вред.[4,5]
- Согласно «парадигме предположение о неизбежности проникновения», весьма вероятно, что каждый достаточно сложный программный продукт имеет критические уязвимости и что обновления либо не предоставляются, либо уязвимость держится в секрете.[6]
- Это исследование будет сосредоточено на политических киберугрозах и будет охватывать криминальную кибер-деятельность только в той мере, в какой она происходит в контексте конфликта. Традиционный шпионаж с помощью кибер-средств будет исключен из этого исследования.

---

[4] "BSI: Critical infrastructures – Definition," Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security, Federal Office of Civil Protection and Disaster Assistance, 2017, www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html.

[5] James Manyika, et al., *The Internet of Things: Mapping the Value beyond the Hype* (McKinsey & Company, June 2015), 11.

[6] "BSI: Critical Infrastructures," 18.

Механизмы сдерживания

Концепция сдерживания так же стара, как стремление человечества воевать друг с другом.[7] Термин «сдерживание» происходит от слова «террор», которое отражает страх перед издержками, связанными с определенным действием. В академической литературе иногда используется термин «разубеждение» для обозначения более широкого круга мер, которые направлены не только на несение издержек, но и на лишение противника определенных выгод.[8] Для четкого разграничения и ввиду преобладающего использования в политической и академической сферах, в этой работе термин «сдерживание» будет использоваться как общий термин, учитывая тот факт, что это понятие гораздо шире.

Джозеф Най также принимает во внимание оба значения, определяя сдерживание как [9]

> … отговаривать кого-то от каких-либо действий, заставляя его поверить, что затраты для него превысят ожидаемую выгоду.

Это означает сохранение статус-кво, не позволяя оппоненту проводить действия, которые считаются неблагоприятными. Речь не идет о принуждении противника к определенному поведению и, таким образом, изменении статус-кво.[10] Рассмотрение ключевых механизмов и их применение в международных отношениях (МО) поможет понять точки соприкосновения и проложить путь к киберсдерживанию.

Согласно теоретику сдерживания сэру Майклу Куинлану,[11] «не существует такого понятия, как государство, неподверженное сдерживанию».[12] В качестве основных условий для успешного сдерживания (независимо от того, в какой сфере) он рассматривает следующие пять пунктов: [13]

1. Вероятности
2. Способность и серьезное намерение

---

[7] Ранние упоминания восходят к работе Фукидида о Пелопоннесской войне, даже до появления христианского календаря, см. Richard Ned Lebow, “Thucydides and Deterrence,” *Security Studies* 16, no. 2 (2007): 163–188, цитата на стр. 163 https://doi.org/10.1080/09636410701399440.

[8] Michael Quinlan, “Deterrence and Deterrability,” in *Deterrence and the New Global Security Environment*, ed. Ian R. Kenyon and John Simpson (London: Routledge, 2006), 5.

[9] Nye, “Deterrence and Dissuasion in Cyberspace,” 45.

[10] Wyn Q. Bowen, “Deterrence and Asymmetry: Non-state Actors and Mass Casualty Terrorism,” *Contemporary Security Policy* 25, no. 1 (2004): 54-70, https://doi.org/10.1080/1352326042000290506.

[11] Бывший постоянный заместитель государственного секретаря Министерства обороны Великобритании; влиятельный стратег в области обороны и сдерживания.

[12] Quinlan, “Deterrence and Deterrability,” 7.

[13] Quinlan, “Deterrence and Deterrability,” 4.

3. Декларация сдерживания
4. Перспектива возникновения многосторонних затрат
5. Использование всего диапазона возможных ответов.

Вероятности

Идеальное сдерживание должно было бы работать с определенностями, например: «Если ты возьмешь мой обед, я сломаю твою игрушку». Но поскольку человеческое взаимодействие носит довольно сложный характер, возникает ряд неопределенностей, и неправильное восприятие и неверное толкование неизбежны. Чтобы принять это во внимание, необходимо учитывать вероятности.[14] Важную роль играют не только потенциальная выгода («обед») и стоимость проигрыша («игрушка»), но и вероятность успеха или проигрыша. Как следствие, параметры вероятности выигрыша («вы не можете быть уверены, что получите мой обед, потому что я попытаюсь его защитить») и вероятности проигрыша («если вы возьмете мой обед, я сделаю все возможное, чтобы уничтожить вашу игрушку» и, может быть, у меня все получится») необходимо добавить к следующему вычислению решения:[15,16]

*Значение выигрыша * Вероятность выигрыша < Величина потери * Вероятность проигрыша*

Эффективное сдерживание в неопределенной среде должно учитывать все четыре фактора неравенства, чтобы левая часть оставалась меньше правой в восприятии противника.

Способности и серьезное намерение

Способности – это основа, на которой противник может рассчитать ценность, которую он может получить или потерять. Однако существует также необходимость в убедительном намерении использовать эти возможности, чтобы оказать воздействие на вычисление вероятностей.[17] Мощные меры, обеспечивающие наступление, могут увеличить величину потерь, серьезность наступательных и защитных мер может изменить расчет вероятности выигрыша и проигрыша.

*Значение выигрыша * Вероятность выигрыша (↓) < Величина потери (↑)* Вероятность проигрыша (↑)*

---

[14] Quinlan, “Deterrence and Deterrability,” 4.

[15] Philip Bobbitt, *Democracy and Deterrence: The History and Future of Nuclear Strategy* (Basingstoke: Palgrave Macmillan, 1988), 8.

[16] Jeffrey R. Cooper, “A New Framework for Cyber Deterrence,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Georgetown University Press, 2012): 105-120, 109.

[17] Scott Jasper, *Strategic Cyber Deterrence: The Active Cyber Defense Option* (Lanham, Maryland: Rowman & Littlefield, 2017), 9.

В то время как способности – это, скорее, вопрос денег, а убедительное намерение может быть доказано только действием, тем не менее, оба требуют «демонстрации силы», чтобы они были восприняты оппонентом.[18]

Декларация сдерживания

Помимо способностей и убедительности, важное значение имеет эффективная передача правильного сообщения о сдерживании правильной аудитории.[19,20] Следовательно, очень важно указать какие действия будут запрещены, что (наступательные или оборонительные) способности для соответствующего реагирования имеются и что они будут задействованы.[21] Здесь чрезмерно точное, самоограничивающее определение не является необходимым и даже может быть вредным, поскольку оно открывает противнику путь для уклонения от ответа или для воспрепятствования ответа.[22] Эффективная коммуникация дает противнику определенные факторы для его расчетов и уменьшает количество неверных интерпретаций или неверных восприятий. Более того, сильное заявление о сдерживании само по себе может повлиять на восприятие вероятностей выигрыша и проигрыша.

*Значение выигрыша * Вероятность выигрыша (🡻) < Величина потери * Вероятность проигрыша (🡹)*

Нынешние эксперты, такие как бывший заместитель министра обороны США по вопросам политики Джеймс Миллер, отмечают, что «на самом деле вы не сдерживаете государства, вы сдерживаете отдельных лиц и группы лиц, принимающих решения …».[23] Это означает, что декларацию о сдерживании необходимо разработать в обратном порядке, начиная с желаемого

---

[18] США продемонстрировали новые способности во время вторжения в Панаму в 1989 году, применив стелс истребитель-бомбардировщик F-117, конечно, не из-за угрозы панамской ПВО, а для демонстрации новых способностей в наборе инструментов, см. Richard A. Clarke and Robert K. Knake, *Cyber War: What It Is and How to Fight It* (New York: HarperCollins, 2010), 194.

[19] Bowen, “Deterrence and Asymmetry,” 51.

[20] Jasper, *Strategic Cyber Deterrence*, 9.

[21] Хотя четко обозначенная красная линия отсутствует, США служат хорошим примером, публично предлагая ИТ-подрядчикам побороться за контракт почти на 500 миллионов долларов на разработку и, при необходимости, развертывание, смертоносного кибероружия. Исполнительный директор киберкомандования США заявил, что США ищут привлекающие внимание кибер инструменты, которые можно проследить до США. Смотри Jasper, *Strategic Cyber Deterrence*, 102.

[22] Quinlan, “Deterrence and Deterrability,” 4.

[23] Sean D. Carberry, “Why There’s no Silver Bullet for Cyber Deterrence,” *Federal Computer Week (FCW)*, June 06, 2017, https://fcw.com/articles/2017/06/06/carberry-cyber-deterrence.aspx.

эффекта и с учетом того, как она будет обрабатываться теми, кого она должна сдерживать.[24] Предположение о том, что противник действует рационально, довольно упрощено, поскольку для этого нужна точная информация и готовность принимать решения, основанные только на стратегических последствиях. Лица, принимающие решения, никогда не имеют точной информации, и на них оказывают влияние многие факторы, такие как эмоции или личные интересы.[25]

Перспектива возникновения многосторонних затрат

Создание защитных сооружений может лишить противника желаемого эффекта или, по крайней мере, уменьшить его. Это посеет семена сомнения в сознании противника, поскольку ему нужно больше времени и ресурсов, и вероятность обнаружения возрастает.[26] Короче говоря, меры лишения увеличивают альтернативные издержки претендента. Сочетание мер возмездия и лишения, а также увеличение разнообразия затрат мешают оппоненту заблаговременно подготовить и укрепить свои ценности.[27] Таким образом, увеличивается как величина потерь, так и вероятность потерь.

*Значение выигрыша * Вероятность выигрыша < Величина потери (↑) * Вероятность проигрыша (↑)*

Чтобы увеличить этот эффект, может быть, целесообразно адаптировать стратегию к конкретному противнику. Это требует контекстного знания мотивов данного актора, процессов принятия решений, структур командования и контроля и будет означать необходимость проведения существенных разведывательных действий и проявления понимания культуры оппонента.[28]

---

[24] То, как противник интерпретирует заявление о сдерживании, зависит от его истории и стратегической культуры и является источником неправильного толкования, основанного на различных предпочтениях и ожиданиях. Смотри James Andrew Lewis, “Rethinking Deterrence,” Report (Washington: Brzezinski Institute on Geostrategy, May 2016), 5, https://csis-website-prod.s3.amazonaws.com/s3fs-public/170713_Deterrence_Stability_0.pdf.

[25] Will Goodman, “Cyber Deterrence: Tougher in Theory than in Practice?” *Strategic Studies Quarterly* 4, no. 3 (Fall 2010): 102–135, 107, https://www.hsdl.org/?view&did=18663.

[26] Bowen, “Deterrence and Asymmetry,” 50.

[27] Такое сочетание аспектов наказания и воспрещения имело место при администрации Джорджа Буша для сдерживания использования нетрадиционного оружия с вызывающими озабоченность режимами посредством сочетания возможностей воспрещения (разработка всеобъемлющей противоракетной обороны) и угрозы неукоснительного наказания. Смотри Bowen, “Deterrence and Asymmetry,” 50.

[28] Bowen, “Deterrence and Asymmetry,” 51.

Использование всего диапазона возможных ответов

Если демонстрируемые затраты не соответствуют средствам или размаху действий, которые пытаются предотвратить, можно сдержать даже противников разных размеров и с разными системами ценностей.[29] Использование всего диапазона возможных ответов затрудняет противнику возможность предугадать ответ и защитить себя. Таким образом, величина потерь, а также вероятность потерь могут быть увеличены.

*Значение выигрыша * Вероятность выигрыша < Величина потери (⬆) * Вероятность проигрыша (⬆)*

Поскольку государство обычно обладает монополией на применение силы и обладает широким спектром кинетических средств, это может быть преимуществом при столкновении с негосударственными противниками. Переключение областей реагирования на классические и знакомые области государственности может укрепить легитимность и убедительность.[30]

Особые последствия для кибер домена

С тех пор как государства и правительства начали взаимодействовать друг с другом на арене МО, сдерживание было ценным инструментом. Наиболее влиятельная эра сдерживания наступила с появлением ядерного оружия и, по существу, определила курс Холодной войны. Есть параллели с кибер-веком, которые могут оказать ценную помощь, но есть также аспекты, которые следует игнорировать.

Атомная бомбардировка Хиросимы и Нагасаки в 1945 году внезапно заставила мир встать лицом к лицу с новым военным потенциалом, который воспринимался как непреодолимый и приводящий к не выживанию. Стратегам потребовалось несколько лет, чтобы перейти от так называемого «массированного возмездия» НАТО через поворотные моменты, вызванные шоком «Спутник»-а и кубинским кризисом, и последующей концепции сдерживания через «взаимное гарантированное уничтожение» до всеобъемлющей стратегии «гибкого реагирования». Это была многоступенчатая концепция, переходящая от обычной обороны к стратегическому применению ядерного оружия. Она был основана на потенциале (обычные и ядерные силы) и, по крайней мере, на некоторой убедительности (США нанесли ядерный удар по Японии), полагаясь на весь спектр средств (от обычных ответных мер до тактических и стратегических ядерных средств), чтобы обещать многогранные затраты (удары по военным и экономическим целям на

[29] Quinlan, “Deterrence and Deterrability,” 4.

[30] Когда пропагандистская машина Исламского государства стала слишком сильной и неконтролируемой, правительство США обратилось к смертоносной силе в виде воздушных ударов по высокопоставленным оперативникам СМИ, которые стали законными мишенями в вооруженном конфликте из-за их связи с террористической группировкой. Смотри Jasper, *Strategic Cyber Deterrence*, 95.

поле боя и на родине), но не было самоограничения в способах реагирования (не было заранее определенной лестницы эскалации).[31]

Эта четко определенная стратегия действительно привнесла определенную стабильность в международную систему и основывалась на пяти факторах, которые характеризовали тогдашнюю современную концепцию войны (и, следовательно, сдерживания) в среде новых и сложных технологий [32]:

1. *Фактор времени:* Исключительно большой ущерб теперь можно было нанести за короткое время, практически без предварительного предупреждения.
2. *Фактор силы:* Немедленно наличные силы превосходили силы мобилизации из-за фактора времени.
3. *Фактор выживания:* необходимо было выжить при первом исключительно тяжелом ударе, чтобы начать контратаку.
4. *Фактор глобализации:* ядерная война немедленно охватила бы весь мир.
5. *Фактор обороны:* оборона НАТО должна была основываться на демонстрации сильных сторон, а не на защите слабых сторон.

НАТО по-прежнему является ядерным альянсом (в основном основанным на потенциале и решимости США), и ядерное сдерживание остается частью его оборонной стратегии. Тем не менее, после холодной войны мировые атомные арсеналы систематически сокращались, и появлялись различные неядерные технологии. Некоторые даже говорят, что в контексте мощных альтернатив, ядерному оружию отводится пассивная и символическая роль в МО.[33] В то же время вертикальное [34] и горизонтальное [35] распространение деструктивных технологий стало легче осуществлять и сложнее контролировать.[36]

---

[31] "Nuklearstrategie – Zwischen Abschreckung und Einsatzdoktrin," *Bundeszentrale für politische Bildung*, https://sicherheitspolitik.bpb.de/m6/articles/nuclear-strategy-between-deterrence-and.

[32] Bruno Thoß, *NATO-Strategie und nationale Verteidigungsplanung: Planung und Aufbau der Bundeswehr unter den Bedingungen einer massiven atomaren Vergeltungsstrategie 1952 bis 1960* (München: Oldenbourg Verlag, 2006).

[33] Lewis, "Rethinking Deterrence," 5.

[34] Увеличение количества и изощренности оружия установившихся обладателей такого оружия. Смотри Ian R. Kenyon and John Simpson, eds., *Deterrence and the New Global Security Environment* (Abingdon: Routledge, 2006).

[35] Распространение ядерной технологии среди других. См. Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

[36] Фактически, признанные ядерные державы обеспокоены тем, что их ядерное сдерживание может быть обойдено или уничтожено с помощью современных обычных вооружений. Они не дойдут до ядерного порога, и таким образом,

Но даже если концепции ядерного сдерживания невозможно скопировать, все же можно узнать как можно разработать комплексную стратегию использования новых и мощных технологий.[37] Параллельно с ядерной эрой, кибер-эра означает развитие новой, созданной руками человека и трудной для понимания технологии, обладающей огромным потенциалом для гражданского использования и, в то же время, для невообразимого разрушения. Эти общие черты позволяют предположить, что те же факторы, что и в ядерном сдерживании, играют, по крайней мере, основную роль в киберсдерживании. В следующем параграфе будут рассмотрены ранее представленные факторы времени, сил, выживания, глобализации и обороны в киберсфере и добавлен к набору аспектов кибер-специфический фактор атрибуции.

Фактор времени

В кибер эпохе для самой атаки влияние фактора времени, похоже, стремится к нулю, поскольку искусственный интеллект использует алгоритмы для выполнения основных, но трудоемких задач, а участники по всему миру подключаются друг к другу за миллисекунды. Эта так называемая «сетевая скорость» создает одновременность причинно-следственной связи, которая устраняет необходимость дорогостоящего и трудного преодоления расстояния. Теперь даже небольшие субъекты могут влиять на состояние без предварительного предупреждения.[38] Однако это справедливо только для самой атаки. Как и во время Холодной войны, подготовка поля битвы – необходимое предварительное условие для атаки на сетевой скорости. Подобно выявлению командных бункеров, продвинутый кибер-атакующий должен проникнуть в систему и воспроизвести ее схему, получить доступ и разместить бэкдоры.[39,40] Это означает, что нужна долгосрочная кампания, которая не может быть проведена полностью с компьютера, а состоит из сложных операций агентурной разведки (HUMINT).[41]

нанесение удара, по силе равного ядерному, по жизненно важным объектам может остаться безнаказанным, см. Lewis, “Rethinking Deterrence,” 4.

37 Clarke and Knake, *Cyber War: What It Is*, 155.

38 Betz, *Cyberspace and the State*, 39.

39 Richard B. Andres, “The Emerging Structure of Strategic Cyber Offense, Cyber Defense, and Cyber Deterrence,” in *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, ed. Derek S. Reveron (Washington, DC: Georgetown University Press, 2012), 89–104.

40 Clarke and Knake, *Cyber War: What It Is*, 30.

41 Jeffrey Carr, “Responsible Attribution: A Prerequisite for Accountability,” Tallinn Paper No. 6 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014).

Фактор силы

Силы с новейшими технологическими знаниями и оборудованием, находящиеся непосредственно и постоянно в расположении, превосходили мобилизационные силы благодаря временному фактору. Все еще правительства используют те же концепции, что и для не кибератак, делегируя задачи защиты и сдерживания мелких субъектов местной полиции и используя федеральные агентства только против государственных субъектов или террористических групп.[42] Это означает фрагментацию ответственности и наличие непоследовательной стратегии. В то же время, технологические знания и оборудование стоят огромных денег и требуют гибких и специализированных структур. И то, и другое доступно только в определенной степени в государственных структурах, и поэтому все более значительная роль отводится частному сектору.

Особое внимание уделяется цепочке поставок программного и аппаратного обеспечения для ИТ. Часто вопросы кибербезопасности и защиты данных не рассматриваются на стадии разработки, и последующее исправление уязвимостей не всегда возможно.[43] Компрометируя оборудование на ранней стадии разработки, можно создать уязвимости и легко распространить их по цепочке поставок.[44] Это позволяет сфокусировать внимание на всю цепочку, вплоть до мельчайшего «умного клапана». Хотя такие мишени могут показаться незначительными, было оценено, что на них концентрируются особо изощренные агенты, представляющие собой угрозу.[45] Таким образом стало критически важно определять кто производит, испытывает и сертифицирует оборудование, откуда поступают запасные части и какие процессы производства и распределения должны находиться под постоянным национальным контролем.

Фактор выживания

Способность пережить первый удар и способность действовать были ключевым элементом в ядерной обстановке. Кибердомен также кажется средой, в которой доминируют наступательные действия, в которой атакующие имеют структурное преимущество перед обороняющимися, и опреде-

---

[42] Andres, “The Emerging Structure of Strategic Cyber Offense,” 91.

[43] ENISA, “Threat-Landscape-Report 2017” (Heraklion: European Union Agency for Network and Information Security), 107, www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017/at_download/fullReport.

[44] Это явление связано не только с киберпространством. В течение многих лет Министерство обороны США борется с контрафактными деталями в своих важнейших цепочках поставок оборонной продукции. См. United States Government Accountability Office (GAO), “Counterfeit Parts: DOD Needs to Improve Reporting and Oversight to Reduce Supply Chain Risk” (Washington D.C.: US GAO, 2016), https://www.gao.gov/products/GAO-16-236.

[45] ENISA, “Threat-Landscape-Report 2017,” 110.

ленная защита невозможна. Более того, промышленно развитые и связанные страны кажутся более уязвимыми, чем менее развитые.[46,47] Это приводит к самосдерживанию мощных, промышленно развитых и связанных государств, как в эпоху ядерной войны. Осознавая свою собственную кибер-уязвимость, возникает нежелание использовать обычное превосходство в других областях (например, в обычных вооружениях).[48] Поскольку кажется невозможным снизить уровень взаимосвязанности в современных обществах, лучшим вариантом является усовершенствование сдерживания и способов защиты.[49]

Фактор глобализации

Подобно ядерной войне, кибератаки игнорируют барьеры и границы в реальном мире. Атакующему больше не нужно находиться рядом с местом действия или в зоне досягаемости обороняющихся.[50] Сетевая скорость сокращает пространственное расстояние до нуля и позволяет субъектам, находящимся за пределами юрисдикции государства, применять силу против него с хорошими шансами никогда не быть привлеченными к ответственности.[51] Это ведет к глобальной кибер-арене, где государственные субъекты часто связаны законами, тогда как нападающие легко ускользают от их действия.[52,53] Даже в большей степени, чем в ядерный век, такие атаки могут иметь широкий спектр последствий, что затрудняет прогнозирование их масштаба. Кибер-инструмент, такой как вирус, может отпрыгнуть назад, распространиться в другие страны или создать непредсказуемый глобальный хаос за считанные минуты.[54]

Еще одним аспектом глобализованной арены является геополитическая симметрия даже для государств, не соседствующих друг с другом. Если государство не обладает преимуществом осуществлять эскалацию (благоприятная асимметрия силы и средств), оно может изо всех сил пытаться адекватно отомстить, поскольку оно должно опасаться проиграть серию эскала-

---

[46] Jack L. Goldsmith, “How Cyber Changes the Law of War,” in *Current and Emerging Trends in Cyber Operations: Policy, Strategy and Practice*, ed. Frederic Lemieux (London: Palgrave Macmillan, 2015), 51–61.

[47] Thomas Rid and Ben Buchanan, “Attributing Cyber Attacks,” *Journal of Strategic Studies* 38, no. 1-2 (January 2015): 4–37, https://doi.org/10.1080/01402390.2014.977382.

[48] Clarke and Knake, *Cyber War: What It Is*, 157.

[49] Clarke and Knake, *Cyber War: What It Is*, 149.

[50] Goldsmith, “How Cyber Changes the Law of War,” 53.

[51] Betz, *Cyberspace and the State*, 39.

[52] Clarke and Knake, *Cyber War: What It Is*, 30.

[53] Andres, “The Emerging Structure of Strategic Cyber Offense,” 92.

[54] Goodman, “Cyber Deterrence,” 116.

ций в конце концов в физической сфере.[55]

Фактор обороны

К сожалению, в киберпространстве отсутствуют четкие нормы того, что такое надлежащая защита и каковы соответствующие ответные меры.[56,57] Помимо того факта, что киберконфликт выходит за рамки традиционного поля боя и имеет место в повседневных системах (например, в банках, телекоммуникациях и управлении воздушным движением[58]), самая большая проблема для сдерживания заключается в том, что наступательные и оборонительные способности поддерживаются в соответствии с кодексом молчания. С одной стороны, противник может подготовить собственную защиту, если он знает о нападении противника, а с другой стороны, нет стимула раскрывать проникновение, поскольку это может испортить репутацию жертвы. Таким образом, нет шанса поучиться у других и разработать надлежащие средства защиты.[59] В контексте сдерживания это контрпродуктивно (поскольку постоянное информирование о четких и целенаправленных ухудшениях сдерживания является ключевым моментом) и должно преодолеваться компромиссом, заключающимся в сохранении в тайне как можно больше информации, но раскрывая и коммуникируя ее количество, достаточное для осуществления эффективного сдерживания.[60]

Фактор атрибуции

Атрибуция не была большой проблемой в ядерный век, и даже сегодня, когда только девять государств обладают ядерным оружием и хорошо известными идентификаторами изотопов каждого арсенала, это не вызывает особого беспокойства.[61] Но в отличие от ядерного оружия, киберсредства труднее отследить, и стопроцентное приписывание оружия к источнику редко возможно.[62] Широко распространено мнение, что это подрывает концепцию сдерживания, но на самом деле, даже при несовершенной атрибуции сдерживание возможно, если речь идет о трех аудиториях [63]:

---

[55] Эстония не хотела приписывать кибератаки 2008 года России (даже если у нее были веские доказательства) из-за геополитического дисбаланса и возможной физической эскалации против значительно превосходящих российских вооруженных сил. См. Goodman, “Cyber Deterrence,” 109.

[56] Carberry, “Why There’s no Silver Bullet for Cyber Deterrence.”

[57] Andres, “The Emerging Structure of Strategic Cyber Offense,” 101.

[58] Clarke and Knake, *Cyber War: What It Is*, 30.

[59] Andres, “The Emerging Structure of Strategic Cyber Offense,” 93.

[60] Goodman, “Cyber Deterrence,” 109; Andres, “The Emerging Structure of Strategic Cyber Offense,” 101.

[61] Nye, “Deterrence and Dissuasion in Cyberspace,” 50.

[62] Clarke and Knake, *Cyber War: What It Is*, 68.

[63] Nye, “Deterrence and Dissuasion in Cyberspace,” 51.

1. *Защищающееся государство* хочет получить относительно высокие гарантии от своих спецслужб и сетевых криминалистов;
2. *Атакующий государственный или негосударственный субъект* знает, что было сделано, но не может быть уверен, насколько хороши противостоящие криминалистика и разведка; даже если он отрицает нападение, он никогда не узнает, насколько правдоподобным был этот обман;
3. *Национальную и международную общественность* необходимо убедить в справедливости возмездия. Следовательно, необходимо раскрыть определенную степень подробностей, даже если при этом определенные методы криминалистической экспертизы могут стать бесполезными для будущих дел.

Качество атрибуции зависит от доступных ресурсов, наличного времени и изощренности противника. Чем меньше в наличии высококлассных криминалистов и высококвалифицированного персонала, тем ниже будет качество атрибуции. Чем выше давление времени для атрибуции, тем ниже будет качество. Чем более опытен оппонент и располагает большим финансированием, тем ниже будет качество атрибуции.[64]

Сегодня вопрос не столько в том, *можно ли* атрибутировать кибератаку, сколько в том, *сколько времени* это займет.[65] Пока все кибератаки следуют шаблону Cyber-Kill-Chain [66] и подразумевают участие человека-противника, будут ошибки, индивидуальные мотивы и отношения, которые сделают возможным отслеживание, противодействие и сдерживание.[67] Этот факт вызывает еще одну параллель с ядерным веком. Работать с людьми нельзя виртуально или из-за компьютера. Лучший способ приписать атаку после того, как она произошла, – это уже иметь развернутую разведывательную кампанию инфильтрации и создания доверенных контактов на месте.[68] Эти довольно традиционные методы агентурной разведки (HUMINT) снова становятся важными и могут опередить предпочитаемые в последнее время и

---

[64] Rid and Buchanan, “Attributing Cyber Attacks,” 32.

[65] Tim Maurer, “Here’s How Hostile States Are Hiding behind ‘independent’ Hackers,” *The Washington Post*, February 1, 2018, www.washingtonpost.com/news/monkey-cage/wp/2018/02/01/heres-how-hostile-states-are-hiding-behind-independent-hackers.

[66] Eric M. Hutchins, Michael J. Cloppert, and Rohan M. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” *Leading Issues in Information Warfare & Security Research* 1, no. 1 (2011): 1–14, 5, www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

[67] “Cybersecurity’s Maginot Line: A Real-World Assessment of the Defense-in-Depth Model,” Complimentary Report (Milpitas: FireEye Inc., June 2014), www.iqpc.com/media/1003877/33776.pdf.

[68] Carr, “Responsible Attribution,” 8.

удобные методы анализа сигналов (SIGINT).[69]

Правовая база киберпространства

Подобно появлению ядерного оружия, информационная эпоха принесла с собой революционные современные технологии, которые изменили представление о МО и их правовых рамках. Некоторые даже утверждают, что эти новые технологии опередили право и что современное законодательство не может полностью регулировать возникающие кибер способности.[70,71] Но поскольку изолированные решения отдельных участников не могут работать, только международное право (МП) может обеспечить правовую основу регулирования в кибер сфере. Международное общество по-прежнему пытается понять последствия дигитализированного мира, и ему нужно время, чтобы воплотить МП в кибер-специфические договоры и обычное право. До тех пор потенциал эскалации в киберпространстве остается значительным, поскольку государства могут полагаться на свободу действий, прибегая к различным позициям в интерпретации.[72] Единственный способ уменьшить этот деструктивный потенциал – обеспечить стабильную и приемлемую правовую основу.

В 2013 году Группа правительственных экспертов ООН согласилась с тем, что международное право – и, в частности, Устав ООН – применимо в кибер сфере.[73] Эта новаторская позиция всемирно признанного органа стала первым важным шагом к заполнению законодательного вакуума в киберпространстве. Она сопровождалась выпуском «Таллиннского руководства по

---

[69] Clarke and Knake, *Cyber War: What It Is*, 215.

[70] Это становится актуальным в контексте «презумпции законности» международного права, согласно которой действия, которые не запрещены, разрешены. Поскольку современные информационные технологии прямо не рассматриваются в международном праве, у государств есть большая свобода действий до тех пор, пока существующие пробелы не закрываются обычным правом или явными договорами. См. Michael N. Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (New York, NY: Cambridge University Press, 2016), 51, Rule 11.9.

[71] Michael N. Schmitt, "The Law of Cyber Targeting," Tallinn Paper No. 7 (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2015), https://ccdcoe.org/uploads/2018/10/TP_07_2015.pdf.

[72] Michael N. Schmitt and Liis Vihul, "The Nature of International Law Cyber Norms," Tallinn Paper No. 5, Special Expanded Issue (Tallinn: NATO Cooperative Cyber Defence Centre of Excellence, 2014), https://ccdcoe.org/uploads/2018/10/Tallinn-Paper-No-5-Schmitt-and-Vihul.pdf.

[73] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/70/174 (United Nations General Assembly, 2015), 12, https://digitallibrary.un.org/record/799853.

международному праву, применимому к кибервойне», а в 2017 году – Таллиннским руководством 2.0, которые были подготовлены как необязывающие исследования под руководством Совместного центра НАТО передового опыта по кибер защите (CCDCOE).[74] ЕС даже пошел дальше этого мнения, заявив в своей Стратегии кибербезопасности, что «те же законы и нормы, которые применяются в других сферах нашей повседневной жизни, применяются также и в киберсфере».[75]

Соответственно, для всех государств правила поведения в киберпространстве определяются условиями МП, и для нахождения эффективной и надежной позиции сдерживания необходимо прояснить следующие моменты:

- Как классифицировать кибератаку в соответствие с международным правом?
- Какая реакция на кибератаку является законной?
- Какие цели являются законными при обмене кибер атак?

Классификация кибератак в соответствие с международным правом

В Таллиннском руководстве 2.0 сказано, что «принцип государственного суверенитета применяется в киберпространстве», и, таким образом, государство может принимать все меры, не запрещенные МП, которые оно считает необходимыми и подходящими для работы со своей кибер-инфраструктурой, с участниками киберпространства или с кибер-деятельностью на своей территории.[76,77] Следовательно, любая враждебная кибероперация, направленная против кибер и не кибер-инфраструктуры государства, означает нарушение суверенитета в случае причинения физического вреда или травм.[78] Не так обстоят дела, если при атаке происходит манипулирование или удаление баз данных с целью подорвать экономику или повлиять на политические процессы. Хотя некоторые теоретики требуют включения этих

[74] NATO Cooperative Cyber Defence Centre of Excellence, https://ccdcoe.org/.

[75] Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace (Brussels: European Union, 2013), 3, https://edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en.

[76] Michael N. Schmitt and Liis Vihul, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* (New York: NATO Cooperative Cyber Defence Centre of Excellence, 2017), 11.

[77] Cited in Jasper, *Strategic Cyber Deterrence*, 142.

[78] Michael N. Schmitt, "'Below the Threshold' Cyber Operations: The Countermeasures Response Option and International Law," *Virginia Journal of International Law*, 54, (2014): 697-732.

нефизических эффектов, они все еще выходят за рамки общей интерпретации.[79]

Кибероперации не являются кинетическими по своей природе и поэтому часто ошибочно воспринимаются как несиловые, хотя их последствия могут варьировать от простого беспокойства до причинения смерти. Таким образом, кибератаки необходимо оценивать в соответствии с их воздействием на реальный мир и, если они имеют результат, сопоставимый с кинетической атакой, они представляют собой «применение силы».[80,81] Однако государству разрешается проводить силовые защитные действия только в случае «вооруженного нападения», что означает, что применение силы должно достигнуть определенного порога.[82,83] Этот уровень иногда сохраняется в состоянии стратегической двусмысленности, чтобы противнику было сложнее прогнозировать потенциальные действия самообороны.[84] Таллиннское руководство 2.0 становится конкретным только для актов сбора кибер разведданных, кибер-кражи и кратковременного прерывания несущественных услуг, которые не квалифицируются как вооруженные нападения из-за отсутствия серьезных травм или смертей или причинения серьезного

---

79 Michael N. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," *Villanova Law Review* 56, no. 3 (2011): 569-605, 574; Schmitt and Vihul, "The Nature of International Law Cyber Norms," 17.

80 Устав ООН запрещает применение силы или угрозу силой, требуя: «все члены должны воздерживаться в своих международных отношениях от угрозы силой или ее применения против территориальной целостности или политической независимости любого государства или любым другим способом, несовместимым с целями Объединенных наций». См. United Nations, "Charter of the United Nations" (United Nations, 2016), Article 2 (4).

81 Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 573.

82 Это также может иметь место, если серия киберинцидентов (каждый из которых по отдельности находится ниже порога вооруженной атаки) суммируется. Следовательно, они должны иметь один и тот же источник, должны быть связаны друг с другом и, вместе взятые, должны иметь необходимый масштаб. См. Schmitt, *Tallinn Manual on the International Law*, 56, Rule 13.8.

83 United Nations, "Charter of the United Nations," Article 51.

84 В соответствии с этим, на саммите НАТО в Уэльсе в 2014 году было решено определять, приведет ли кибератака к применению статьи 5 (и таким образом, будет считаться вооруженным нападением) в каждом конкретном случае. См. See Schmitt and Vihul, "The Nature of International Law Cyber Norms," 26. По мнению Lewis, "Rethinking Deterrence," 9, эта стратегическая двусмысленность пороговых значений создает путаницу и ослабляет сдерживающий эффект. Ядерная стратегия НАТО «Гибкое реагирование», напротив, держала свою лестницу эскалации в стратегической двусмысленности (понимая, что способности были известны в любом случае), но делала красные линии очень четкими. См. Kenyon and Simpson, *Deterrence and the New Global Security Environment*.

ущерба.[85,86] Для атак, которые не достигают порога вооруженного нападения, но представляют собой незаконное применение силы, могут применяться только контрмеры, направленные на прекращение нападения.[87] Если применение силы сводится к вооруженному нападению, осуществляемому с помощью классической военной силы, которое вызывает или может привести к уничтожению имущества и ранениям или смерти, тогда разрешаются силовые оборонительные действия. Если кибероперация является составной частью общей военной операции, она представляет собой вооруженное нападение, даже если в отдельности не может быть квалифицирована как таковое.[88] Следовательно, у государств есть стимул быстро рассматривать чистые кибероперации как вооруженное нападение, чтобы оправдать силовой оборонительный ответ, что значительно увеличивает вероятность эскалации.[89]

Законные меры реагирования на кибератаки

Государство, ставшее жертвой незаконной кибероперации, имеет определенные права в соответствии с международным правом, если атака достигает как минимум уровня применения силы. Это всегда начинается с законного требования компенсации за физические или финансовые потери и с ненасильственных ответных действий, таких как блокирование входящей передачи данных. Кроме того, в ответ на выявленное применение силы могут быть приняты типичные технические, политические или экономические контрмеры, направленные на прекращение и возмещение ущерба. Эти меры могут включать ограниченную степень применения военной силы и обычно противоречат международным обязательствам, но являются закон-

---

85 Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, 339.

86 Цитируется в Jasper, *Strategic Cyber Deterrence*, 142.

87 Таллиннское руководство 2.0 гласит в правиле 20, что государства имеют право принимать контрмеры (кибермеры или не кибермеры) в ответ на нарушение международно-правовых обязательств другим государством. Правило 69 гласит, что кибероперация представляет собой применение силы, если они имеют сопоставимые эффекты, такие как операции, не связанные с киберпространством, которые можно квалифицировать как применение силы. Контрмеры в этом случае могут быть направлены только на устранение существующего ущерба, пока существует угроза, а не на цели возмездия. Кроме того, противник должен быть предупрежден заранее, чтобы дать ему возможность прекратить атаку. См. Schmitt and Vihul, *Tallinn Manual 2.0 on the International Law*, цитируется в Jasper, *Strategic Cyber Deterrence*, 174.

88 Schmitt, “Cyber Operations and the *Jus Ad Bellum* Revisited,” 587.

89 Подход США в этом вопросе несет в себе именно эту опасность, но кажется эффективным на кибер-арене, поскольку любое использование силы рассматривается как вооруженное нападение и может подвергаться силовому ответу. См. Schmitt, “‘Below the Threshold’ Cyber Operations,” 730.

ными, если они соразмерны нанесенному ущербу и ниже порога вооруженного нападения. Однако необходимо заранее призвать противостоящее государство воздерживаться от продолжения или принять меры для прекращения действий, исходящих с его территории.[90,91] Право принимать контрмеры сохраняется за государствами, даже если существуют частные ИТ-компании, чьи кибер-возможности превышают арсенал государства. Тем не менее, Таллиннское руководство 2.0 прямо упоминает право потерпевшего государства обращаться к частным фирмам для проведения кибероперациий от его имени. Конечно, ответственность за контрмеры, проводимые капером, лежит на государстве.[92,93]

Если применение силы достигает уровня вооруженного нападения (независимо от того, было ли оно инициировано государством или негосударственным субъектом), применяется право на самооборону, и могут проводиться необходимые и соразмерные силовые действия против атакующего противника.[94] Поскольку нет международного консенсуса относительно границы между применением силы и вооруженным нападением, это становится вопросом интерпретации и убедительности потерпевшего государства, поскольку МП не диктует уровень достоверности атрибуции, чтобы начать действия в целях самообороны.[95] Возникает вопрос, как реагировать на действия негосударственных субъектов, которые, по определению, не могут нарушать запрет на применение силы по международному праву, установленный для государств. В таких случаях ответственность государства предлагает возможность в любом случае применить МП. Государство несет ответственность не только за действия своих правительственных органов, но и за поведение отдельных лиц или групп, которые действуют по указанию или под контролем государства.[96] Более того, государство может быть привлечено к ответственности за противоправные действия негосударственных субъектов на его территории, если оно не принимает надлежащих мер для прекращения атак или не предоставляет всю доступную

---

[90] Schmitt, *Tallinn Manual on the International Law*, 36, Rule 9.

[91] Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 581.

[92] Schmitt, "'Below the Threshold' Cyber Operations," 727.

[93] Jasper, *Strategic Cyber Deterrence*, 179.

[94] Schmitt, *Tallinn Manual on the International Law*, 54, Rule 13.

[95] Carr, "Responsible Attribution," 7.

[96] Международный Суд (ICJ) создал прецедент решением по делу Никарагуа, в котором он признал США ответственными за нарушения международного гуманитарного права, совершенные повстанческой группировкой, которую США «эффективно контролировали». См. Schmitt, "Cyber Operations and the *Jus Ad Bellum* Revisited," 578.

поддержку для расследования инцидентов.[97,98] Если такое государство не желает или неспособно выполнять свои юридические обязанности, пострадавшее государство может действовать в порядке самообороны и остановить атаку кинетическими или кибер-средствами даже на территории другого государства. Но самооборона возможна не только в ответ на продолжающееся вооруженное нападение. Ее также можно проводить в условиях неминуемой атаки (о чем свидетельствуют враждебные действия, такие как подготовительные кибероперации, которые приведут к последствиям на уровне вооруженной атаки), без какой-либо другой разумной надежды на ее отражение, кроме немедленного ответа.[99]

Законные цели при обмене кибератаками

Если ситуация доходит до того, что силовая самооборона или возмездие становится законным вариантом, возникает вопрос о том, как и что атаковать. Киберсфера характеризуется повсеместной инфраструктурой двойного назначения, которая может быть предназначена для использования в гражданских целях, но по характеру, местоположению, назначению или применению может использоваться в военных целях.[100] Поэтому, в соответствии с международным гуманитарным правом (МГП) эта инфраструктура становится законной военной мишенью, поскольку ее полное или частичное разрушение, захват или нейтрализация предлагает прямое и конкретное военное преимущество. В конечном итоге, это означает, что из-за сильной зависимости от гражданских продуктов и гражданской инфраструктуры, диапазон целевых объектов на кибер-арене расширяется, и системы с важными гражданскими функциями могут стать законным объектом воздействия.[101] В случае силового ответа в обмене кибератак это дает определенную гибкость в выборе целей, но, в то же время, кибер-средства сталкиваются с проблемой сложной масштабируемости и специфического выбора мишеней. МГП требует, чтобы применяемое оружие позволяло отличать комбатантов от гражданских лиц и гражданских объектов от военных. Если кибероружие не может быть направлено на конкретный военный объект

[97] Международный Суд создал прецедент в деле о проливе Корфу, приняв решение о том, что государство нарушает свои международные обязательства, если оно позволяет сознательно использовать свою территорию для противоправных действий против других государств. См. Schmitt, “Cyber Operations and the *Jus Ad Bellum* Revisited,” 578.

[98] Goodman, “Cyber Deterrence,” 108.

[99] Schmitt, “Cyber Operations and the *Jus Ad Bellum* Revisited,” 592.

[100] Это могут быть системы управления воздушным пространством или линии связи, которые частично используются в военных целях.

[101] Schmitt, “The Law of Cyber Targeting,” 11.

или создает неконтролируемые последствия, его применение запрещено.[102] Эти ограничения не применяются к защитным мерам и к ненасильственным средствам, таким как вредоносные программы, которые не вызывают травм, повреждений или потери функциональности систем, даже если они могут распространиться на гражданские системы.[103] Если в кибератаке участвуют некомбатанты, не связанные с организованной вооруженной группой и не находящиеся под контролем государства, они могут стать целью на время, пока они принимают непосредственное участие во враждебных действиях. В киберпространстве такое участие может начаться со сбора и распространения военной разведывательной информации с помощью кибер-средств, зондирования систем противника для выявления уязвимостей или разработки программного обеспечения, предназначенного для атак.[104]

Применение сдерживания в кибердомене

При рассмотрении опыта, накопленного с основными механизмами сдерживания, и с учетом особых последствий и правовых характеристик кибердомена, становится ясно, что киберсдерживание не может применяться изолированно, но должно быть одним из жизненно важных компонентов всеобъемлющей стратегии безопасности.[105,106] В отличие от ядерных концепций, защита и устойчивость являются фундаментальной отправной точкой для лишения противника шансов на успех.[107] Помимо *воспрещения* посредством обороны, важную роль как сдерживающий фактор играет классический аспект *возмездия*, как угроза наказания. Поскольку это исследование основано на более широком понимании сдерживания, в центре внимания находятся еще два пути: сдерживание путём *обвязывания* и установление *нормативных табу*.[108]

Сдерживание воспрещением

Сосредоточение внимания на обороне становится все более важным, поскольку число потенциальных противников государства с наступательными

[102] Несмотря на это, если кибероружие является альтернативой кинетическому оружию и оказывает аналогичное воздействие на противника, его следует предпочесть, поскольку в большинстве случаев сопутствующий ущерб менее вероятен, см. Schmitt, “The Law of Cyber Targeting,” 18.

[103] Schmitt, “The Law of Cyber Targeting,” 16.

[104] Schmitt, “The Law of Cyber Targeting,” 14.

[105] Nye, “Deterrence and Dissuasion in Cyberspace,” 46.

[106] Cooper, “A New Framework for Cyber Deterrence,” 105.

[107] Carberry, “Why There’s no Silver Bullet for Cyber Deterrence.”

[108] Nye, “Deterrence and Dissuasion in Cyberspace,” 54.

кибер-возможностями постоянно растет.[109] Сдерживание посредством воспрещения направлено на повышение устойчивости и способности восстанавливаться. Таким образом, выгоды от атаки для противника могут быть уменьшены до такого уровня, что нападение станет бесполезным, а после удара можно будет гарантировать, что имеются кибер- и некибер военные ответы для возмездия. Существуют методы различной изощренности и с разными затратами,[110] но все они имеют общую цель – съедать ресурсы и время противника и нарушать его расчет предполагаемой вероятности и ценности выигрыша.[111,112] Согласно «парадигме предполагаемого прорыва», невозможно предотвратить успешное проникновение в чьи-либо сети. Но использование уязвимостей можно сделать сложным и утомительным. Тогда нападающий издает больше «шума», ему требуется больше времени, и его становится легче идентифицировать, поскольку он оставляет больше следов.

На пути к культуре устойчивости жизненно важную роль играют публично-частное партнерство (ПЧП) и обеспечение кибер страховок. ПЧП объединяют, с одной стороны, государство (как законодателя с богатыми ресурсами рабочей силы, которая ориентирована не на прибыль, а на результативность, и может полагаться на разведывательные службы) с частными лицами, ориентированными на эффективность (которые обладают большим опытом и технически специализируются в кибернетической области, где они имеют доступ к большому количеству данных и информации).[113] С другой стороны, обязательное обеспечение кибер страховок в экономике способствует повышению системной устойчивости и предотвращению того, что экономика страны может подвергнуться угрозе. Установление цены на различные частные кибер практики порождает стимул к более высоким

---

[109] The Worldwide Threat Assessment of the US Intelligence Community shows a rise from probably three states in 2007 to over 30 states in 2017. См. Daniel R. Coats, “Worldwide Threat Assessment of the US Intelligence Community” (Washington D.C.: Director of National Intelligence, February 2018), 6, https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf.

[110] Примером сложных и дорогостоящих мер является накопление резервных промышленных генераторов энергии и трансформаторов. Пример простых и дешевых мер: обучение военных астронавигации на случай потери систем глобального позиционирования. См. Nye, “Deterrence and Dissuasion in Cyberspace,” 56.

[111] Nye, “Deterrence and Dissuasion in Cyberspace,” 56.

[112] Jasper, *Strategic Cyber Deterrence*, 111.

[113] Правительство США подчеркивает этот подход в своей Стратегии национальной безопасности: «В соответствии с принципами защиты гражданских свобод и неприкосновенности частной жизни правительство США расширит сотрудничество с частным сектором, чтобы мы могли лучше обнаруживать и атрибутировать атаки». См. *National Security Strategy of the United States of America* (Washington D.C.: The White House, 2017), с. 13, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

стандартам и к соблюдению «элементарной кибергигиены» там, где противник может срывать низко висящие фрукты и быстро добиваться успеха.[114] Более того, создание отчетов и систематизирование данных, связанных с атаками, можно значительно улучшить за счет получения выгоды от комплексных центров и процессов кризисного реагирования в страховой отрасли.[115] Таким образом, информационная асимметрия между частниками и правительством может быть наконец уменьшена, время реакции может быть увеличено, и может быть обеспечена основа для создания культуры обмена информацией, основанной на доверии. Чтобы дополнительно стимулировать частно-государственное сотрудничество, необходимо внедрить «соглашения об ответственном раскрытии информации»[116] и «временные допуски».[117]

Дальнейшие отправные точки для повышения устойчивости и способности к восстановлению можно найти в самой структуре защиты. Недостаточно защитить только внешние периметры системы. Поскольку взлом возможен в любое время, существуют меры для глубокой защиты, способные обнаружить злоумышленника внутри системы, отследить, идентифицировать и побеспокоить его. Такой подход может поддерживаться сегментированными сетями и сегментированными секторами, которые не позволяют, когда злоумышленник проник внутрь, получить доступ ко всей системе. На первый взгляд, сохранение жизненно важных способностей посредством дублирования может быть дорогостоящим, но значительно снижает вероятность получения выигрыша для противника. Наконец, необходима защита цепочки поставок, чтобы избежать проникновения противника. Это

---

[114] При соответствующем обучении для повышения осведомленности пользователей можно избежать до 50 % инцидентов. См. “ENISA Threat Landscape Report 2016” (Heraklion: European Union Agency for Network and Information Security, 2017), 81, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2016/at_download/fullReport.

[115] Umar Choudhry, *Der Cyber-Versicherungsmarkt in Deutschland: Eine Einführung* (Wiesbaden: Springer, 2014).

[116] Соглашение между специалистом по поиску уязвимостей и производителем программного обеспечения о соблюдении крайнего срока публикации. Поисковик избегает риска быть ответственным за использование уязвимости, производитель получает необходимое время для анализа и исправления уязвимости, а пользователь может полагаться на тот факт, что исправления не продолжаются больше, чем необходимо. См. *Die Lage der IT-Sicherheit in Deutschland 2017* (Bonn: Bundesamt für Sicherheit in der Informationstechnik, 2017), с. 21, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf.

[117] Ограниченно по времени, связанное с конкретным делом, приостановление ограничения доступа спецслужбами для оперативной группы, чтобы обеспечить эффективный обмен информацией между агентствами и привлеченными частниками.

требует интенсивного обсуждения вопросов встроенной при проектировании безопасности с последующей проверкой производителей и поставщиков услуг и оценкой того, какие части критически важных цепочек поставок должны находиться под национальным контролем.

Сдерживание путем воспрещения – это больше, чем просто отражение кибератаки. Проводимое комплексно, оно может повысить влияние фактора времени и фактора выживания, восстановить значение фактора силы и обеспечить основу для фактора атрибуции, на основе которого становится возможным возмездие. При надлежащем коммуникировании способности защиты государства могут значительно повлиять на расчет оппонента в отношении ценности и вероятности выигрыша, а также дать правительству свободу действий для реагирования на основные угрозы в киберпространстве.[118]

Сдерживание возмездием

Ответить на нежелательное поведение наказанием – это самый известный способ сдерживания. Цель состоит в том, чтобы пообещать нанести противнику расходы, которые перевешивают выгоды, ожидаемые от первоначальной атаки.[119] Это работает только в том случае, если атака может быть атрибутирована злоумышленнику в достаточной степени, а атрибуция адресована трем вышеупомянутым аудиториям.[120] Возмездие не обязательно должно оставаться в киберпространстве, но может принимать форму дипломатических, информационных, военных и экономических действий, адаптированных к противнику и с учетом потенциальных эффектов обратной связи из-за международной взаимозависимости.[121] Кроме того, ключевую роль играет геополитическая симметрия. Месть противнику может означать инициирование серии эскалации ответных действий за пределами киберпространства, что в конечном итоге может привести к выигрышу только в том случае, если доминирование эскалации будет на одной стороне.[122]

Меры противодействия в киберсфере могут быть самыми разнообразными и находиться на различных уровнях агрессивности.[123] За пределами

---

[118] Nye, “Deterrence and Dissuasion in Cyberspace,” 56.

[119] США «… будут применять меры с быстрыми и дорогостоящими последствиями к иностранным правительствам, преступникам и других субъектам, которые предпринимают значительные злонамеренные действия в киберпространстве». См. *National Security Strategy of the United States of America*, 13; Goodman, “Cyber Deterrence,” 106.

[120] Nye, “Deterrence and Dissuasion in Cyberspace,” 51.

[121] Jasper, *Strategic Cyber Deterrence*, 13.

[122] Goodman, “Cyber Deterrence,” 109.

[123] Как предлагается в порядке возрастания в Jasper, *Strategic Cyber Deterrence*, 177:

- разрешать злоумышленникам красть фальшивые файлы или встраивать маяки, которые показывают их местоположение;

кибердомена санкции являются наиболее распространенной реакцией на нежелательное поведение, хотя в большинстве случаев они затрагивают население государства больше, чем правительство. Поэтому более эффективным оказывается инвестировать ресурсы в выявление злоумышленников и нацеливать санкции на этих лиц.[124] Даже если имя конкретного человека не может быть названо, все же возможно направить ответные меры на отношения и социальные сети, в которых участвуют злоумышленники. Это работает, поскольку все злоумышленники связаны зависимостями, и их расчет выигрыша и потерь может быть затронут косвенно. Подозреваемые группы могут быть лишены таких привилегий, как участие в финансовом сообществе, и общественное возмущение можно использовать для внутреннего давления на преступников и даже для объявления их вне закона до такой степени, что сеть повернется против них, чтобы избежать несения ущерба.[125]

Эффективное возмездие требует использования факторов времени, силы, выживания и атрибуции в качестве основы, чтобы способствовать фактору защиты. Кинетические средства оказались эффективными инструментами государства для ответа на кибератаки. В результате могут быть выбраны как обычные военные средства, так и ядерный ответ в чрезвычайно тяжелых случаях.[126]

Сдерживание обвязыванием

Современная международная система характеризуется различными зависимостями, взаимосвязями и общими уязвимостями. Сдерживание путём

- файлы-приманки с вредоносным ПО, чтобы сфотографировать злоумышленников с помощью веб-камеры;
- инфильтрация сетей злоумышленников для извлечения, изменения или удаления украденных данных;
- внедрение вредоносных программ для повреждения или программ-вымогателей для блокировки компьютеров-исполнителей;
- вставление логических бомб в файлы перед кражей, чтобы повредить компьютеры при открытии;
- использование DDoS-атак, чтобы помешать вредоносной деятельности.

[124] Президент Обама сделал именно это, подписав Указ о блокировании собственности и интересов людей, которые вмешиваются в работу ИТ-систем критически важной инфраструктур. См. Jasper, *Strategic Cyber Deterrence*, 97.

[125] Cooper, “A New Framework for Cyber Deterrence,” 114.

[126] В недавно разработанной ядерной стратегии США прямо предусмотрена возможность ядерного возмездия за разрушительные кибератаки. См. David E. Sanger and William J. Broad, “Pentagon Suggests Countering Devastating Cyberattacks with Nuclear Arms,” *The New York Times*, January 16, 2018, www.nytimes.com/2018/01/16/us/politics/pentagon-nuclear-review-cyberattack-trump.html.

обвязывания пытается поощрять ответственное поведение государства, делая упор на отдачу от сотрудничества во имя взаимных интересов.[127] Если атака имеет отрицательный сопутствующий эффект для атакующего и способствует статус-кво и его продолжению, злонамеренное взаимодействие теряет привлекательность. Связанность усиливает значение факторов выживания и глобализации, а также увеличивает восприятие противником ценности выигрыша и вероятности потерь, даже если от атаки активно не защищаются или нет страха возмездия. Эффект сдерживания зависит от сложных международных отношений сдерживания и работает лучше, когда взаимозависимость сильнее.[128]

Для усиления эффекта связанности подходящим инструментом являются меры укрепления доверия для укрепления международного мира и безопасности за счет расширения межгосударственного сотрудничества, прозрачности, предсказуемости и стабильности.[129] В киберпространстве возможными вариантами являются горячие линии связи, региональные центры связи, предварительные уведомления и соглашения о неприменении атак на конкретные цели, которые могут быть дополнены криминалистической помощью в случае ИТ-инцидентов и соглашениями о невмешательстве в работу групп реагирования на компьютерные чрезвычайные ситуации. Только установление режима контроля над кибероружием сталкивается с некоторыми трудностями. Большинство технологий, которые можно охарактеризовать как кибероружие, имеют двойное назначение (например, программы оценки уязвимости, которые могут либо найти бреши в безопасности для защиты системы, либо для ее использования), и в результате нет единого мнения о том, что такое кибер- оружие действительно.[130] Кроме того, проверка арсеналов кибероружия практически невозможна, поскольку это оружие нельзя потрогать и оно может быть легко спрятано или воссоздано после удаления.[131] Чтобы решить эту проблему, необходимо обращать внимание на «последствия», а не на «использованное оружие».[132] Кроме того, могут быть установлены нормативные табу, что является последним из четырех способов киберсдерживания.

---

[127] Jasper, *Strategic Cyber Deterrence*, 16.

[128] Китай, который выводит легитимность своей правящей партии из экономического роста, и таким образом, зависит от Интернета, гораздо больше связан с западным миром, чем довольно изолированная Северная Корея. См. Nye, “Deterrence and Dissuasion in Cyberspace,” 58.

[129] Jasper, *Strategic Cyber Deterrence*, 150.

[130] Jasper, *Strategic Cyber Deterrence*, 16.

[131] Nye, “Deterrence and Dissuasion in Cyberspace,” 60.

[132] Goodman, “Cyber Deterrence,” 116.

Сдерживание с использованием нормативных табу

При установленных строгих нормах, агрессивный субъект несет репутационные потери, которые вредят его мягкой силе, превышающие выигрыши, полученные от атаки. Если государство нарушает табу (например, использует ядерное оружие в незначительном конфликте против более слабого государства), оно сталкивается с опасностью подвергнуться остракизму со стороны международной системы. Этот эффект сдерживания работает, хотя нет активной защиты или гарантированного возмездия, но требует определенной степени достоверности атрибуции. Исторически сложилось так, что международное сообщество согласовало несколько подразумеваемых и явных норм, таких как запрет химического и биологического оружия в Женевской конвенции.[133]

В киберпространстве первым важным шагом стало принятие нормативного соглашения о применимости международного права и Устава Организации Объединенных Наций. В 2013 году «Группа правительственных экспертов ООН по развитию в области информации и телекоммуникаций в контексте международной безопасности» предложила базовые нормы, такие как выполнение международных обязательств в случае, если противоправное деяние приписывается государству, отказ от использования прокси субъектов и недопущения использования негосударственными субъектами территории государства для совершения противоправных действий.[134] Кроме того, мощной нормой для сдерживания и коммуникирования предупреждающего послания может быть использование международных трибуналов и Международного уголовного суда для преследования киберпреступников, террористов и государственных акторов.[135] Нормы, связанные с киберпространством, могут направлять поведение государства и повышать предсказуемость, доверие и стабильность в киберпространстве, а также снижать вероятность конфликта из-за неправильных восприятий. Это работает только в том случае, если нормы принимаются большинством государств и со временем институционализируются, например под эгидой ООН.[136] Нормативные табу могут в определенной степени способствовать контролю над кибероружием, даже если установить режим контроля над

[133] Хотя это табу не помешало Башару аль-Асаду использовать химическое оружие против своего населения, международная реакция (уничтожение сирийского химического оружия в 2014 году и ответные удары США в 2018 году) отразила возросшие затраты на нарушение нормативного табу. См. Nye, “Deterrence and Dissuasion in Cyberspace,” 60.

[134] Jasper, *Strategic Cyber Deterrence*, 17.

[135] Quinlan, “Deterrence and Deterrability,” 8.

[136] Jasper, *Strategic Cyber Deterrence*, 145.

кибероружием невозможно. Они должны быть направлены на табуированные результаты и цели, и таким образом, помогать различать, какое поведение терпимо, а какое подвергается остракизму.[137]

Заключение

Становится очевидным, что основные механизмы сдерживания работают во всех сферах, в том числе и в киберпространстве. Тем более, что ядерное сдерживание теряет актуальность в МО, а текущие конфликты все больше характеризуются кибер-компонентами, необходимость во всестороннем понимании киберсдерживания неоспорима. Более того, было показано, что пять основных факторов (времени, силы, выживания, глобализации, защиты) новой технологии, меняющей правила игры, такой как атомная бомба, могут быть адаптированы к киберпреступности. Кроме того, в киберпространстве решающую роль играет атрибуция, и ее необходимо добавить в обсуждение. Стало ясно, что международная система все еще находится на ранней стадии применения МП в киберпространстве и что законодательство должно пройти долгий путь, чтобы догнать технологические разработки.

Выведенные четыре способа применения сдерживания в кибербезопасности (воспрещение, возмездие, связанность и нормативные табу) обеспечивают реальный подход к интеграции аспектов киберсдерживания в стратегию кибербезопасности государства (зная, что киберсдерживание может быть только одним из столпов) общей стратегии безопасности). Однако эти способы никогда не работают изолированно, а скорее в комплексном пакете с переменным весом отдельных элементов.[138] Благодаря соблюдению основных механизмов сдерживания и адаптации их пакета к конкретным субъектам угрозы, универсальное и надежное сдерживание становится возможным.

Таким образом, высказанная в этой работе гипотеза может быть подтверждена: *даже в кибер-веке сдерживание может быть мощным инструментом государства и способствовать защите интересов национальной безопасности государства!*

Тем не менее, эффективное сдерживание не возникает само по себе. Над ним нужно осуществлять стратегический менеджмент, иначе его последствия нельзя будет контролировать. Политики и стратеги всего мира должны подготовиться к новой и требовательной эпохе сдерживания, чтобы избежать превращения лунатизма в настоящую кибервойну.

В следующей статье полученные результаты будут применены к примеру Германии. Будет объяснено, как Германия, как важный игрок во все

[137] Nye, “Deterrence and Dissuasion in Cyberspace,” 60.

[138] Например, против довольно изолированной Северной Кореи связанность не может быть основной частью стратегии, тогда как против могущественной России связанность играет гораздо большую роль, чем возмездие.

более дигитализированной международной системе, может подойти к стратегии киберсдерживания, чтобы поддержать свои интересы национальной безопасности.

Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами автора и не отражают точку зрения Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

Издание *Connections: The Quarterly Journal*, том 18, 2019 осуществляется при поддержке правительства Соединенных Штатов.

Об авторе

Мануэль Фишер – профессионал в области безопасности, работающий в оборонном секторе Германии и специализирующийся на решениях по борьбе с БПЛА. Он имеет двенадцать лет службы в немецкой армии (Бундесвере) в качестве офицера военной полиции. За это время он получил степень магистра экономики и организационных наук в Университете Федеральных вооруженных сил в Мюнхене. После службы в армии он учился в Европейском центре исследований по вопросам безопасности им. Джорджа Маршалла, где окончил магистерскую программу исследований в области международной безопасности, посвященную кибербезопасности.
E-mail: fischermanuel@web.de.