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

Мика Керттунен, *Connections QJ* 18, № 1-2 (2019): 72-80
https://doi.org/10.11610/Connections.rus.18.1-2.04

Рецензированная статья

Помимо наказания: сдерживание в цифровой сфере

Мика Керттунен

Институт киберполитики, Тарту, Эстония, https://cpi.ee/

Резюме: Теория сдерживания с момента своего появления оправдывала наращивание и поддержание арсеналов оружия, предположительно гарантируя наше выживание. Однако мы не знаем, работает ли теория сдерживания на практике: крупных войн, возможно, удалось избежать по многим другим причинам, кроме страха наказания или (другие) высоких затрат. Скептицизм в отношении киберсдерживания используется для оправдания односторонних, карательных, даже превентивных, упреждающих или постоянных действий против предполагаемых противников. Сдерживание, ориентированное на ядерное оружие, с упором на недопущение безрассудного поведения государства, могло бы быть улучшено, чтобы противостоять современным, пронизанным технологиями реалиям, где абсолютная нетерпимость к допущению ошибок или инцидентов, критически важная в сфере ядерного сдерживания, нереальна. В результате мы пришли к принятию кибероперации или отказу от них в зависимости от их целей и последствий. В качестве вклада в достижение ответственного поведения государства в киберпространстве, автор предлагает в полной мере использовать расчет затрат, лежащих в основе теории сдерживания, и включить обещание вознаграждений в наши варианты политики.

Ключевые слова: кибербезопасность, сдерживание, кибердомен, соответствие, толерантность, атрибуция.

Комфортабельная леность теории сдерживания

Можно ли сказать что-нибудь новое и значимое о сдерживании? Не обязательно начиная с Гермократа Сиракузского, любой анализ сдерживания должен, по крайней мере, отметить, что сдерживание в узком понимании

касается угрозы наказания.[1] В то же время следует отметить, что более широкое прочтение признает два аспекта сдерживания: наказание и воспрещение. Более того, уместно представить последнюю интерпретацию, специально разработанную для кибер проблем, которая добавляет аспекты связанности и нормативных табу.[2]

Интеллектуальный анализ начинается со ссылки на логику сдерживания. Во-первых, в основе лежит чисто предполагаемая логика, или закон, экономики. Рациональный актор – это расчетливое создание, которое знает, что выбрать: более низкую стоимость (Формула 1).

Стоимость соблюдения < Стоимость несоблюдения

Формула 1. Чисто экономическая логика сдерживания. (авторская компиляция)

Независимо от того, что, как предполагается, вызывает сдерживающий эффект – воздержание от мыслимого поведения: боль, неудачи, вознаграждения, накопление затрат или стыд – теория или теории предполагают, что противник агрессивен, но, несмотря на это, действует рационально, основывая свое решение на расчетах, взвешивая весь потенциал, учитывая при этом вероятные затраты и выгоды.[3] Во-вторых, не помешает упомянуть фундаментальный тезис Шеллинга о силе выбора между *ущербом и отсутствием ущерба*:

> Но для страдания нужна жертва, которая может чувствовать боль или ей есть что терять. Причинение страдания ничего не приносит и ничего не спасает напрямую; оно может только заставить людей вести себя так, чтобы избегать этого. Единственная цель ... должна заключаться в том, чтобы повлиять на чье-то поведение, заставить его принять решение или сделать выбор. Чтобы осуществлять принуждение нужно, чтобы было предчувствие насилия. И чтобы этого можно было избежать за счет подчинения. Сила причинять боль – это сила торговаться. Использовать ее – это дипломатия – зловещая дипломатия, но дипломатия.[4]

---

1 Thomas C. Schelling, *The Strategy of Conflict* (Cambridge, MA: Harvard University Press, 1960/1980); also Thomas C. Schelling, *Arms and Influence* (New Haven: Yale University Press, 1966/2008); and Paul K. Davis, "Deterrence, Influence, Cyber Attack, and Cyber War," *New York University Journal of International Law and Politics* 47, no. 2 (Winter 2014): 327-355. For Hermocrates of Syracuse, see Thucydides, trans. Martin Hammond, *The Peloponnesian War* (Oxford: Oxford University Press, 2009).

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

3 Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security* (Princeton: Princeton University Press, 1961).

4 Schelling, *Arms and Influence*, 2.

Наконец, необходимо признать ограниченность сдерживания. Теория сдерживания – и что наиболее важно, доверие к ней – предполагает сходство между навязываемыми угрозами, ценностями противника и ожидаемым рациональным поведением. Сдерживание, как основное политическое обязательство, является абсолютным, но реальный выбор и практическое применение сдерживания требует непростого выбора ценностей.[5] Сколько, например, ущерба, затрат или боли необходимо, и что представляют собой затраты, боль или стыд?

И как Другой узнает о наших возможностях и о расчетах, которые мы провели от его/ее имени? Коммуникация несовершенна, и совершенное понимание невозможно. Более того, существует асимметрия информации. Например, хотя можно с уверенностью предположить, что нападающий достаточно хорошо осведомлен о целевой киберсистеме и связанных с ней ценностях, обороняющийся не обязательно знает идентичность, стратегию или выгоды нападающего. Более того, кибер обороняющийся может быть вынужден действовать только в определенные моменты времени, в то время как кибер нападающий может активизироваться в любое время. Это демонстрирует дилемму между *дискретным временем* для одного игрока и *непрерывным временем* для другого.[6]

Что касается киберпространства, уместно отметить, что сдерживание в киберпространстве является сложной задачей или вообще не работает. Сам факт проведения злонамеренных кибероперациий установить сложно. Дополнительным фактором является скрытый, быстрый или непредсказуемый характер кибер-деятельности, которая часто осуществляется негосударственными субъектами, или отсутствие соответствующих средств или политико-правовых рамок для наказания киберпреступников.

Фактически, само утверждение о том, что сдерживание работает, не может быть проверено или опровергнуто. Сам сдерживающий эффект имеет когнитивный характер. Теория сдерживания, хотя и часто обременена расчетами, не может объяснить или предсказать какое-либо поведение; в лучшем случае, это *идеальный или гипотетический набор фактов, принципов*

---

[5] Andrew Radin, *Hybrid Warfare in the Baltics: Threats and Potential Responses* (Santa Monica, CA: RAND, 2017), 21–22, https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf; Andrew Higgins, "Two Border Cities Share Russian History – and a Sharp European Divide," *The New York Times*, November 9, 2017, https://www.nytimes.com/2017/11/09/world/europe/narva-estonia-ivangorod-russia.html.

[6] Kien C. Nguyen, Tansu Alpcan, and Tamer Basar, "Security Games with Incomplete Information," in *Proceedings of the 2009 IEEE International Conference on Communications*, 14-18 June 2009, Dresden, Germany, https://doi.org/10.1109/ICC.2009.5199443 (studying the game theory of security games and discrete time); Stefan Rass, Sandra König, and Stefan Schauer, "Defending Against Advanced Persistent Threats Using Game-Theory," *PLoS ONE* 12, no. 1 (2017), https://doi.org/10.1371/journal.pone.0168675.

или обстоятельств, или просто абстрактная мысль.[7]

Соответственно, изучение сдерживания превратилось в изучение определенных элементов, которые считаются важными в установленном каноне сдерживания. Более того, скептицизм по отношению к киберсдерживанию используется для оправдания односторонних, карательных, даже превентивных, упреждающих или постоянных действий: поскольку сдерживание не работает в киберпространстве, оно несет ответственность за принятие мер и причинение дорогостоящих последствий для предполагаемого Другого, особенно в том случае, если нет угрозы уничтожения в результате возмездия. Это убеждение основано на ограниченном понимании киберсдерживания. Несмотря на свою узкую формальную правильность, оно опасно неверно.[8]

Мы просто не знаем, действительно ли сдерживание работает или нет. Эта неопределенность вместе с фактом, утверждением или предположением о том, что с киберпространством мы вошли, по крайней мере, частично, в новую операционную среду, требует нового описания сдерживания.

Новый нарратив сдерживания: четыре утверждения

Измененный контекст

Хотя логика сдерживания может быть прослежена до общего и древнего человеческого поведения, генеалогия теории сдерживания обусловлена биполярной Холодной войной. В те годы можно было сказать, что обоюдное намерение двух сверхдержав состояло в том, чтобы обладать достаточной силой, чтобы уничтожить другую, обеспечивая при этом выживание человечества на планете. Концепция сдерживания позволяла оправдывать первое и гарантировать второе.

Ядерное оружие и способность сверхдержав уничтожить планету никуда не делись. Тем не менее, условия и контекст киберсдерживания различны. В то время как ранее сдерживание подчеркивало необходимость избегать безрассудного поведения государства, в современном кибер-дискурсе основное внимание уделяется ответственному поведению государства. Сдерживание, как мы его знаем, не кажется уместным и заслуживающим доверия.

---

[7] *Merriam-Webster English Dictionary.*

[8] Точно так же неправильно было бы некритически предполагать, что кибер-деятельность невидима, быстра и не подлежит атрибуции. Любой анализ, выходящий за рамки дорожной литературы, может выявить ощутимые последствия, месяцы и годы подготовки кибератак, а также официальную аттрибуцию государственным и негосударственным субъектам. Скорость света, а также скорость пули или истребителя – очень плохие индикаторы для определения скорости атаки, операции или кампании.

Более широкая терпимость

Кроме того, будь то в ядерной обстановке, во времена Холодной войны или сейчас, всегда преобладала культура нулевой терпимости. Неудачи в сдерживании, по крайней мере в чистом смысле, были бы неприемлемы. Ядерная или любая крупная военная атака была бы встречена ответными ударами, даже возмездием, когда все уже было бы потеряно.

В кибер-делах никто не может жить с нулевой терпимостью. Информационные и коммуникационные системы по своей природе уязвимы, подвержены техническим инцидентам или человеческим ошибкам, не говоря уже о преднамеренных атаках. Фактически, если во время Холодной войны военная конфронтация сверхдержав была допустима на глобальной периферии – в Азии, Африке и Латинской Америке, – то теперь мы имеем три уровня фактического принятия кибероперациий.

С готовностью принимаются операции, проводимые спецслужбами, органами безопасности, правоохранительными органами и вооруженными силами против общепризнанных экстремистских, террористических или преступных организаций, поскольку, например, Резолюция 1373 (2001) Совета Безопасности Организации Объединенных Наций (СБ ООН) определяет все формы терроризма как представляющие угрозу международному миру и безопасности. Поэтому международному сообществу относительно легко принять, даже приветствовать наступательные военные кибероперации США против «Исламского государства». С другой стороны, государственные кибероперации в рамках существующих бинарных конфликтов или против менее значимых целей, лицемерно или нет, условно принимаются. Например, израильские кибероперации против сирийского правительства или «Хезболлы» не вызывают международных возражений сверх обычного – в отличие от американских операций против тех же целей. Предполагаемая операция голландской разведслужбы, проникшей в системы Московского Государственного Университета,[9] не произвела никакого шума, возможно потому, что государства не хотят проблематизировать разведывательную деятельность, которую они все проводят, а может быть потому, что мишенью операции была (как утверждается) кибер-преступная группировка российского происхождения. Действия, которые воспринимаются как неприемлемые, представляют собой те операции, которые каким-нибудь образом ставят под угрозу международный порядок или национальную безопасность. Поэтому такие операции, как проникновение на серверы Национального конгресса Демократической партии в 2016 году и кража данных или попытка взлома серверов Организации по запрещению химического

[9] Rick Noack, “The Dutch Were a Secret U.S. Ally in War against Russian Hackers, Local Media Reveal,” *The Washington Post*, January 26, 2018, www.washingtonpost.com/news/worldviews/wp/2018/01/26/dutch-media-reveal-country-to-be-secret-u-s-ally-in-war-against-russian-hackers/.

оружия в 2017 году, считаются опасными и безответственными, и подверглись широкому международному осуждению.

Очевидно, такая фактическая терпимость к кибероперациям бросает вызов устоявшейся логике сдерживания: они несовместимы. Само отсутствие каких-либо серьезных кибероперациий свидетельствует скорее либо о неспособности государств, либо об их осторожности проводить такие действенные и глубокие операции в мирное время, чем о сдерживании. Тем не менее, практика кибероперациий, подвергающих проверке пороговые значения применения силы и вооруженного нападения, бросает вызов международному праву и, что самое серьезное, верховенству права, которые многие из активных операций на словах поддерживают.

Другие подходы

С концептуальной точки зрения и заимствуя из древнекитайского мышления, сдерживание наказанием является негативным подходом, а сдерживание лишением – нейтральным. Как нам говорят, первый активно стремится уменьшить ценности плохого субъекта, а второй отрицает какое-либо увеличение этих ценностей. Если расчетная логика рационального человека верна, как предполагается, то предложение вознаграждения также должно удерживать игрока от действий, которые он в противном случае предпринял бы – позитивное сдерживание: сдерживание с помощью выгод.

Такие выгоды можно создать несколькими способами. Отражая зеркально концепцию сдерживания с помощью наказания, сдерживание с помощью выгод может вознаграждать определенное поведение государств. Принимая во внимание концепцию сдерживания путем лишения, оно может включать развитие инфраструктуры, моделей сотрудничества, обмен ноу-хау или постановку плюрилатеральных, субрегиональных или других общих целей, которые используют экономические и социальные преимущества информационных и коммуникационных технологий. Выгоды также могут быть получены в контексте взаимной связанности в результате сокращения расходов и оптимизации затрат путем совместного снижения киберрисков. Кроме того, ожидаемыми выгодами могут быть улучшение репутации, рейтинг в соответствующих международных организациях или оценках, или признанное лидерство в международных процессах. В отличие от нормативных табу и инструментов нулевой терпимости, сдерживание выгодой подчеркивает максимизацию общих выгод и, следовательно, полную поддержку и всеобщее принятие/одобрение определенного поведения.

Далее выдвигается гипотеза, что классическая теория сдерживания больше не удовлетворяет в достаточной мере политические амбиции государств. Особенно в Европе существует сильная нерешительность в отношении жестких средств сдерживания, включая санкции и контрмеры, вводимые в соответствии с международным правом и особенно на его периферии. Вместо этого государства все больше интересуются экономическими и социальными стимулами, лежащими в основе поведения их контрагентов.

Ключевой критикой сдерживания наказанием является тот факт, что всякий раз, когда наказание применяется, сдерживание по определению потерпело неудачу. Соответственно, в случае получения выгод упреждающий и превентивный характер сдерживания максимизируется. Можно также утверждать, что сдерживание выгодами максимизирует взаимность и, следовательно, обещает создание максимально широкой платформы общих интересов и всеобщее принятие определенных поведенческих модальностей. Расширяя исследования по изменению вычисления злонамеренных или враждебных действий, государства могут увеличить отдачу от инвестиций в безопасность. Предполагается, что уменьшение военно-политического риска также снижает вынужденные оборонные и военные расходы, одновременно увеличивая социальный и экономический бюджет, что создает устойчивость и укрепляет информационное общество.

В свою очередь, инвестиции в обеспечение устойчивости и надлежащие методы обеспечения безопасности могут значительно увеличить стоимость плохого поведения, тем самым создав дополнительные пороги лишения. В этом контексте особое внимание уделяется устойчивости как нейтральной к действующим лицам мере.

Тонкие инструменты

Таким образом, государства или группы государств должны смотреть за рамки санкций или негативных аспектов в целом. В самом деле, мы должны признать, насколько хорошо работает устойчивость как неявное сдерживание путем лишения: количество создающих эффект кибероперациий очень мало, особенно по сравнению с киберпреступностью и расхожими разговорами о ведении кибервойны.[10] На самом деле, сам масштаб киберпреступности свидетельствует о недостаточных государственных и организационных инвестициях в потенциал, необходимый для того, чтобы помешать киберпреступникам в достижении их целей. Более того, национальная и международная политика кибербезопасности должна включать позитивные программы с вознаграждением.

Заключение

Как мы узнали, сдерживание – это громоздкий и неподходящий инструмент для понимания киберсферы. Условия киберпространства и новая генеалогия сдерживания отличаются от условий и сдерживания ядерным оружием и имеют гораздо больше нюансов.

[10] Eneken Tikk, Kristine Hovhannisyan, Mika Kerttunen, and Mirva Salminen, *Cyber Conflict Fact Book: Effect-Creating State-on-State Cyber Operations* (Jyväskylä: Cyber Policy Institute, 2019). Этот анализ основан на публично известных государственных кибероперациях, собранных Советом по международным отношениям «Cyber Operations Tracker» и другими базами данных.

Поскольку технологические, политические и социальные параметры и предпосылки различны, то и вывод тоже. Киберсдерживание, чтобы функционировать как кибернетический механизм управления поведением государства, парадоксальным образом требует принятия ошибок и инцидентов, а также атак низкой интенсивности. Это признание проводит границу между терпимым и неприемлемым. Мы, Запад, должны сделать так, чтобы стандарты ответственного поведения государств стали настолько высокими, насколько это возможно. Наше стремление использовать наше технологическое превосходство и проводить кибероперации не должно подрывать верховенство закона и более высокие моральные принципы. Поскольку сдерживание субъекта как теоретически сомнительно, так и практически невозможно в киберсфере, санкции всех видов призваны создать государственную практику и установить границы ответственного / безответственного поведения государств.

Менеджмент новой обстановки неопределенности, размытых линий ответственности, множества пороговых значений и множества действующих лиц не может полагаться исключительно на черно-белую логику негатива, то есть наказания. Устойчивость должна заменить в нашем стратегическом лексиконе балансирование на грани наказания и предостережения. Надежная (национальная) устойчивость, как нейтральная к угрозам и приводящая к деэскалации, также лучше подходит для условий непредсказуемости, качество, которое более актуально для кибер-контекста, чем сдерживание или постоянное взаимодействие в этом отношении. Успех подходов, основанных на доминирующем риске и угрозе (со стороны субъекта), или одновременном сдерживании и постоянном взаимодействии, обусловленных точностью (предварительных) оценок, сам по себе слишком рискован.[11] Запад должен стимулировать ответственное поведение в киберпространстве. Устойчивость и вознаграждение вместе создают мощный и мирный вариант политики, который не может предложить ни одно другое государство или группа государств.

Таким образом, в новой формуле сдерживания (формула 2 ниже) по-прежнему действует закон экономики, но затраты заменяются вознаграждением.

---

[11] Gerard de Vries, Imrat Verhoeven, and Martin Boeckhout, “Governing a Vulnerable Society: Toward a Precaution-Based Approach,” in *Vulnerability in Technological Cultures: New Directions in Research and Governance*, ed. Anique Hommels, Jessica Mesman, and Wiebe E. Bijker (Cambridge, MA: MIT Press, 2014), 225. Упомянутая глава основана на докладе «Ненадежная безопасность», который Голландский научный совет по правительственной политике (WRR) принял в качестве официальной рекомендации голландскому правительству. Управление рисками, принятое или по крайней мере упомянутое во многих национальных стратегиях кибербезопасности, направлено на выявление и оценку рисков с точки зрения вероятности и степени ущерба и проектирования, а также принятие мер по ограничению или контролю тех рисков, которые считаются неприемлемыми.

Награды за соблюдение требований > Награды за несоблюдение

Формула 2. Новая экономическая логика сдерживания.
(компиляция автора)

Этот поворот не предполагает почти автоматической воинственности Другого. Таким образом, мы избегаем иллюзии сдерживания Другого в ситуации, когда считается, что такая воинственность не обязательно имеет место. Вместо этого мы сосредотачиваемся на более вероятной мотивации и амбициях правительств – положительном вознаграждении. Очевидно, что лидер, решившийся пойти на войну, не будет разубежден угрозой наказания, ожидаемыми трудностями или благосклонным вознаграждением.

Такой поворот мышления не будет оценен по достоинству оборонным киберпромышленным комплексом, который оправдывает свое существование угрозой и перспективами апокалиптического будущего. Для остального человечества, предпочитающего мир, процветание и глобальную справедливость, такой поворот имел бы смысл.

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

Подполковник (в отставке, финские сухопутные силы) **Мика Керттунен**, доктор социологических наук (пол.), Директор по исследованиям Института киберполитики (Тарту, Эстония). Он окончил Финскую военную академию и курс офицеров Генерального штаба, а также Королевский норвежский командно-штабной колледж. Керттунен изучал мировую политику в Университете Хельсинки, и в своей диссертации 2009 года проанализировал внешнюю и ядерную политику Индии. После службы в армии он сосредоточил внимание на кибер-проблемах внешней политики и политики безопасности, разработке кибер-норм, а также разработке национальных стратегий кибербезопасности и военных кибер-доктрин. Д-р Керттунен является советником финской делегации в Группе правительственных экспертов ООН по информационной безопасности (2016-2017) и приглашенным преподавателем юридического факультета Тартуского университета.