УДК 004.056

Савченко В.А.

СДЕРЖИВАНИЕ В КИБЕРПРОСТРАНСТВЕ

В докладе рассмотрены вопросы сдерживания в киберпространстве, как одного из ключевых элементов информационной безопасности государства. Проанализированы сходство и различия сдерживания в ядерной сфере и киберпространстве. Сделаны выводы относительно возможности реализации идеи сдерживания в сфере информационных технологий.

***Ключевые слова*:** киберпространство, кибератака, киберзащита, сдерживание

События последних лет, информационные войны и кибератаки, которые в полной мере зацепили и нашу страну, демонстрируют необходимость поиска эффективных механизмов защиты государства и его критической инфраструктуры. В этом аспекте вспоминается опыт относительно недавнего прошлого, когда мы жили в биполярном мире с двумя ключевыми игроками. При этом мирное состояние поддерживалось благодаря эффекту сдерживания силы.

Как известно, человек мыслит аналогиями и потому вполне резонно возникает вопрос: «А можно ли перенести идеи и механизмы сдерживания на киберпространство?».

Для ответа на этот вопрос нужно рассмотреть следующие положения:

- общая концепция сдерживания;
- параллели и отличия между ядерным и киберсдерживанием;
- проблемы сдерживания в киберпространстве;
- как обеспечить сдерживание в киберпространстве?;
- сдерживание в междоменных областях.

Если полистать толковые словари, то можно найти следующее определение сдерживания: «Процесс и/или результат переубеждения кого-либо с целью изменения его мнения или отказа от достижения поставленной цели». Таким образом, целью сдерживания является изменение конечного состояния объекта или его отказ от достижения поставленной цели.

Сдерживание является ключевым элементом любой модели безопасности и на протяжении многих веков остается мощным инструментом государства осуществлять его власть. Составляющими частями сдерживания являются две субмодели – упреждения и возмездия. В первом случае злоумышленник должен воспринимать потенциальные значительные трудности в достижении своей цели (материальные, финансовые, технологические или социальные – через человеческие жизни). Во втором случае сдерживание базируется на страхе от ответных действий состороны жертвы.

Таким образом, сдерживание базируется на трех основных китах, к которым относятся:

наличие средств влияния (вооружение, ресурсы и т.д.);

возможность реакции (разведка, системы контроля и управления);

желание реакции (внутренняя и внешняя политическая ситуация).

Сдерживание реализуется путем соответствующего информационного влияния. Именно информация о наличии у вас сил, возможностей и решительности реализовать эти возможности заставит противника изменить свои намерения или отказаться от достижения цели.

В таком случае возникает соблазн выдать желаемое за действительное и потому в этом отношении нужно быть предельно осторожным. В любом случае – желательно чтобы ваши заявления совпадали с вашими возможностями.

Как уже отмечалось, существует некоторая схожесть между вооруженным (в т.ч ядерным) и киберсдерживанием. Но существует ли в действительности такая параллель? Давайте попытаемся ответить на этот вопрос.

Первые упоминания о проблеме защиты киберпространства появились примерно 15-20 лет назад в официальных докладах администрации США после громких скандалов, связанных с потерей информации различных силовых структур. В последствии тональность различных заявлений американских президентов и других членов правительства только усиливалась.

В 2013 году госсекретарь США Джон Керри назвал Кибероружие эквивалентом ядерного оружия 21 века. Сегодня уже практически не существует политика, лидера государства или представителя бизнеса, который не обращался бы к теме кибербезопасности. Некоторые из них предлагают построить модель всеобщей безопасности на идеях сдерживания в киберпространстве по аналогии с ядерным сдерживанием в период холодной войны.

Но давайте рассмотрим так называемый вихрь эскалации войны (рис. 1). В этом вихре различным видам вооружения соответствуют уровни разрушения. Чем больше уровень разрушения, тем больше влияние оказываетсяна противника.

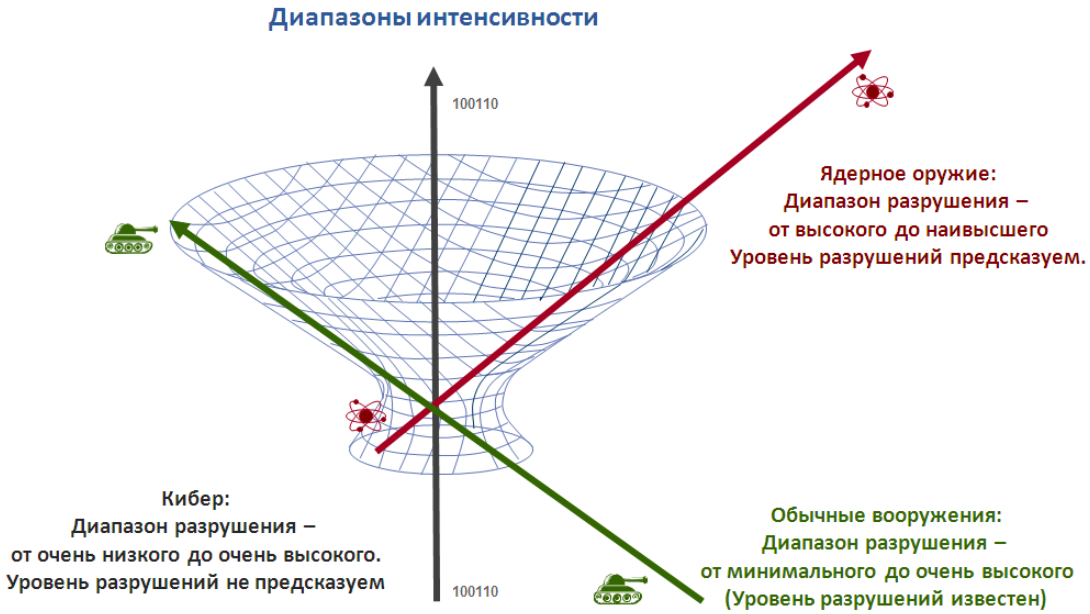

Рис. 1. Вихрь эскалации войны

Обычные вооружения имеют уровень разрушения от минимального до очень высокого (например в случае высокоточного вооружения большой мощности). При этом уровень разрушений практически всегда предсказуем.

Ядерное оружие имеет уровень разрушения от высокого до наивысшего. Уровень разрушений предсказуем а сами вооружения достаточно хорошо контролируются.

В киберпространстве все не так однозначно. Диапазон разрушений изменяется от очень низких до очень высоких – и это не тайна. Вместе с тем, очень сложным является процесс предсказания этого уровня.

Таким образом есть две основных параллели между ядерным и киберсдерживанием. Обе они базируются на общих характеристиках ядерной и кибервойны. Осознание сторонами значительного возможного материального ущерба или даже взаимоуничтожения сдерживает стороны от активных действий.

На этом, пожалуй, сходство между ядерным и киберсдерживанием заканчивается. В чем же заключаются различия между различными видами сдерживания?

Если в ядерной войне диапазон градаций акций достаточно узок, то в кибервойне он практически безграничен.

В ядерной сфере нормальной ситуацией является отсутствие какой-либо активности а действия основных актеров весьма прозрачны. Число самих актеров весьма ограничено а определение атаки практически всегда однозначно. В то же время в киберпространстве даже в спокойном состоянии происходит огромная активность. При этом действия актеров трудноопределимы и непрозрачны. Авторство многих атак остается неизвестным. Киберпространство дает возможность реализовать схему ассиметричных действий, когда на любое влияние может последовать неадекватно мощный ответный удар.

Стоимость развития ядерных вооружений огромна, в то время, как стоимость реализации кибератак достаточно низка.

В ядерной сфере достаточно просто демонстрировать силу (если у вас есть ядерное оружие). В то же время в сфере кибервооружений продемонстрировать силу весьма сложно. Большинство атак имеют одноразовый характер.

Таким образом рассмотренное выше дает возможность сделать первые выводы:

Кибервойна позволяет осуществлять влияние на противника сравнимое с тем, что может бать получено с применением ядерних средств или обычных вооружений большой мощности/точности.

Модель ядерного сдерживания не может быть в точности применена в киберпространстве.

Какие же существуют проблемы сдерживания в киберпространстве?

Основная проблема – организация эффективной защиты. Причем эти трудности возрастают экспоненциально из-за роста количества уязвимостей, средств нападения и сложности систем, которые подлежат защите. Создание вредоносного программного обеспечения требует в среднем нескольких десятков строчек кода в то время как создание самих приложений и средств их защиты – тысяч и, часто, миллионов строк.

Если войны в большинстве доменов ведутся государствами а их осуществление ограничивается применением воинских формирований, то в виртуальном пространстве существует много разновидностей оружия, которые могут быть одинаково эффективными.

Основными действующими лицами этого театра военных действий могут быть и тинэйджеры, и профессиональные хакеры и правительственные структуры.

Ввиду непредсказуемости последствий, как правило, даже государственные структуры не брезгуют помощью хакеров и киберкриминальных элементов.

Одно и то же действие в киберпространстве может быть классифицировано как киберпреступление, кибертерроризм или кибервойна в зависимости от обстоятельств, мотивации и взаимодействующих актеров.

Среди мотивов главенствующую роль на сегодняшний день занимают киберпреступления. В то же время киберпространство является благодатным полем для разведывательной деятельности, шпионажа и других видов атак.

Более того, в то время как в сфере военногопротивостояния активность ограничивается лимитированным числом конфликтов, эволюцию которых можно постоянно отслеживать, в виртуальном пространстве существует непрекращаемая высокая активность, часто – без какого либо контроля.

На этом слайде показаны DDoS атаки, осуществляемые ботнетами. При этом в атаках берут участие десятки тысяч машин, разбросанных по всему миру, владельцы которых даже не подозревают об их существовании.

Определение авторства таких атак сегодня практически невозможно. Анонимность достигается сравнительно легко даже при ограниченных финансовых ресурсах.

Еще одной проблемой является возможность влияния на третью сторону. Мы помним атаку прошлого года вирусом WannaCry, целью которой, по одной из версий, была инфраструктура стран восточной Европы. Но, при этом, больше всего пострадала медицинская система Великобритании, которая массово использовала уже не поддерживаемую, но все еще популярную операционную систему WindowsXP.

Таким образом, в глобализированном взаимосвязанном мире очень сложно будет добиться точечности и адресности атаки. Неизбежно будут страдать и непричастные акторы.

Все это усиливается следующей проблемой, которая поддерживает высокую криминализацию киберпространства – безнаказанностью. Недооценка правительствами необходимости защиты привела к тому, что уже появилось целое поколение людей, живущих по принципу «Все что происходит в Вегасе остается в Вегасе».

На сегодняшний день законодательство большинства стран мира не приспособлено к новым реалиям. Требуют законодательного определения многие термины, привычные нам в реальном мире.

Что такое вооруженное нападение в киберпространстве?

Когда правомерно применять право на самооборону?

Существует много попыток перевода этих терминов в виртуальную реальность, но пока еще мало практических результатов.

В связи с этим очень сложно определить момент применения силы с целью самообороны против кибератак. Кроме того, определение этого порога само по себе установит границу, которую легко будет нарушить.

Следующей проблемой является проблема демонстрации силы. В ядерной войне для этого достаточно провести хотя бы одно успешное испытание. Но все не так просто в киберпространстве. Кибероружие является одноразовым. И, применив его один раз, невозможно будет воспользоваться им снова.

Таким образом мы можем сделать следующие выводы.

Сдерживание в киберпространстве методом упреждения – неприменимо.

Сдерживание через возможность возмездия – утопия!

Возникает вопрос: Как же обеспечить сдерживание в киберпространстве?

Одно из направлений – повышение обороноспособности страны в киберпространстве. Для этого предлагается реализация 10 необходимых шагов:

1. Анализ рисков.
2. Распределение ответственности за защиту.
3. Обеспечение физической безопасности.
4. Постоянная защита информации.
5. Безопасность мобильных устройств.
6. Защита от вредоносных программ.
7. Своевременные обновления и внесение изменений.
8. Обеспечение безопасности сетей.
9. Постоянный мониторинг активности.
10. Эффективное управление защитой.

Второе направление – поиск и наказание преступников. Очень важно обеспечить неотвратимость наказания за совершенные неправомерные действия в киберпространстве.

В этой связи необходимым условием является наличие серьезных возможностей по проведению цифровых судебных экспертиз, которые позволили бы определять авторство атак, которые будут содействовать сдерживанию путем возмездия.

Немаловажным также является сотрудничество: как международное так и национальное. Направления такого сотрудничества – информирование об угрозах, расследование инцидентов, обучение, повышение осведомленности, наука и т.д.

Еще одним аспектом сдерживания есть укрепление правовых основ. Эти правовые нормы могут действительно повлиять на сдерживание. В этом аспекте весьма продуктивными являются Таллинское руководство и Будапештская конвенция. Но еще предстоит принять не один правовой акт для формирования полноценной модели управления в киберпространстве.

Всвязи с этим логичным будет следующий вывод:

*Эффективное сдерживание в киберпространстве требует мультидисциплинарного подхода, который охватывает сферу обеспечения оборонных возможностей, атрибуции атак, правового регулирования, контроля и сотрудничества в киберпространстве***.**

Остался еще один нерассмотреный вопрос, а именно – сдерживание в междоменных областях. До сих пор мы рассматривали лишь сценарий, когда и агрессия и ответ осуществлялись лишь в киберпространстве. Но ведь ответные действия не обязательно должны проводиться в то й же области, что и нападение. Теоретически, на авиаудар можно ответить достаточно мощнойкибератакой.

Можно достаточно долго моделировать поведение противников в такой игре. Вместе с тем, победу одержит тот, кто нанесет противнику больший ущерб. Таким образом – не важно, в какой сфере удар, главное – ущерб. Естественно, более целесообразно осуществлять действия там, где затраты будут минимальны.

В связи с этим еще несколько заключительных положений:

Формы и способы ведения обычной войны мало применимы в киберпространстве.

Мощные наступательные возможности в киберпространстве могут сдержать противника от проведения наступательных действий в других областях.

Правительство и население предпочтут реализовать наступательные возможности в киберпространстве, чем в сфере обычных вооружений.

И, как общий вывод, необходимо отметить:

Мощное государство не может быть слабым в киберпространстве.

Список использованной литературы:

1. Martin C. Libicki. Cyberdeterrence and cyberwar. (2009).
2. MAJ Lee Hsiang Wei. The Challenges of Cyber Deterrence. (2015).
3. Tang Lan, Zhang Xin, Harry D. Raduege, Jr., Dmitry I. Grigoriev, Pavan Duggal y Stein Schjølberg. Global Cyber Deterrence. Views from China, the U.S., Russia, India, and Norway. (2016).
4. Joshua Tromp. Law of Armed Conflict, Attribution, and the Challenges of Deterring Cyber-attacks. (2010).
5. James A. Lewis. Cross-Domain Deterrence and Credible Threats. (2010).
6. Annegret Bendiek, Tobias Metzger. Deterrence theory in the cyber-century. (2015).
7. Michael Chertoff & Frank J. Cilluffo. Choosing to lead. American Foreign Policy for a Disordered World. Chapter 20: A strategy of cyber deterrence. (2015).
8. Keneth Geers. The Challenge of Cyber Attack Deterrence. Computer Law & Security Review, 26(3), pp. 298-303. (2010).
9. Patrick Cirenza. The flawed analogy between nuclear and cyber deterrence. (2016).
10. Rhea Siers. The Myth of Cyber Deterrence. (2016).

Надійшла: 5.05.2018 Рецензент: к.т.н. Довбешко С.В.