«ВЗАИМНОЕ ГАРАНТИРОВАННОЕ УНИЧТОЖЕНИЕ» (ВГУ)

Умурбаев Рустам Шакиржанович
Студент 4-го курса Ташкентского государственного университета востоковедения город Ташкент
urustam316@gmail.com
+998946995982

Аннотация. *Появление ядерного оружия коренным образом изменило ход военных действий. Во время холодной войны между Соединенными Штатами и Советским Союзом, обе стороны разработали достаточно ядерного оружия, чтобы многократно уничтожить друг друга. Каждая сторона воспринимала другую как «разумного оппонента», чье поведение определялось «угрозами ядерного возмездия» с ее стороны. Каждая сторона полагалась на то, что другая сторона заботится о собственном выживании и не предпринимает действий, которые привели бы к ее собственному уничтожению в результате ядерного возмездия. Несмотря на то, что имели место некоторые вторичные и опосредованные конфликты, ни одна из сторон не могла рискнуть применить ядерное оружие из-за ожидаемого ответа. Модель «стратегической биполярности», которая определяла холодную войну, больше не отражает состояние мира с точки зрения физического конфликта.*

Ключевые слова: *конкретный конфликт, холодная война, ядерные ракеты, существенный.*

ВВЕДЕНИЕ

Доктрина взаимного гарантированного уничтожения (ВГУ) предполагает, что каждая сторона обладает достаточным количеством ядерного оружия, чтобы уничтожить другую сторону; и что любая из сторон, в случае нападения другой стороны по какой-либо причине, обязательно нанесет ответный удар с равной или большей силой. Ожидаемым результатом является немедленная необратимая эскалация боевых действий, приводящая к взаимному, полному и гарантированному уничтожению обеих воюющих сторон. Далее, доктрина предполагает, что ни одна из сторон не осмелится нанести первый удар, потому что другая сторона нанесет его по предупреждению (также называемому «смертельно опасным») или с привлечением вспомогательных сил («второй удар»), что приведет к уничтожению обеих сторон. Ожидается, что результатом доктрины ВГУ станет напряженный, но стабильный мир во всем мире.

Основное применение этой доктрины началось во время холодной войны (1940-1990), в ходе которой ВГУ рассматривалась как средство предотвращения любых прямых полномасштабных конфликтов между Соединенными Штатами и Советским Союзом, в то время как они вели небольшие войны чужими руками по всему миру.

Это также привело к гонке вооружений, поскольку обе страны изо всех сил пытались сохранить ядерный паритет или, по крайней мере, сохранить способность нанести ответный удар. Хотя холодная война закончилась в начале 1990-х годов, доктрина взаимного гарантированного уничтожения, безусловно, продолжает действовать. Сторонники ВГУ как части стратегической доктрины США и СССР полагали, что ядерную войну лучше всего предотвратить, если ни одна из сторон не сможет рассчитывать на то, что переживет полномасштабный обмен ядерными ударами как дееспособное государство. Поскольку достоверность угрозы имеет решающее значение для такой уверенности, каждая сторона должна была вложить значительный капитал в свои ядерные арсеналы, даже если они не были предназначены для использования. Кроме того, нельзя было ожидать, что ни одна из сторон не сможет должным образом защитить себя от ядерных ракет другой стороны. Это привело как к ужесточению, так и к диверсификации систем доставки ядерного оружия.

МАТЕРИАЛ И МЕТОДЫ

В киберпространстве может не быть четкой границы между миром и войной, поскольку разные государства по-разному определяют, что является военным актом или деятельностью в военное время, если у них вообще есть такая политика. Кроме того, тот факт, что одно и то же оружие может оказывать столь сильно различающееся воздействие, может привести к эскалации до кошмарных сценариев с широкомасштабными последствиями.

Концепция ВГУ применялась к кибервойнам в нескольких предыдущих исследованиях. В разделе «Кибервойна» сама кибервойна описывалась как война, включающая «кибербезопасность, операции в компьютерных сетях, электронную войну или все, что связано с сетью». Оно было определено как включающее действия, которые атакуют электронные носители и защищают их, а также атаки и средства защиты с использованием этих средств. Неэлектронные действия, связанные с вышеизложенным, также по своей сути включены. Морган, Филбин, Най, Бендиек и Мецгер предлагают адаптировать подходы к сдерживанию ядерной эры, основанные на ВГУ, к киберпространству. Лонсдейл предлагает, в частности, использовать подход, основанный на ведении боевых действий, при котором (в рамках ядерного сдерживания) ядерное оружие рассматривалось не как комплексное средство сдерживания, а скорее, как часть более широкой стратегии, призванной обеспечить возможности сдерживания и пост-отказного сдерживания. Кросстон, в свою очередь, предлагает концепцию «взаимно гарантированного ослабления», признавая, что кибератаки могут не разрушать (как это сделал бы немедленный ядерный взрыв), но могут быть катастрофически разрушительными для городов, стран и их экономики.

РЕЗУЛЬТАТЫ

Ридо предлагает более детальную стратегию, добавляющую концепции защиты и жизнестойкости к концепции сдерживания, основанной на рекламе. Другие разработчики также изучили и развили эту концепцию. Чуквуди, Удока и Чарльз

рассматривают применение теории игр к сдерживанию. Дэвис рассматривает вопрос об эскалации и ступенях эскалации в киберпространстве. Гирс предполагает, что сдерживание может оказаться «невыполнимой задачей» из-за проблем асимметрии и необходимости определения причин нападения, в то время как Гейл и Мокаррам обсуждают использование ВГУ и сдерживание в стратегии Соединенных Штатов и европейской стратегии, соответственно. Хьюстон оценивает факторы, которые могут повлиять на использование технологий Дж. Страуба в гражданской войне, и те, которые могут привести к сдерживанию гражданского населения.

В этом разделе рассматриваются методы рекламы в киберпространстве и методы противодействия рекламе. В нем также рассматриваются методы, не связанные с рекламой, которые могут быть использованы для противодействия рекламным методам в киберпространстве. Кибервойна может использоваться для реализации нескольких различных методов рекламы. Операции в киберпространстве могут служить средством получения информации и оказания влияния, как обсуждалось в предыдущих разделах. С человеком можно связаться, принудить или убедить его по электронным каналам совершить действие, которое приведет к значительным разрушениям. Это может быть целенаправленный контакт или реализация угрозы, или вознаграждения в киберпространстве, адресованной конкретному лицу. Операции в киберпространстве также могут быть использованы более непосредственно. Они могут быть использованы для компрометации ядерного оружия или другой системы, которая может непосредственно привести к значительным разрушениям, и для электронного управления ими. Атака или выход из строя электронных систем также может быть использована для нанесения немедленного или долговременного ущерба, препятствуя передаче данных или другим процессам, необходимым для поддержания жизнедеятельности.

ОБСУЖДЕНИЕ

Представленные модели предоставляют удобный способ описания и перспективу, с которой можно подходить к оценке сценариев ВГУ и сравнению рекламных возможностей отдельных злоумышленников в одной среде или в нескольких средах. Они также поддерживают сценарии, в которых существуют два сильных альянса, и сценарии, в которых существует более двух противников, включая сценарии со слабыми и меняющимися альянсами. Однако, как и у любой модели, их самая большая слабость заключается в том, что они полагаются на правильную совокупность информации, а специалисты по планированию и лица, принимающие решения, которые используют модели, имеют доступ ко всей необходимой информации. Внутренний контроль может затруднить использование удобных возможностей. Союзники могут также не раскрывать в полной мере свои возможности. С другой стороны, проблемы «тумана войны» могут привести к значительному завышению или занижению оценок возможностей противника и североатлантического союза. Раскрытие возможностей противника в соответствии с

договорами или другими обязательствами и содействие инспекциям объектов также могут вызывать подозрения и быть предметом манипуляций.

Учитывая, что как у противников, так и у союзников могут быть причины предоставлять неверную информацию о возможностях, было бы крайне желательно проверить эти утверждения. Однако, поскольку кибервозможности могут быть разработаны без необходимости в наглядных демонстрациях и тестировании, может возникнуть значительный потенциал для искажения информации. Даже те действия, которые обнаруживаются, могут быть проблематичными из-за проблем с атрибуцией. Недостаток информации может быть, как полезным, так и проблематичным. Это выгодно, потому что создает предел погрешности, позволяя двум сторонам обладать возможностями, более различными, чем это могло бы быть приемлемо в противном случае, чтобы одна из сторон не почувствовала, что у нее есть преимущество, и не атаковала. С другой стороны, существенного неверного прогнозирования возможностей противника может быть достаточно для создания такого же сценария, когда одна из сторон считает («ошибочно»), что в ее интересах атаковать в данный момент.

ЗАКЛЮЧЕНИЕ

В данной статье была рассмотрена дилемма, связанная с существованием множества рекламных технологий, которые отличаются масштабами, оперативностью, долгосрочным воздействием и методами воздействия. В частности, в нем рассматривалось, как сценарии ВГУ могут разыгрываться в нескольких доменах и средах и как сценарий ВГУ может быть создан с использованием рекламных технологий из разных доменов и различных возможностей, которые удовлетворительно сочетаются, чтобы уравновесить собственные возможности злоумышленника. Кроме того, в этом документе представлены модели для сценариев с одним доменом, двумя противниками, а также для расширенных сценариев, в которых задействовано несколько доменов, несколько противников и у противников есть множество возможностей в некоторых или во всех доменах. В нем описано, как эти модели могут быть использованы для оценки, обсуждения и презентации работы по анализу ВГУ. В нем также обсуждаются ограничения, накладываемые на модели, в основном из-за их зависимости от участия человека. Будущая работа будет включать рассмотрение вопроса о включении в модели негосударственных субъектов, которые обладают некоторыми возможностями ГУ и могут учитывать сценарии ВГУ как в настоящее время, так и в будущем. Разработка модели, учитывающей вопросы атрибуции и анонимности, включая преднамеренные операции «под чужим флагом», является еще одним ключевым направлением будущей работы. Также планируется дальнейшая оценка предложенной здесь модели путем ее применения к соответствующим сценариям.

ПОДТВЕРЖДЕНИЕ

Учитывая вышеизложенное, можно сделать вывод, что модели обеспечивают основу для рассмотрения сценариев ВГУ, а также номенклатуру и систему представления для них. Они не могут гарантировать, что сравнительные расчеты возможностей ГУ и ВГУ верны в любом конкретном конфликте. Качество, полнота и точность информации, вводимой в модели, абсолютно необходимы для обеспечения того, чтобы полученный ответ был пригоден для принятия решений.

СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Curtis, W. The assured vulnerability paradigm: can it provide a useful basis for deterrence in a world of strategic multi-polarity? 16 (3) (2000), pp. 239-256.

2. Salehyan, I. The delegation of war to rebel organizations. Confl. Resolut., 54 (3) (Jun. 2010), pp. 493-515.

3. Andre, V. The janus face of new media propaganda: the case of Patani neojihadist YouTube warfare and its islamophobic effect on cyber-actors Islamic-Christian Relations, 25 (3) (Jul. 2014), pp. 335-356.

4. Forest, J. Perception challenges faced by Al-Qaeda on the battlefield of influence warfare on JSTOR Perspect. Terror., 6 (1) (2012), pp. 8-22.