Сдерживание и эскалация в междоменных операциях: где смыкаются космос и киберпространство?

Винсент Манзо

аналитик Центра стратегических исследований Института Национальных Стратегических Исследований Национального Университета Обороны США

Война стала еще более сложной с тех пор, как Ричард Смоук дал ей описание эскалации в 1977 г. Национальная Стратегия Космической Безопасности США описывает космос как «перегруженное, оспариваемое и конкурентоспособное пространство», пока спутники лежат в основе военной и экономической власти США. Деятельность в киберпространстве пронизывает каждый аспект человеческой деятельности, в том числе военные операции США, но перспективы эффективной киберзащиты не внушают оптимизма. Многие другие акторы тоже зависят от постоянного доступа в эти области, но не так сильно, как в Соединенных Штатах.

По этой причине некоторые аналитики утверждают, что Китай первым даст залп в конфликте с Соединенными Штатами, который будет разворачиваться в космосе и киберпространстве. В наихудшем случае по оценкам возможных сценариев можно сделать вывод, что такая атака может сделать Соединенные Штаты слепыми, глухими и немыми, и почти исключительно через некинетические средства, хотя неясно, насколько эффективны атаки в космосе и киберпространстве будут в реальном военном конфликте. Как такие понятия, как эскалация, сдерживание и пропорциональность применяются в таком контексте? Что за «случайные протуберанцы» могли бы создать противодействие в космосе и привести к эскалации кибератак? Что является критическим порогом для атак в междоменных операциях? И что именно означает междоменный? Эта статья исследует эти вопросы, используя иллюстративный пример гипотетического американо-китайского конфликта, потому что обе страны обладают различными стратегическими возможностями, которые охватывают воздух, землю, море, космос и киберпространство.

Определение междоменной зоны: платформы или эффекты?

Междомен - неоднозначный термин. Доктрина США идентифицирует землю, воздух и море как домены. Последние документы США в области политики и стратегии безопасности также признают космос и киберпространство как

домены.[1] Предполагая, что все пять являются стратегическими доменами, есть, по крайней мере, два различных способа действия, которые могут пересекать домены. Междомен может быть определен в соответствии с платформой, с которой актор начинает атаку и платформой, на которой находится цель. Уничтожение спутника с помощью противоспутниковой системы наземного базирования является междоменным, тогда как уничтожение его с орбитальной системы (например, маневренным спутником) таким не является. Удар по кораблю крылатой ракетой с воздуха представляет собой междоменное нападение, в то время как нападения на ту же цель крылатой ракетой с корабля — нет. Определение междомена по платформам показывает, что междоменные операции не новы. Воздушные атаки на военно-морские силы, военно-морские нападения на воздушные силы, а также атаки с обеих доменов на сухопутные войска широко распространены в современной войне. На самом деле, во многих случаях междоменная операция может быть просто наиболее целесообразным вариантом. Как, например, нация, атакуемая ракетами с кораблей, может иметь множество причин атаковать военно-морские активы противника быстрее самолетами, а не подводными лодками и надводными кораблями.

Это определение может быть слишком упрощенным. Большинство вооруженных сил США на суше, в воздухе и на море используют кибер и космические активы, и самые сложные миссии интегрируют участие нескольких доменов. Можно даже утверждать, что точность обычного удара является междоменной атакой, независимо от того, находится ли платформа атакующего и цель в одном и том же домене, если он использует спутники и компьютерные сети. По тем же соображениям, характеристика кибератаки (в противоположность кибер эксплуатации) против американских военных компьютерных сетей как однодоменной, вводит в заблуждение. В случае успеха такая атака будет иметь важные междоменные эффекты: это подорвет воздушные, наземные, или военно-морские силы, которые зависят от деградированных компьютерных сетей. Эти косвенные эффекты в других областях часто являются основной целью кибератак.[2] Та же логика применима к атаке с орбитальных противоспутниковых систем; даже если платформы находятся в той же области, то эффекты будут междоменными. Таким

[1] См. Department of Defense (DOD), Quadrennial Defense Review Report (Washington, DC: DOD, February 2010), 33–34, 37–39; The White House, National Security Strategy (Washington, DC: The White House, May 2010), 22; DOD, National Security Space Strategy (Washington, DC: DOD, January 2011); The White House, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World (Washington, [D]C: The White House, May 2011); DOD, Department of Defense Strategy for Operating in Cyberspace ([W]ashington, DC: DOD, July 2011).

[2] В докладе Национального исследовательского совета 2009 г. кибератаки определяются как умышленные действия, которые «изменяют, нарушают, деградируют или уничтожают компьютерные системы или сети или информацию и/или программы». См.: National Research Council, Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack CapabilitiesWashington, DC: National Academies Press, 2009, P. 80.

образом, междомен также может быть определен в соответствии с последствиями операции. Согласно этому подходу нападение является междоменным, если его последствия предназначены для разворачивания в другом домене, чем цель атаки. Это определение показывает, что отношения между доменами (нашим и нашего противника) создают стратегические уязвимости.[1] Например, обычные операции США по нанесению точных ударов зависят от доступа к нескольким доменам. Потенциальный противник мог бы оказаться неспособным уничтожить самолеты или атомные подводные лодки США, но он может быть в состоянии напасть на космические и кибер активы, которые позволяют этим платформам уничтожать цели. Эта логика, кажется, лежит в основе интересов Китая к контрпространству и кибератаке: такие нападения сдвигают конфликт в домены, где наступательные вооруженные силы Китая имеют преимущество перед обороной США, тем самым изменяя потенциал США в областях (например, воздушной и морской), где Китай мог бы быть поставлен в невыгодное положение.[2] Этот междоменный подход будет неэффективным, если воздушные, морские, и наземные силы США не будут зависеть в большой степени от космоса и кибератривов. Без этого связующего элемента Китай не смог бы перевести уязвимость США в космосе и киберпространстве в оперативное воздействие на другие области. Междоменные атаки, таким образом, позволяют актору наилучшим образом использовать свои сильные стороны и использовать уязвимости противника в некоторых случаях. Данные о том, что Соединенные Штаты осуществили кибератаки в начале операции НАТО в Ливии, предполагают, что американские военные также воспринимают междоменные атаки как полезные для эксплуатации уязвимостей противника.[3]

[1] См. Mark E. Redden and Michael P.Hughes, Global Commons and Domain Interrelationships: Time for a New Conceptual Framework? INSS Strategic Forum 259 (Washington, DC: National Defense University Press, October 2010).

[2] Дискуссии о военных возможностях Китая в космосе и киберпространстве см.: David C. Gompert and Phillip C. Saunders, The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability (Washington, DC: National Defense University Press, 2011), chapter 3; James Dobbins, David C. Gompert, David A. Shlapak, and Andrew Scobell, Conflict with China: Prospects, Consequences, and Strategies for Deterrence (Santa Monica, CA: RAND, 2011), 5–7; Office of the Secretary of Defense, Annual Report to Congress, Military and Security Developments Involving the People's Republic of China 2010(Washington, DC: DOD, August 2010), 22–37; Jan Van Tol with Mark Gunzinger, Andrew Krepinevich, and Jim Thomas, AIRSEA Battle: A Point-of- Departure Operational Concept (Washington, DC: Center for Strategic and Budgetary Assessments, 2010), 17–47; Roger Cliff et al., Entering the Dragon's Lair: Chinese Anti-Access Strategies and their Implications for the United States (Santa Monica, CA: RAND, 2007), 51–60.

[3] Eric Schmitt and Thomas Shanker, "U.S. Debated Cyberwarfare in Attack Plan on Libya," The New York Times, October 18, 2011, and Ellen Nakashima, "Pentagon Officials Had Weighed Cyberattack on Gaddafi's Air Defenses," The Washington Post, October 18, 2011.

Междоменные операции и сдерживание

Эти определения подчеркивают тот факт, что военные акторы часто пересекают домены. В самом деле, американское военное устройство по своей сути междоменно: наступательное и оборонительное оружие США рассредоточено на воздушных, морских и сухопутных платформах; космос и кибератривы широко распространены и используются в операциях американских военных и создают преимущества в других доменах, и очень маловероятно, что будущие конфликты с США развернутся исключительно в пределах одного домена. С этой точки зрения сдерживание со стороны США по своей сути тоже междоменно: когда Соединенные Штаты угрожают отреагировать на действия, которые опасны для интересов США и их союзников, они угрожают, хотя это и неявно в большинстве случаев, междоменными ответами. Платформы, которые используют Соединенные Штаты, цели, подвергаемые атаке, и эффект от атаки могут быть в разных доменах и могут отличаться от доменов, которые используются и пострадали от первой атаки противника.

По той же логике Соединенные Штаты традиционно сдерживают атаки в целом, без различения между атаками, которые пересекают домены и тех, которые таковыми не являются. Военно-морские нападения на военно-морские силы не являются более или менее опасными, чем воздушные нападения на военно-морские силы. Соединенные Штаты пытаются сдержать оба вида, и средства, цель и масштабы реакции США будут зависеть от последствий нападения и целей США, а не доменов. Таким образом, Соединенные Штаты предостерегают от нападения, независимо от того, пересекает ли атака домены, угрожая ответом, который, скорее всего, будет междоменным, и будет отличаться от первой атаки. Учитывая, что между доменами сдерживание не является новым или редким явлением, реальный вопрос, который возникает в последнее время по теме, это: как Соединенные Штаты могут смягчить уязвимость, которая связана с зависимостью от космоса и киберпространства? Оба домена являются доминантными в деле нападения, где американская оборона неадекватна и политики не уверены в том, как эффективно угрожать возможному агрессору, чтобы он отказался от своих намерений. Хотя потенциальные противники менее зависят от космоса и киберпространства, чем Соединенные Штаты, это не объясняет, почему угрозы реагирования на кибератаки в других областях считаются менее надежными, чем междоменные ответы на атаку в воздухе, земле или на море.

Общая структура для оценки пропорциональности и эскалации в космосе и киберпространстве

Концепция Томаса Шеллинга, связанная с исследованием оружия и влияния, будет полезной отправной точкой для ответа на эти вопросы. Шеллинг утверж-

дал, что угрозы сдерживания являются более понятными для потенциальных противников и, таким образом, они более внушительны, если они являются соразмерными и связаны с действиями, которые предназначены для сдерживания: существует идиома в этом взаимодействии, тенденция использовать тот же язык, чтобы сделать наказание соответствующим характеру преступления … Это помогает оппоненту понять свою мотив, а также предоставляет ему основу для оценки ожидаемых последствий от его собственных действий … прямая связь между действиями и ответом помогает исключить возможность стечения обстоятельств и заставляет появиться другое следствие.[1]

Конечно, такое общение требует, чтобы страны интерпретировали военные действия и репрессии аналогично, другими словами, чтобы они общались через общую идиому действия. Шеллинг также признал, что нарушение шаблона поведения (то есть, эскалация) может быть необходимо в некоторых случаях, «чтобы вывести противника из равновесия для отображения ненадежности и дать возможность противнику реагировать естественно». Даже тогда, однако, общее понимание пределов, норм, и ожидаемых ответов создает необходимые рамки, с помощью которых акторы различают соразмерное и эскалационное поведение: «ломка правил является более драматичным, и больше сообщает о своем намерении именно потому, что это может рассматриваться как отказ от соблюдения правил».[2]

Идиома военных действий никогда не была такой последовательной, коммуникабельной и общепризнанной в реальности, как она описана у Шеллинга. Тем не менее, во времена Холодной войны эскалация была общепринятой от традиционных угроз до химического, биологического и ядерного оружия. В обычном конфликте было понимание того, что эскалация может произойти за счет расширения географической зоны боевых действий, расширение целей нападения (например, переход от узко военных к более широким, социальным целям), и увеличения интенсивности насилия (например, с помощью большего количества сбрасываемых бомб за вылет или переход к более разрушительным видам обычного оружия), характерные пороги отличаются в каждом обычном конфликта. К сожалению, страны не имеют общей базы для интерпретации того, чему кибератаки соответствуют в лестнице эскалации. Конкуренция и уязвимость в космосе и киберпространстве являются новыми по отношению к земле, воздуху и морю. Страны имеют меньше опыта ведения войны, где космос и киберпространство являются частью поля боя. В отличие от обычных и ядерных вооружений, эксперты менее уверены в точных последствиях нападений в этих доменах. По этим причинам, широко распространенных рамок для оценки того, как действия в космосе и кибератаки соответствуют и взаимодействуют с другими областями и, что

[1] Thomas C. Schelling, Arms and Influence. (New Haven: Yale University Press, 1966), 146–149.

[2] Ibid., 150–151.

более широко, с политическими отношениями между потенциальными противниками в мирное время, в условиях кризиса и на войне, еще не существует. Без этого лицам, принимающим решения, будет трудно отличать пропорциональные и эскалационные атаки, а также репрессии, которые переходят от традиционных стратегических доменов к этим новым, и наоборот. Отсутствие общей структуры внутри стратегического сообщества США усложняет эффективное междоменное планирование на случай чрезвычайных ситуаций. Разработка последовательных, эффективных и применимых вариантов реагирования на нападения в космосе и киберпространство требует, чтобы военные планировщики в разных службах и боевые команды обладали похожими предположениями о пропорциональности между доменами и эскалацией. Например, первый заместитель секретаря обороны по политике Джеймс Миллер показал, что США ответы на атаки в космосе «могут включать необходимость и пропорциональные ответы за пределами области космоса».[1] Но есть множество видов для нападения и еще более потенциальные мишени вне космоса. Общая основа будет способствовать планированию по определению, какие «некосмические» ответы лучше всего соответствуют атакам в космосе различного действия и тяжести. Отсутствие общей базы между Соединенными Штатами Америки, союзниками и потенциальными противниками подрывает сдерживание и увеличивает потенциал для просчета. Эффективное сдерживание требует, чтобы чиновники в США повлияли на восприятие потенциальных противников в отношении вероятных последствий от их действий, от которых США хотели бы их удержать. Соединенные Штаты могли бы угрожать ответом на нападения определенного типа в космосе или киберпространстве, используя различные возможности против различных целей в других областях. Такие угрозы, однако, имеют меньше шансов, чтобы резонировать как заслуживающие понимания потенциальными противниками, если они не воспринимают предположений США о том, как домены связаны между собой и почему тот или иной ответ является логичной и пропорциональной реакцией на первую атаку. В качестве примера, представьте, что Соединенные Штаты угрожают ответить на атаку на американские спутники разведки, наблюдения и рекогносцировки нападением на сети ПВО противника. Логика, лежащая в основе этой политики состоит в том, что Соединенные Штаты могут использовать самолеты разведки, наблюдения и рекогносцировки над территорией противника для компенсации утраченных спутников. Нападение на сеть ПВО будет необходимо для того, чтобы самолет мог эффективно проникать в воздушное пространство страны. Эта политика пропорциональна, потому что Соединенные Штаты восстанавливают утраченные возможности разведки, наблюдения и рекогносцировки, тем самым, отрицая преимущества атаки на спутники. Тем не менее, реакция

[1] James N. Miller, testimony for the House Armed Services Committee, Subcommittee on Strategic Forces, March 2, 2011.

США будет отличаться от нападения противника. Вместо ответа в космосе Соединенные Штаты будут атаковать цели на родине противника или вокруг нее. Чтобы еще более усложнить ситуацию, Соединенные Штаты могут использовать обычное оружие, чтобы уничтожить систему ПВО, даже если первая атака была некинетической. Без общего шаблона потенциальные противники могли бы рассмотреть такую угрозу сдерживания нелогичной и, следовательно, не заслуживающей доверия. Если сдерживание не удалось, они могут воспринимать такую реакцию США как произвольную и эскалационную. Даже с общим шаблоном они могут по-прежнему считать этот ответ как эскалацию войны, но они также будут понимать о вероятном последствии действий против Соединенных Штатов до отдачи приказа об атаке. Чтобы было ясно, общая база не будет, и не может прописать набор действий для всех мыслимых сценариев. Скорее, она должна определить универсальную лестницу эскалации, понятный по умолчанию или широко определенный кодекс поведения, который даст лицам, принимающим решения, лучшее чувство о том, какие действия и ответы ожидаются и приемлемы для сценариев реального мира, которые будут пересекать пороговые значения, нагнетающие обстановку. Это открыло бы путь для более когерентного междоменного планирования в правительстве США, а американское сдерживание воспринималось бы потенциальными противниками более ясно и понятно. Соединенные Штаты также будут лучше понимать исчисление потенциала противника в их усилиях по сдерживанию действий США. Культивирование такой общей базы является конструктивной целью на будущее, потому что сдерживание, регулирование кризисов и контроль эскалации были бы легче, если в разных странах пропорциональность, связность и эскалация интерпретировались бы аналогично. Привлечение стратегического сообщества США к тщательному диалогу по этим вопросам является первым шагом к достижению этой цели. Формирование рабочей группы по сдерживанию регионалистами, функционалистами и юристами может быть плодотворным подходом для запуска этого разговора.

Что может стать основой для оценки акций в космосе и кибератак в общем шаблоне? Должен ли ответ на кинетические атаки также быть кинетическим, чтобы он являлся пропорциональным? Является ли кинетический ответ на некинетические атаки всегда эскалацией? Может ли кибератака быть пропорциональна ракетному удару? Как чиновники сравнивают атаки, которые поражают цели в некоторых доменах и влияют на возможности и действия в других доменах? Космическая оборона и кибератаки могут значительно варьироваться по интенсивности, с эквивалентом того, как кладется рука на плечо и кулак бьет в лицо. Очевидно, что сам факт расширения конфликта в этих доменах является недостаточным показателем для оценки атак и калибровки ответов. Скорее, в реальном мире последствия таких атак, как внутри домена нападения, так и в

других доменах, должны определить, являются ли они эскалацией войны, и какие ответы были бы уместны.

Переменные в общем шаблоне

Культивирование общего шаблона между потенциальными противниками для оценки последствий и выработки соответствующих ответов будет трудным, независимо от количества участвующих доменов. Чиновники в США и других странах интерпретируют события через различные призмы. Культурные различия, контрастные стратегические цели, различия в структуре вооруженных сил и доктринах, различные сильные стороны и уязвимости могут привести лиц, принимающих решения в Соединенных Штатах и других странах, к различным выводам о пропорциональности и эскалации.[1] Эта задача не нова, но неопределенности в развивающихся стратегических доменах, обсужденные в предыдущих абзацах, могут усугубить ее. Представьте себе, что Китай столкнется с американскими спутниками через некинетические средства (лазером, который ослепит их, или с помощью заглушки) во время военного кризиса, который еще не перерос в вооруженный конфликт. Соединенные Штаты могут попытаться подорвать возможности Китая атаковать спутники США, возможно, отслеживания поток данных через кибератаки. Кто-то будет утверждать, что этот ответ пропорционален, потому что он ограничен в тех системах, которые использует Китай против Соединенных Штатов и не пересекает кинетический порог. С другой стороны, можно утверждать, что нападение в новом домене является эскалацией войны, открывая дверь репрессиям и контррепрессиям в киберпространстве и других доменах. Как китайские чиновники различают нападения на военные компьютерные сети от сетей, поддерживающих операции по внутренней безопасности режима? Если этого нет, то они могут интерпретировать этот «пропорциональный» ответ как экзистенциальное нападение, особенно, если они считают, что кибератака США вызовет побочный ущерб в более чем одной целевой компьютерной сети. Что делать, если изначальное нападение китайцев является кинетическим? Будут ли США, союзники и китайские чиновники воспринимать некинетический ответ против потенциала по космическим отслеживаниям Китая слабым, даже если он сумеет защитить спутники США? С другой стороны, была бы кинетическая атака на оружие Китая, которое он применяет, пропорциональной? Или пересечение географического порога (при условии, что цели находятся на материковой части Китая) сделают этот ответ эскалацией войны? Можно утверждать, что симметричный ответ — кинетическое нападение на китайский спутник –пропорционален. Однако, если спутники играют меньшую роль в китайских военных опе-

[1] Christopher P. Twomey, The Military Lens: Doctrinal Differences and Deterrence Failure in Sino-American Relations (Ithaca: Cornell University Press, 2010).

рациях, можно также утверждать, что такой ответ менее чем пропорционален, потому что он не налагает сопоставимые эксплуатационные расходы на Китай.[1]

Баланс между нападением и защитой в этих доменах будет также влиять на восприятие эффектов, эскалацию, пропорциональность и оптимальные стратегии сдерживания. Например, если нападение продолжает доминировать в космосе и киберпространстве, а потенциальные противники хотят атаковать американские активы в этих доменах именно потому, что они являются «мягким подбрюшьем» американских военных, ставки США в любом конфликте будут расти в геометрической прогрессии после таких атак потому, что эффекты в других областях будут глубокими. В результате , американские официальные лица могут почувствовать давление, чтобы осуществить превентивное действие до такого нападения, или они могли бы пойти на риск, чтобы быстро прекратить конфликт и наказать противника последствиями. Связь между уязвимостями в космосе и киберпространстве, и эффективностью возможностей США в других областях делает американские спутники и компьютерные сети важными целями, что также делает угрозу сильных репрессий более правдоподобной: это было бы соразмерным последствием нападению. Передача этого послания потенциальным противникам будет центральным компонентом стратегии сдерживания. Подчеркивание такой связи, возможно, даже повысит доверие к приверженности США к ответным мерам. Кроме того, Соединенные Штаты могут достичь способности не допустить, чтобы противники имели преимущества в атаке в этих доменах, выстраивая кибероборону и предоставляя наземные средства для спутников. В этом случае стратегия сдерживания США будет стремиться убедить потенциальных противников в том, что они не смогут повлиять на сухопутные, воздушные, морские и ядерные силы США, атакуя спутники и компьютерные сети. Такое послание может сделать угрозы США на ответные действия непропорциональным и менее правдоподобными, но это будет компромиссом, если Соединенные Штаты разработают оборонительные преимущества в космосе и киберпространстве. Лица, принимающие решения, также воспринимают нападения в космосе и киберпространстве по-разному, в зависимости от контекста. Атака на военные спутники и компьютерные сети может быть отложена и начата только тогда, как только начнется обычная война. Но подобные атаки могут вызвать конвенциональный конфликт, если они происходят до военных действий, когда обе страны хотят предотвратить кризис от перерастания в войну, но обеспокоены остаться слепыми, глухими и немыми от первого удара в космосе и киберпространстве.

Пропорциональность и эскалация — это относительные понятия: действия, которые являются эскалацией войны во время кризисов, могут

[1] Этот пример показывает, что симметричные и асимметричные ответы на атаки в космосе и киберпространстве не являются синономичными пропорциональным и эскалационным ответам.

быть соразмерными в ограниченных войнах и снижать ответные меры, так как интенсивность конфликта выросла.

С этим связан вопрос, будет ли американская реакция на кибер эксплуатацию в мирное время влиять на сдерживания в период кризиса? Хотя технологии и операции по кибер эксплуатации и кибератаки похожи, цели и эффекты различны: эксплуатация связана с извлечением информации из компьютеров и сетей без соответствующего разрешения; а атака направлена на уничтожение, деградацию или их изменение для достижения эффектов в других доменах. Но новости часто описывают случаи кибер эксплуатации против правительства США в качестве кибератак и свидетельствуют о ведущейся войне в киберпространстве.[1] Соединение этих операций вместе способствует впечатлению, что сдерживание США уже не удалось. Потенциальные противники могут сделать вывод, что угрозы США в ответ на кибератаки в других областях не правдоподобны и зависит от того, как США отреагировали на предыдущие операции по эксплуатации. Это восприятие может повлиять на учет рисков и преимуществ кибератак в кризисных ситуациях. Как могут официальные лица США публично передать то, что кибер эксплуатация и нападения представляют различные угрозы и требуют различной реакции, особенно учитывая частичное совпадение между этими ними? Подчеркивая, что реальные последствия от атак и эксплуатации могут отличаться, это станет первым шагом на пути к установлению порога между ними. Это послание укрепило бы веру, что сдерживание не провалилось, потому что эффекты от эксплуатации в киберпространстве еще не гарантируют военных ударов США по другим доменам. Это уточняет типы действий, которые Соединенные Штаты пытаются сдерживать.

Некоторые стратеги могут заключить, что пропорциональные действия в космосе и киберответы невозможны, потому что контроль за эскалацией в этих доменах слишком сложен. Там есть «бесконечное число сценариев, которые не являются ни показателем инцидента нарушения, ни стратегического нападения» в космосе и киберпространстве.[2] Оценка последствий от таких атак и выбор соответствующих ответных мер на фоне стресса и путаницы военного кризиса могут быть трудными. Чиновники в США и других странах, скорее всего, будет иметь разные мнения по поводу последствий некинетических сбоев, что сведется к простым клише, а препятствование выработке общих рамок может быть слишком грозным. Кроме того, последствия от сложных атак на спутники и компьютерные сети могут быть неразборчивыми и слишком трудно предсказуемыми. В этом случае стратегия сдерживания может акцентировать, что ограниченные действия

[1] Michael Riley and Ashlee Vance, "Cyber Weapons: The New Arms Race," Bloomberg Businessweek, July 20, 2011

[2] Susan J. Helms, "Schriever Wargame 2010: Thoughts on Deterrence in the Non-Kinetic Domain," Air Force Space Command High Frontier 7, no. 1 (November 2010), 14.

в космосе и кибератаки несут невыносимый риск неправильного восприятия, просчета и непреднамеренной эскалации. Вызывая «угрозы, которые оставляют что-то на волю случая», официальные лица США могут реально утверждать, что они не уверены в том , что они будут делать, потому что такие нападения будет включать «процесс, который не предвидится… реакции, которые не полностью предсказуемы… решения , которые не являются полностью преднамеренными... события, которые не в полной мере под контролем».[1] Конечно, выражение беспокойства о непреднамеренной эскалации может иметь неприятные последствия. Противники могут заключить, что угрозы таких атак вынудят США пойти на уступки.

Вывод

Многие системы вооружений и большинство военных операций требуют доступа к нескольким доменам (земля, воздух, море, космос и киберпространство). Эти связи создают уязвимости, которые акторы могут использовать, запустив междоменные атаки; Соединенные Штаты могут попытаться удержать такие нападения, угрожая междоменными ответами. Тем не менее, поскольку правительство США и потенциальные противники не имеют общей базы для анализа того, как такие понятия, как пропорциональность, эскалация, достоверность и сдерживание применяются в космосе и киберпространстве, это позволит не только перейти к операциям в другой домен, но и стать частью поля боя. В реальном мире последствия атак, поражающих цели в космосе и киберпространстве, влияют на возможности и события в других доменах, и должны стать основой для оценки их последствий и определении того, какие ответы в различных доменах являются соразмерными или приводят к эскалации.

Интеграция действий в развивающихся стратегических доменах космоса и киберпространства с действиями в традиционных доменах на четкой эскалационной лестнице может стать первым шагом к более согласованному междоменному планированию в правительстве США. Связывание этих рамок с потенциальными противниками будет способствовать более эффективному сдерживанию и антикризисноему управлению.

[1] Schelling, 95.