Connections: The Quarterly Journal
ISSN 1812-1098, e-ISSN 1812-2973

Оливер Фиттон, *Connections QJ* 15, № 2 (2016): 123-135
http://dx.doi.org/10.11610/Connections.15.2.08

Рецензированная статья

Кибер операции и серые зоны: вызовы для НАТО

Оливер Фиттон

Департамент политики, философии и религии Университета Ланкастера, http://www.lancaster.ac.uk/

Резюме: Серая зона представляет собой пространство между мирным соперничеством между государствами и войной. Действующие в этом пространстве акторы разработали гибридные стратегии для расширения своего влияния. Эту концепцию конфликта лучше всего иллюстрируют действия России в Восточной Украине в 2014 году. Доктрина Серой зоны использует неопределенность для создания среды, в которой противник не в состоянии уверенно принимать своевременные стратегические решения. К этому типу конфликта, благодаря сложности определения источника, относятся и кибер-операции. В этой статье рассматриваются связи между Серой зоной и кибер-операциями и вопросы, которыми НАТО следует заняться, чтобы адаптироваться к новым реальностям.

Ключевые слова: кибер-война, серая зона, неопределенность, НАТО, гибридная война.

Введение

Аннексия Крыма Россией в 2014 году является серьезнейшим вызовом для НАТО. События, которые имели место в Восточной Украине, предполагают наличие гибридной стратегии, которая в большой степени основывается на неопределенности. Стратеги в Москве использовали конвенциональные силы, влияние на русскоязычные СМИ, свободное толкование международного права, местные доверенные лица, информационные операции и кибер-операции в качестве инструментов для оперирования в серой зоне между войной и миром. Хотя то, чего Россия добилась в Крыму, является гораздо большим, чем просто мирное соперничество между государ-

ствами, тем не менее это было достигнуто без инициирования широкомасштабного военного конфликта.

В 2007 году Россия начала проведение еще одной операции в серой зоне, которая развивалась по тонкой грани между войной и миром. Атака типа «отказа в обслуживании», которая парализовала Эстонию в апреле того года, была результатом нарастания напряженности между двумя государствами. Россия не использовала для ответа вооруженные силы, что неминуемо задействовало бы Статью 5 Североатлантического договора. Вместо этого был использован новый тип операции, от ответственности за проведение которой легко отказываться, и которая входит в серую зону: кибер-операция.

Везде в этой статье доказывается, что кибер-операции являются и будут и дальше являться эффективным инструментом противников НАТО в рамках стратегии серой зоны. В работе исследуется новая концепция серой зоны и проливается свет на ее связь с гибридной войной. Применимость кибер-операций в рамках стратегии серой зоны рассматривается в плане затруднений пострадавшего возложить ответственность на виновного и возможностей для отрицания причастности, которые она предоставляет нападавшему. В конце статьи представлены три вызова с которыми сталкивается НАТО в результате кибер-операций в серой зоне. Во-первых, проблема которая состоит в неопределенности возможности применить Статью 5 Североатлантического договора; во-вторых, как можно осуществлять сдерживание против ограниченных операций, которые подрывают влияние НАТО; и наконец, какой курс выбрать в этой новой форме конфликта, которую либеральные демократические принципы запрещают. Вопрос разрешения этих проблем выходит за рамки задач этой статьи; скорее, целью является убедить академическое сообщество включиться в разрешение проблем серой зоны и рассмотреть вопрос, как кибер-операции будут ассимилированы будущими стратегиями.

Серая зона

Серая зона между войной и миром является основной особенностью современных конфликтов. Карл фон Клаузевиц рассматривает войну как продолжение дуэли между двумя сторонами, «как акт насилия, направленный на принуждение оппонента к выполнению нашей воли».[1] Для большей части истории человечества это определение было самоочевидным. Со времен Пелопонесских войн состояние войны подразумевало наличие известного противника с ясными политическими целями, которые входили в противоречие с собственными политическими целями. Как говорил генерал Кертис ЛеМэй, выигрывать войны было просто: «Вы начинали убивать людей и когда убивали достаточное количество, они пере-

[1] Carl von Clausewitz, *On War*, ed. Anatol Rapoport (Harmondsworth: Penguin Books, 1982), 101.

ставали сопротивляться».[2] Определение войны Клаузевица основано на трех неизменных характеристиках войны – война связана с насилием, война используется как инструмент и война есть политическое явление.[3] Однако, повышенное внимание, которое проявляют академические круги и политики (в частности, в рамках НАТО) к концепциям гибридных войн, неопределенных войн и ограниченных войн, дает основание думать, что характер войны изменился – по крайней мере, угрозы с которыми сталкивается Альянс становятся все более трудно определяемыми.

Из теоретиков, работающих в разнообразных областях, которые связаны с концепцией гибридной войны многие годы,[4] возможно наиболее цитируемым является Фрэнк Хоффман. Согласно его определению, гибридная война есть отклонение от предшествовавших воплощений войны: «Вместо отдельных вызовов с фундаментально отличающимися подходами (конвенциональный, нерегулярный, террористический), мы можем ожидать встреч с соперниками, которые будут применять все формы войны и тактики, возможно, одновременно».[5] Ярким примером такой доктрины для Хоффмана была стратегия Хезболла во Второй ливанской войне в 2006 году, во время которой Хезболла отбросила конвенциональные силы Израиля, имевшие огромное превосходство, путем использования конвенциональных и неконвенциональных тактических приемов.[6] В соответствие с интерпретацией Хоффмана гибридных угроз, Соединенные Штаты (США) все более часто будут сталкиваться с противниками, которые могут применять такие конвенциональные оружия как противотанковые и крылатые ракеты и беспилотные летательные аппараты, и в то же время использовать такие нерегулярные тактические приемы, как скрываться среди гражданского населения и использование самодельных взрывных устройств. Количество литературы по кибер-операциям и их значению в рамках гибридных стратегий весьма ограничено.[7] Однако, ведется гораздо более обширное обсуждение концепции кибер-войны в качестве отдель-

---

2 Richard Rhodes, *The Making of the Atomic Bomb* (London: Simon & Schuster, 2012), 586.

3 Thomas Rid, *Cyber War Will Not Take Place* (London: Hurst, 2013).

4 Смотри к примеру Larry R. Jordan, *Hybrid War: Is the US Army Ready for the Face of 21st Century Warfare*, Master's thesis (US Army Command and General Staff College, 2008); Mackubin Thomas Owens, "Reflection on Future War," *Naval War College Review* 61:3 (2008): 61–76; and Russell W. Glenn, *All Glory Is Fleeting: Insights from the Second Lebanon War* (Santa Monica, CA: RAND, 2012).

5 Frank G. Hoffman, "Hybrid Warfare and Challenges," *Joint Force Quarterly* 52 (2009): 35.

6 Там же, 37.

7 See Sascha-Dominik Bachmann and Hakan Gunneriussan, "Hybrid Wars: The 21st Century's New Threats to Global Peace and Security," *Scientia Militaria, South African Journal of Military Studies* 43:1 (2015): 77–98.

ной концепции, которая сильно связана с темой гибридной войны и конфликтов в серой зоне.[8]

Конфликт в серой зоне и гибридная война не являются взаимозаменяемыми концепциями. Действительно, использование термина «конфликт» для первой и «война» для второй является преднамеренным. Использование терминов «неконвенциональная» и «нерегулярная» тактика не ограничивается только строгими рамками парадигмы Клаузевица о войне. Концепция серой зоны пытается охватить операции, которые находятся на грани войны благодаря своей интенсивности, законности или (что наиболее интересно) неопределенности. Если надо использовать этот термин в содержательном смысле, то неконвенциональная тактика может охватывать информационные, дипломатические или экономические операции, не попадающие под определение «война». Командующие в НАТО начали публично выражать свою обеспокоенность такими неконвенциональными угрозами.[9] Как раз широкое использование неконвенциональной тактики способствовало развитию кризиса уверенности в НАТО.[10] Командование по специальным операциям США приступило к выполнению исследовательского проекта продолжительностью в год, под наименованием *Серая зона*. Этот проект должен дать руководству США инструменты для понимания угроз серой зоны и обеспечить эффективный ответ на них. Серая зона определяется как область между войной и миром, для которой все еще нет полного понимания. Действия, предпринимаемые в серой зоне, выходят за рамки нормального мирновременного соперничества, но чуть-чуть не доходят до полноценной войны.[11]

Российские операции в Восточной Украине и в Крыму имели как гибридный, так и неопределенный характер. В 2014 году Россия использовала сочетание конвенциональных военных сил (например, увеличение численности граничных и морских патрулей на границе с Украиной) и неконвенциональной тактики (к примеру, «маленькие зеленые человечки» и информационное превосходство, достигнутое использованием

---

[8] Смотри, к примеру, John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12:2 (1993): 141–165; Richard A. Clarke, *Cyber War: The Next Threat to National Security And What To Do About It* (New York: HarperCollins, 2010); and Rid, *Cyber War Will Not Take Place*.

[9] John Vandiver, "Breedlove: NATO Must Redefine Responses to Unconventional Threats," *Stars and Stripes*, 31 July 2014, http://www.stripes.com/news/breedlove-nato-must-redefine-responses-to-unconventional-threats-1.296129 (по состоянию на 23 января 2016).

[10] Peter Apps, "'Ambiguous Warfare' Providing NATO with New Challenges," *Reuters*, 21 August 2014, available at http://uk.reuters.com/article/uk-nato-summit-idUKKBN0GL1KA20140821 (по состоянию на 23 января 2016).

[11] United States Special Operations Command, "The Gray Zone," White paper, 9 September 2015), 1, http://army.com/sites/army.com/files/Gray%20Zones%20-%20USSOCOM%20White%20Paper%209%20Sep%202015.pdf (по состоянию на 23 января 2016).

русского национализма на Восточной Украине) для обеспечения аннексии Крыма. Эти действия вызвали тревогу в Альянсе, несмотря на то, что Украина не является членом НАТО. Преднамеренная двусмысленность российских действий и российской риторики парализовали способность Альянса эффективно реагировать и такой подход располагает потенциалом дать те же результаты, если эта доктрина будет применен против членов НАТО в Восточной Европе.[12] Является ли такая тактика новой или имеет исторические прецеденты остается спорным вопросом.[13] Однако, предельно ясно то, что НАТО не готово для конфликта в серой зоне.

Как было продемонстрировано в Восточной Украине, двусмысленность является полезным инструментом. Без полной картины проверенной информации, для стратега трудно выбрать оптимальный курс действий. Позволяя неопределенности иметь место при принятии стратегических решений или активно встраивая двусмысленность в стратегию, вполне возможно затуманить зрение противника. Соединенное Королевство (СК) использует политику преднамеренной неопределенности в своей политике стратегического ядерного сдерживания. В результате этого, противники Соединенного Королевства не знают «когда, как и в какой степени»[14] руководство Соединенного Королевства пожелает использовать ядерные оружия, в том числе и то, будут ли они использованы для нанесения первого удара. Четкая декларация планированного использования ядерного сдерживания позволила бы врагам более точно рассчитать собственную стратегию. Неопределенность в стратегическом ядерном сдерживании позволяет государствам предпринимать действия ниже порога конфликта, не угрожая явным образом индивидуальному противнику. Именно баланс между известными переменными и стратегией неопределенности поддерживал стабильность во времена Холодной войны.

Стратегия серой зоны используется нелиберальными демократическими государствами и авторитарными негосударственными акторами. Такая стратегия, особенно использование неопределенности, является несовместимой с обществами, основанными на социальном плюрализме, обязательных правовых принципах и подотчетности руководства. Подотчетность и прозрачность являются объектом пристального внимания в публичном дискурсе, касающегося военных действий после вторжения в

---

[12] Насчет дальнейшего обсуждения этой темы смотри House of Commons Defence Committee, *Towards the next Defence and Security Review: Part Two – NATO* (London: House of Commons Defence Committee, 2014), и, в частности, доказательства, представленные Комитету сэром Бобом Расселом.

[13] Питер Р. Мансоор обсуждает эту дискуссию, которая сконцентрирована на конкурирующих определениях понятия «гибридная война» в вводной главе «Гибридная война в истории» работы *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present*, ed. Williamson Murray and Peter R. Mansoor (Cambridge: Cambridge University Press, 2012).

[14] HM Government, *The Future of the United Kingdom's Nuclear Deterrent*, December 2006, Cm 6994, at 18.

Ирак в 2003 году и публикации печально известного «фальшивого досье».[15] Это внимание физически ощущалось в Соединенном Королевстве во время последних дебатов об интервенции в Сирию. Демократическая подотчетность ограничивает степень в которой правительства могут применять неопределенность.

Россия, однако, не ограничена социальным плюрализмом и подотчетностью правительства. Инакомыслие встречалось насилием.[16] Администрация Путина крепко держит в своих руках большинство русскоязычных медиа в регионе.[17] Процесс принятия решений в России намного менее прозрачен чем в странах-членах НАТО. Поэтому Россия относительно неограниченна в своей способности использовать как конвенциональные, так и неконвенциональные операции против своих врагов. Свободу операций в еще большей степени дает Даиш, поскольку он пренебрегает международным правом. В простом сценарии войны в духе Клаузевица, война ясно понятна и применимы установленные правила боевых действий. НАТО организовано так, чтобы выигрывать такие войны. В конфликте серой зоны неясно кто есть враг и каковы его намерения, что заставляет либеральные демократии подвергать сомнению законность своих реакций с гораздо большей дотошностью, чем это делают недемократические акторы. Либеральные демократии сильно ограничены в ситуациях в которых автократические государства и негосударственные акторы вовсе не ограничены. Это приводит к стратегическому дисбалансу, который угрожает и подрывает стратегическое превосходство, обеспечиваемое НАТО.

Кибер-операции

Так как противники НАТО разрабатывают стратегии использования серой зоны, вероятно, конвенциональные силы будут использоваться новыми способами и появятся новые неконвенциональные тактические приемы. Некоторые неконвенциональные тактические приемы, похоже, более эффективны, чем другие. Кибер-операции представляют собой развивающийся неконвенциональный подход, который может быть очень эффективным в конфликтах в серой зоне.

---

[15] Основанный на недостаточных доказательствах и неясно кем составленный разведывательный доклад, в котором утверждалось, что иракские оружия массового уничтожения могут быть приведены в боевую готовность за 45 минут. Это досье было использовано правительством Блэра, чтобы оправдать военную интервенцию в Ирак в 2003 году.

[16] К примеру, смерть Бориса Немцова в феврале 2015 года и насильственное задержание членов музыкальной группы Пусси Райот во время их демонстраций в 2014 году на Зимних Олимпийских Играх в Сочи..

[17] Scott Gehlbach, “Reflections on Putin and the Media,” *Post-Soviet Affairs* 26:1 (2013): 78.

Кибер-операции облегчаются опорой на сетевую коммуникацию. В них используется компьютерный код для изменения, сбора данных или деактивирования компьютерных систем в которых есть программное обеспечение, аппаратная часть и человеческий элемент. Нельзя считать, что кибер-операции напрямую связаны с использованием насилия, поскольку компьютерный код не может напрямую нанести ущерб человеку подобно кинетическим, энергетическим и химическим оружиям.[18] Тем не менее, они стали примечательным элементом современного конфликта, в том числе используются для нарушения работы инсталляций для обогащения ядерных материалов[19] и для того, чтобы шпионить за чужими правительствами.[20] В опубликованных недавно Национальной стратегии безопасности и Стратегическом обзоре обороны и безопасности Соединенного Королевства за 2015 год, правительство решило выделить £1.9 миллиардов на «защиту Соединенного Королевства от кибер-атак и на развитие … суверенных способностей в кибер-пространстве».[21] Кибер-операции имеют особую ценность в конфликтах в серой зоне благодаря двум своим ключевым характеристикам: органически присущие им проблемы с возложением ответственности за их проведение и легкость с которой нападающий может отрицать свое участие.

Для противников, которые хотят добиться стратегического превосходства не переходя порог, установленный Статьей 5 договора о НАТО, идиома «в Интернете никто не знает, что вы собака» оказывается особенно верной. Анонимность является центральной характеристикой деятельности в кибер-пространстве. Приписывание кибер-нападений противникам (лицам, негосударственным акторам или национальным государствам) является сложным, времяемким и проблемным делом. Кроме того, маловероятно что окончательный вердикт относительно возложения вины будет настолько определенным, чтобы оправдать использование традиционного военного ответа. Поэтому, сдерживающее действие, которое НАТО так успешно осуществляло в контексте вооруженного конфликта в Европе, не относится к кибер-операциям. Действительно, многие члены НАТО подверглись разным формам кибер-атак, наиболее заметной из которых была атака типа «отказ в обслуживании» против Эстонии в 2007.[22]

---

[18] Rid, *Cyber War Will Not Take Place*, 13.

[19] Насчет подробностей об инциденте с вирусом Stuxnet, смотри Nicolas Falliere, Liam O. Murchu and Eric Chien, *W32.Stuxnet Dossier* (Cupertino, CA: Symantec Corporation, 2011).

[20] Для более подробной информации об инциденте с GhostNet смотри "Tracking GhostNet: Investigating a Cyber Espionage Network," *Information Warfare Monitor*, 29 March 2009.

[21] HM Government, *National Security Strategy and Strategic Defence and Security Review 2015: A Secure and Prosperous United Kingdom*, November 2015, Cm 9161, с. 40.

[22] Kenneth Geers, "Cyberspace and the Changing Nature of Warfare," White paper presented at the 2008 Black Hat Conference, 7.0.

В 2015 году Томас Рид и Бен Бьюкенен провели оценку проблемы атрибуции в попытке понять ее вызовы и дать рекомендации людям, определяющим политику, касательно возможного решения. Они пришли к заключению, что анализ атрибуции [возложения ответственности – прим. ред.] является в какой-то мере искусством, требующим «умений, инструментов и организационной культуры: работающих команд, способных сотрудников, заработанного тяжелым трудом опыта и прежде всего трудно определяемого ощущения, что 'что-то не в порядке'».[23] Кроме того, они предостерегают, что атрибуция не есть взаимоисключающая дилемма «возможно-невозможно». Скорее, возложение ответственности можно осуществить с некоторым уровнем вероятности. И возможно, наиболее важное, Рид и Бьюкенен указали на то, что атрибуция есть вопрос политической воли: она зависит от ресурсов, которые государство желает выделить на решение проблемы.

Рид и Бьюкенен разработали систему, которую они назвали «Q моделью» атрибуции. Эта модель требует трехуровневое изучение ситуации, включающее тактический (технический), оперативный и стратегический анализ. На тактическом уровне, техники устанавливают, что кибер-атака имела место и используют все средства, находящиеся в их распоряжении, для того, чтобы понять, *как* было осуществлено нападение. Как противник вошел в систему и как он получил желаемый результат после осуществления доступа? На этом этапе анализ может быть сфокусирован на выслеживании интернет (IP) адресов, на наблюдении за движениями противника в вопросной системе, на реверсивном инжиниринге вредоносного кода и на множестве других технических аспектах. На оперативном уровне, результаты технического анализа накапливаются и оцениваются на фоне других источников информации, например нетехнического анализа (возможно сигнальная разведка или агентурная разведка), анализ схожих атак и более широкого геополитического контекста для создания гипотез о том, что случилось – так сказать, *что* атаки. И наконец, стратегический анализ помогает понять *кто* и *почему* предпринял нападение. На этом этапе субъекты, принимающие решение, рассматривают оперативные гипотезы, обсуждают кто может нести ответственность и формулируют ответную реакцию на основе значимости атаки. Последним моментом Q модели является коммуникация атрибуции к более широкой общественности.

Однако, эта модель не решает проблему атрибуции. Квалифицированные оппоненты все еще могут в определенной степени прикрыть свою роль в кибер-операциях, вероятнее всего указав пальцем на другого актора. Этого можно добиться использованием определенного языка или умелым размещением как будто ошибок в коде. Рид и Бьюкенен обращают внимание на то, что «Совершенная кибер-атака так же неуловима,

[23] Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies* 38 (2015): 30.

как и совершенное преступление».[24] Однако, противникам в гибридной войне не нужно осуществлять совершенные кибер-атаки, не подлежащие атрибуции; им нужно просто вызвать сомнения в головах аналитиков, достаточные для ограничения или замедления реакции политиков.

Второй отличительной чертой кибер-операций, которую исключительно важно понимать в контексте гибридных стратегий, является возможность отрицания причастности. Наблюдается усиливающаяся тенденция партнерства в отрицании причастности к кибер-операциям между государствами и группами специалистов по кибер-операциям, что обеспечивает защиту государства от возложения на него вины за подрывные неконвенциональные кампании. На ранних этапах гражданской войны в Сирии, режим президента Башара аль-Асада создал сомнительные отношения с группой, названной Сирийской Электронной Армией (СЭА). СЭА была поддерживающим Асада движением, которое взламывало западные вебсайты и аккаунты в социальных сетях, искажая их и распространяя проасадовские послания. В число более значимых целей входили *Onion*, Ассошиэйтед Пресс (АП) и Гарвардский университет.[25] Однако, СЭА не была персональной кибер-армией Асада и их отношения часто в глазах публики выглядели обтянутыми.[26] В результате этого Асад мог правдоподобно отрицать, что его режим несет ответственность за взлом западных вебсайтов и за кражу данных из институций США, используя тактические успехи СЭА. Предположительно, Россия использовала туже модель проведения кибер-атак на грузинское правительство в 2008 году и на эстонские финансовые институции в 2007, через организацию, известную как Российская Бизнес Сеть (РБС).[27]

Возложить вину за проведение кибер-операций трудно и в некоторых случаях причастность к их проведению можно отрицать, даже если на виновного можно указать. Они так же располагают потенциалом быть исключительно опасными. Хотя компьютерная программа никогда не убьет напрямую человеческое существо, очень возможно, что кибер-нападения на промышленную или социальную инфраструктуру могут привести к смерти людей. К примеру, в 2006 году эксперимент Аврора показал, что

---

[24] Там же, 32.

[25] Относительно более подробного обсуждения деятельности Сирийской Электронной Армии и проводимых ею нападениями, смотри Oliver Fitton and Mark Lacy, "The Syrian Electronic Army Is Rewriting the Rules of War," *The Conversation*, 3 September 2013, http://theconversation.com/the-syrian-electronic-army-is-rewriting-the-rules-of-war-17618 (по состоянию на 23 января 2016).

[26] Adam Jones, "Syrian Electronic Army Turns on Assad Regime," *Seczine: Security Magazine*, 21 August 2013, http://seczine.com/cyber-security/2013/08/syrian-electronic-army-turns-on-assad-regime/ (по состоянию на 23 января 2016).

[27] Joseph Menn, *Fatal System Error: The Hunt for the New Crime Lords Who Are Bringing Down the Internet* (New York: Public Affairs, 2010), 212–213.

компьютерные эксплойты могут привести к кинетическим последствиям,[28] и в 2010 вирус-червь Stuxnet оказался ответственным за отказы центрифуг ядерного объекта Натанз в Иране. Потенциал как для неопределенности, так и для эффективности, означает, что кибер-операции весьма вероятно будут использоваться противниками серой зоны в будущем, как это они делали и в прошлом.

Вызовы для НАТО

НАТО осознает, что гибридная война является стратегией, которую оно должно начать понимать и научиться ей противостоять. НАТО должно специально обратить внимание на роль, которую играют кибер-операции в рамках гибридных стратегий с учетом на их неопределенного характера. Очевидными являются три конкретных вызова. Во-первых, стоит вопрос о том, как применять Статью 5 Североатлантического договора в случае кибер-нападений на члена НАТО с учетом того, что атрибуция не является «или-или» вердиктом. Во-вторых, если атрибуция и возможность для отрицания причастности удерживают НАТО от использования силы, то тогда Альянс должен найти способ удерживать врага от применения низкоинтенсивных тактик, подобные тем, что были использованы в Эстонии, Грузии и Восточной Украине. И последнее, надо проверить может ли НАТО использовать кибер-операции в рамках стратегии серой зоны, соблюдая при этом либерально-демократические принципы, которые отличают Альянс от его противников. Иными словами, НАТО поступило бы мудро, если займется стратегиями серой зоны.

Статья 5 Североатлантического договора говорит, что «вооруженное нападение на одного из членов, или на нескольких членов в Европе или в Северной Америке будет считаться нападением на всех членов». Поэтому, Альянс предпримет «такие действия, которые он сочтет нужными, в том числе, использование вооруженной силы, для восстановления и обеспечения безопасности Североатлантического региона».[29] Первая проблема, в связи со Статьей 5, касающаяся кибер-атак выражается в споре о степени в которой кибер-атаки являются «вооруженным нападением».[30] Если кибер-атаки нельзя считать связанными с использованием насилия[31] то тогда спорным является их статус «вооруженного нападения». Если кибер-атаку не считать вооруженным нападением, то такое событие не запускает автоматически процесс реакции, на котором основывалась безопасность Ев-

[28] Fortinet, “Securing SCADA Infrastructure,” White paper (Sunnyvale, CA: Fortinet, 2010), 6.

[29] “The Atlantic Charter,” last modified 1 October 2009, доступно на www.nato.int/cps/ bu/natohq/official_texts_16912.htm.

[30] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013), 3.

[31] Смотри Rid, *Cyber War Will Not Take Place.*

ропы после Второй мировой войны. Однако, эта точка зрения стала спорной после кибер-атак против Эстонии в 2007 году. Генеральный секретарь НАТО, Йенс Столтенберг, подтвердил, что НАТО рассматривает кибер-атаки в духе требований для предприятия действий, основанных на обязанностях в соответствие со Статьей 5.[32] Это отражает одностороннею позицию, занимаемую Соединенными Штатами.[33]

Следующий вопрос, связанный с первой проблемой, это как оправдать военный ответ на кибер-атаку по Статье 5 при условии, что процесс атрибуции (как он описан Ридом и Бьюкененом) требует времени, инвестиций и многоуровневого подхода для того, чтобы дать ответ, который, вероятно, не будет на сто процентов определенным. Даже если есть согласие о законности вооруженной реакции на кибер-атаку, уверенность командиров НАТО в их действиях все равно будет основываться на подверженной ошибкам науке атрибуции. Более того, для НАТО будет затруднительно реагировать решительно, если противник подозреваемый в осуществлении кибер-атаки располагает встроенной способностью отрицать свою причастность, как в случае с Россией и РБС или с режимом Асада в Сирии и СЭА. Если бы кибер-операции проводились одновременно с конвенциональными военными операциями (как в Грузии в 2008), действия, основанные на Статье 5, были полностью оправданными. Если кибер-операции предшествуют использованию конвенциональных тактик в рамках гибридной стратегии, НАТО может оказаться ограниченным в своей реакции, разделенным и неспособным действовать решительно в результате преднамеренной неопределенности, создаваемой противником путем правдоподобного отрицания.

Вторая проблема, которую НАТО надо преодолеть, это как удерживать противника от проведения кибер-операций против членов НАТО. Полный охват кибер способностей государства по необходимости является неоднозначным вопросом. Если конкретные способности будут раскрыты, эксплойты на которых они основываются будут исправлены и соответствующая способность станет бесполезной. Это фундаментально иной вызов по сравнению с конвенциональным и ядерным сдерживанием. Хотя кибер-операции могут никогда не стать сравнимыми с конвенциональными и ядерными средствами ведения боевых действий до степени, чтобы они представляли собой экзистенциальную угрозу для национального государства, весьма вероятно, что их могут использовать для дестабилизации общества, экономики и населения в сфере влияния противника, как часть бо-

[32] Paul McLeary, "NATO Chief: Cyber Can Trigger Article 5," *Defense News*, 25 March 2015, доступно на www.defensenews.com/story/defense/policy-budget/warfare/2015/03/25/nato-cyber-russia-exercises/70427930 (по состоянию на 23 января 2016).

[33] Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal*, 31 May 2011, доступно на http://www.wsj.com/articles/SB10001424052702304563104576355623135782718 (по состоянию на 23 января 2016).

лее широкой гибридной доктрины. Такая дестабилизация может способствовать эрозии влияния НАТО и его способности гарантировать достижения стратегических целей.

Последний вызов касается того, как либерально-демократические принципы НАТО удерживают его от применения тех же тактик, что и противник, несмотря на возможность делать это, и добиваться, таким образом, стратегического успеха. Члены НАТО, в частности США и Соединенное Королевство, делают одни из самых больших инвестиций в кибер-операции. Однако, это государства, которые в высшей степени ограничены в открытом использовании неконвенциональных тактик. Либерально-демократические принципы, включающие верховенство закона, подотчетность правительства и прозрачность ограничивают эти государства в использовании неконвенциональных операций в мирное время. В результате этого, НАТО подвергается риску оказаться в доктринальном дефиците, который труднее преодолеть, чем любое технологическое отставание. Таким образом, противники НАТО могут использовать преимущество серой зоны между войной и миром: Даиш может захватывать территорию распространяя страх и свои радикальные послания, а Россия может получать территориальные и психологические приобретения в Восточной Европе, тогда как НАТО философски обвязано соблюдением строгих ценностей. В результате влияние НАТО подрывается, поскольку оно не может играть по тем же правилам и проигрывает.

Несмотря на все это может оказаться, что прагматизм перевешивает ценности. Россия давно обвиняет Запад в использовании весьма неоднозначных стратегий, которые сейчас западные академические круги приписывают России.[34] По мнению Тимоти Л. Томаса, российские теоретики давно рассматривали поражение Советского Союза как результат тайной информационной войны.[35] Есть вопросительные относительно того, насколько устойчивой может быть такая доктрина в современной эпохе. Вполне возможно, что члены НАТО могут создать подлежащие отрицанию отношения с онлайн негосударственными акторами с целью установить партнерские отношения, которые легко отрицать, подобные тем, которые используют Асад и Путин. Естественно, это было бы более легким путем для либерально-демократических держав. В число принципов многих онлайн групп входят свобода, равенство и позитивизм, если не верховенство закона. Однако, любое свидетельство о таком партнерстве породит напряженность между населением и правительством в пост-викиликс мире. Кроме того, способность отрицать, которой пользуются противники НАТО, оплачивается ценой за командование и управление, что может привести к нежелательным последствиям в сильно охваченных сетями обще-

[34] Timothy L. Thomas, “Nation-State Cyber Strategies: Examples from China and Russia,” in *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Dulles: Potomac Books, 2009), 486.

[35] Там же, 477.

ствах. В результате, партнерства, которые можно отрицать, вряд ли будут привлекательны для НАТО в рамках стратегии серой зоны.

Заключение

Конфликт серой зоны маркирует продолжение гибридной войны в пространстве между миром и войной. В нем для достижения политических целей применяются конвенциональные и неконвенциональные методы, а так же неоднозначность для затуманивания оценки противника. Кибер-операции являются неконвенциональной тактикой, которая использовалась и будет и дальше использоваться в серой зоне противниками НАТО. Проблемы, касающиеся атрибуции кибер-операций, и продуманной возможности отрицать причастность со стороны противника сильно ограничивает способность НАТО предпринимать ответные меры против кибер-операций. Для НАТО жизненно важно разработать средства для ответа и сдерживания в случае использования такой тактики, не только из-за ущерба, который могут нанести кибер-операции, но и из-за их потенциал подрывать влияние НАТО в сферах, где имеет место конкуренция.

Об авторе

Оливер Фиттон является аспирантом на кафедре политики, философии и религии Университета Ланкастера, Соединенное Королевство, и исследователем для Security Lancaster, Центра профессиональной квалификации по кибер-безопасности ШКГК. Предметом его исследований являются кибер-операции и неоднозначность в современном и будущем конфликте.
E-mail: o.fitton@lancaster.ac.uk.