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

Фил Лестер, Шон Мур, *Connections QJ* 19, № 1 (2020): 43-49
https://doi.org/10.11610/Connections.rus.19.1.04

**Национальная политика кибербезопасности**

# Реакция на киберугрозу: точка зрения вооруженных сил

## *Коммодор авиации Фил Лестер, Королевские Военно-воздушные силы, капитан Шон Мур, Королевский Военно-морской флот*

**Резюме**: В статье рассматривается вклад Вооруженных сил Объединенного Королевства в национальный подход к кибербезопасности, охватывающий континуум внутригосударственной деятельности, начиная от состояния мира, через сотрудничество, конкуренцию, конфронтацию, конфликта и до состояния войны. В соответствие с доктриной Объединенного Королевства, вооруженные силы выполняют активные и пассивные оборонные функции в киберпространстве, проводят наступательные кибер операции, кибер разведку, наблюдение и рекогносцировку, кибер оперативную подготовку среды, а ответные действия не ограничиваются только кибер доменом.

**Ключевые слова**: военные кибер способности, кибер операции, стратегический обзор обороны, доктрина комплексирования.

В 2015 году в *Стратегии национальной безопасности* и в *Стратегическом обзоре обороны* правительство Объединенного Королевства выразило понимание растущей угрозы национальной стабильности, безопасности и процветанию, проистекающие из действий, происходящих в киберпространстве, или вытекающих из киберпространства. Наши национальные кибер способности поддерживают наши стратегические цели через три основные функции: предотвращение конфликтов и материализации угроз; защита Объединенного Королевства и его заморских территорий от нападений специально (но не исключительно) в и через кибер пространство; и про-

ецирование влияния и мощи быстро и адекватно, либо напрямую из Объединенного Королевства, либо в рамках экспедиционной операции.[1] Это национальные функции и вооруженные силы имеют свой вклад в каждую из них; тем не менее, мы понимаем, что военное участие под и над порогом войны следует рассматривать как продолжение политики.[2] Поэтому военный вклад является поддерживающей функцией в контексте более широкой, комплексной, пан-национальной реакции и используется в соответствие с применимым законодательством, включая – когда существует состояние войны – международное гуманитарное право (т.е. правовые нормы, относящиеся к вооруженному конфликту или к войнам). В этой короткой статье мы пытаемся описать участие вооруженных сил в общенациональном подходе к проблемам кибербезопасности и то, как существующие международные правовые и нормативные рамки дают достаточные основания для проведения операций в, из или через киберпространство.

Хотя киберпространство признается НАТО и национальной военной доктриной Объединенного Королевства доменом ведения войны, оно также имеет далеко идущие невоенные аспекты, которые оказывают влияние на нашу повседневную жизнь.[3] По этой причине, деятельность в киберпространстве должна соответствовать основанной на правилах международной системе. Поэтому мы признаем, что существуют границы приемлемого поведения государства в киберпространстве, также как и во всякой другой сфере. В 2013 группа правительственных экспертов ООН по использованию кибертехнологий подтвердила применимость существующего международного права к кибер деятельности государств. 26 июня 2015 Группа экспертов ООН, в которую входят не только Объединенное Королевство и США, но и Китай и Россия, подтвердила, что Устав ООН применим во всей его целостности и к киберпространству. Группа подтвердила применимость органически присущего права государства на самооборону в ответ на кибероперацию, которая выше порога вооруженного нападения. Кроме того, доклад Группы от 2015 года подтвердил, что фундаментальные принципы защиты международного гуманитарного права – необходимость, пропорциональность, гуманность и дифференцирование – применимы к киберпространству.

---

1 Ministry of Defence, “Cyber Primer,” Second Edition (Shrivenham, UK: Development, Concepts and Doctrine Centre, July 2016), 2.

2 Под- или надпороговое участие следует рассматривать как способность осуществить массированное (и не-приписываемое) воздействие без вызова существенной реакции, таким образом размывая нормальное, и потому приемлемое, соперничество государств. Это не просто узкая лента, которая лежит на границе между миром и войной, а текучее и изменяющееся пространство, которым можно манипулировать во времени, домене и среде.

3 Joint Doctrine Publication 0-01 UK Defence Doctrine, 6th Edition (Draft).

Версия этой статьи была представлена на конференции Кибер нормы в МТИ, Бостон. Многое из того, что мы говорили, резонирует с этой публикацией, и поэтому мы использовали свою прежнюю работу для включения в этот журнал.

Соответственно, деятельность в рамках кибер обороны, позволяющая военные действия или поддерживающая более широкую деятельность правительства, охватывает континуум межгосударственной деятельности от Мира через кооперацию, конкуренцию, конфронтацию и конфликт, и до Войны. Реальность повышенной враждебной деятельности государства через киберпространство и под порогом вооруженного конфликта вызывает повышенную озабоченность увеличивающимся риском все более разрушительных кибератак, а также и потенциально непреднамеренных побочных эффектов атаки на нашу собственную инфраструктуру. Эта реальность требует от нас рассмотреть как можно использовать военные инструменты для противодействия таким угрозам и действиям в период постоянного соперничества и ниже порога вооруженного конфликта.[4] Чтобы сделать это, мы развернем некоторые из тем, которые проистекают из наименования, например «ответ», «комплексирование», «усмотрение», «следует обязательно» или «можно», и представим в более широком контексте, включающем военный вклад в рамке пяти доменов – интегрированные воздушное пространство, космическое пространство, киберпространство, морское пространство и сухопутное пространство – через нашу модель Совместных операций для достижения военных целей национальной стратегии.[5]

Во-первых, использование слова «ответ» вызывает отрицательные ассоциации – оно подразумевает реактивный характер действий и определенную пассивность перед действием. Очень часто ответ используется в сочетании с военным – «военный ответ». Но это скрывает органически присущий наступательный характер и полезность упреждающих качеств военных инструментов. Надо признать, что жесткие кинетические действия не всегда подходящие или необходимы. Вооруженные силы могут предложить больше, чем чисто наступательные или оборонительные способности. Итак,

---

[4] «Постоянное соперничество» можно определить, как интенсивная враждебная деятельность государств вне рамок основанной на правилах международной системы, которая ниже порога, который мог бы привести к вооруженному конфликту.

[5] «Совместные действия» является нашим рамочным подходом интегрирования информационной активности с огневым воздействием (с летальными и нелетальными последствиями), маневром и пропагандой с целью получения конкурентного преимущества – добиваясь влияния в качестве главного результата и используя интеграцию в качестве главного принципа. Темп и точность воздействия создаются главным (но не единственным) образом совместными силами, быстрым планированием и проведением операций в рамках одного или нескольких доменов «для сохранения инициативы и создания множества неразрешимых дилемм для противника.

здесь упор на том, что существует широкий диапазон военных возможностей, которые имеют большую полезность применения, давая свой вклад в комплексный национальный подход левее нанесения удара по противнику или в зоне подпорогового постоянного соперничества. Это может быть содействие упреждающему сдерживанию или стратегии принуждения, или содействие целостному подходу к национальной безопасности. Тем не менее, мы должны признать, что вклад вооруженных сил, конечно, может не быть кибер действием. Итак, наша способность действовать более эффективно «левее взрыва», как мы любим говорить, требует ресурсов и политического аппетита действовать таким образом. Все это надо упражнять и пробовать, чтобы доказать работоспособность такого подхода – и это не может быть чисто военным мероприятием. Военное участие надо «комплексировать» с другими – разведывательными ведомствами, правительством, другими правительственными департаментами, индустрией и критической национальной инфраструктурой, например. Мы говорим о постоянном соперничеством с нашими противниками; следовательно, наш подход предполагает постоянное участие – физическое, виртуальное и когнитивное – с использованием национальной мощи, дипломатии, информации, экономики и вооруженных сил не только для демонстрирования национальной решимости, но и для обеспечения сохранения конкурентного преимущества.

Это приводит к «комплексированию» («фьюжн») и, естественно, к Доктрине комплексирования правительства Объединенного Королевства. Принципы Фьюжн доктрины, по нашему мнению, не являются чем-то новым. У нас есть «интегрированный подход», «комплексный подход» и «подход полного спектра», и все они направлены на комплексирование всей деятельности Уайт-холла. Тем не менее, Фьюжн доктрина идет дальше, поскольку она внушает настоящее ощущение совместного мышления и совместной практики для получения успешных результатов в ответ на множество вызовов. Ключевой функцией Фьюжн доктрины является формирование стратегии сдерживания противника. И сдерживание киберагресии или кибератак должно включать все аспекты национальной жизни, гарантируя, что все секторы будут формировать свою реакцию не в изоляции, а когерентно, последовательно и скоординировано с другими. В результате, наш подход к современному сдерживанию несколько отличается от сдерживания времен Холодной войны. Сдерживание сегодня должно быть более нюансированным использованием жесткой и мягкой силы, причем вклад в комплексную стратегию сдерживания конкретных угроз и конкретного поведения должны давать все департаменты.

Итак, что «могут» делать в этом плане вооруженные силы? Ответ на этот вопрос следует разделить на две части: общий вклад, что мы делаем и о чем мы заботимся, когда поддерживаем приоритеты Правительства, а также и конкретная кибер роль. Рассмотрим сначала наш общий вклад.

Через вооруженные силы Государство упражняет свое право легитимировать использование силы, и эта сила используется для достижения более широких политических целей, на первом месте, безопасность нашей нации. Наши цели четко определены в Стратегии национальной безопасности и в политике обороны. Из этих целей проистекает определение и обеспечение ресурсами ряда военных задач.

Наличие способных, профессиональных и хорошо обученных вооруженных сил дает государствам более широкий набор вариантов ответа на кибер угрозы. Как сказал бывший Генеральный прокурор Объединенного Королевства, «Государства, которые являются объектом вражеских кибер операций, имеют право отвечать на эти операции с использованием возможностей, которыми они располагают в соответствии с законом …».[6] Враждебная кибер операция не предполагает непременно кибер ответ. Для государств, которые находятся под ударом, открыты все законосообразные возможности, в том числе и вооруженная реакция, когда это оправдано.

Хотя вооруженные силы Объединенного Королевства обеспечиваются ресурсами и конфигурируются для защиты нашей национальной безопасности, наши большие морские, сухопутные, воздушные, космические и кибер способности можно использовать и в других кризисах, например, для оказания гуманитарной и военной поддержки другим департаментам правительства. Таким образом, наша реакция на кризис или событие, вызванные действиями в киберпространстве, может включать полный спектр конвенциональных военных способностей для использования при выполнении ограниченных или дискретных функций и ролей. Это не отличается от того, что мы видели при вспышке ящура в Объединенном Королевстве в 2001, при забастовках противопожарной службы или при наводнениях, когда военные способности использовались для усиления других департаментов или гражданских организаций. Но одна область, в которой военные могли бы обеспечить очень ценную общую поддержку, это наши организации командования и управления, которые создаются с задачей реализации интегрированных, межфункциональных связей, координации и управления. Эти штабы очень опытны в комплексировании разведданных и информации из разных источников для направления деятельности, и они смогут коммуникировать оборонный вклад и гарантировать то, что он будет согласован с более широким нарративом. Наши штабы также очень опытны при применении правил вступления в бой и стандартов пропорциональности и дифференциации использования военных способностей – будь то летальная, или не-летальная сила. Поэтому мы считаем, что вооруженные силы умеют сдерживать себя и используют проверенные процессы для усиления или ослабления использования или угрозы использования силы для достижения желаемого результата. Мы также используем «вилки и розетки» для

[6] Речь Королевского адвоката Джереми Райта в Чатем-хаус 23 мая 2018.

привлечения не-институциональных или необоронных структур в архитектуру принятия решений. В сочетании, все это позволяет осуществление эффективного, быстрого и основанного на фактах процесса принятия решений.

Давайте рассмотрим конкретный кибер вклад. Доктрина Объединенного Королевства четко расписывает как сектор обороны распределяет свои операции в кибер пространстве, и как эти операции способствуют достижению военных результатов и поддерживают достижение более широких политических целей. Здесь мы не будем вдаваться в подробности – но с уверенностью можно сказать, что наша доктрина определяет следующие функции в киберпространстве: оборонные[7] (активные[8] и пассивные[9]), а также наступательные[10] кибер операции, кибер разведка, наблюдение и рекогносцировка[11] и оперативная кибер подготовка среды.[12]

В плане того, что «должен» представлять собой вклад вооруженных сил, наш подход является двухсторонним. Во-первых, мы должны продолжать интегрировать наше мышление и действия в киберпространстве со всеми вооруженными силами. Ключом здесь являются доктрина и образование. Из-за чувствительного характера кибер домена, в настоящее время наша доктрина засекречена, что ограничивает доступ к ней и мешает нашей способности расширять понимание кибер операций в среде вооруженных сил Объединенного Королевств. Мы рассматриваем пути для расширения доступа к нашей кибер доктрине для усиления ее применения в качестве элемента нашего подхода к интеграции пяти доменов (морское пространство, сухопутное пространство, воздушное пространство, космическое пространство и киберпространство). Параллельно, мы начинаем разрабатывать некоторые самые современные подходы концептуального мышления для ведения будущих итераций нашей доктрины, образования и практики. В сочетании, все это повысит нашу информированность в киберпространстве, нашу маневренность и, следовательно, нашу способность создавать кибербойцов, способных действовать в киберпространстве, а не кибервоинов – хотя последние тоже нужны. Второй элемент должен и дальше направлять внимание на то, что нам нужно для гарантирования того, что наши сети и

---

[7] Активные и пассивные меры для сохранения способности использовать киберпространство.

[8] Деятельность, которая направлена против враждебных кибер операций для сохранения нашей свободы маневрирования в киберпространстве.

[9] Специфические для конкретной угрозы оборонные меры для уменьшения эффективности кибер деятельности.

[10] Деятельность, которая проецирует мощь для достижения военных целей в или через киберпространство.

[11] Деятельность по Разведке, Наблюдению и Рекогносцировке (PHP) в и через союзническое, нейтральное или вражеское киберпространство для установления понимания.

[12] Все виды деятельности для подготовки и обеспечения кибер PHP, а также оборонительных и наступательных операций.

наш интерфейс настолько устойчивы, насколько это возможно, и что наши оборонные меры соответствуют и скоординированы с теми, кто законным образом имеет доступ или участвует в наших системах. Это не простая проблема, особенно необходимость обеспечить кибер устойчивость во всех наших программах развития, а также гарантирования того, что наши старые программы и способности смогут быть адаптированы к быстро меняющейся динамике угроз в киберпространстве, сейчас и в будущем.

Итак, в заключение, вооруженные силы могут дать существенный вклад в борьбу с киберугрозой, и многое уже делается. Мы также должны признать, что вне всякого сомнения наш вклад имеет три главные направления. Во-первых, гарантировать, что наша кибероборона будет прочной и устойчивой, в том числе и то, что она согласована и скоординирована с оборонительными подходами тех, кто участвует в наших сетях. Во-вторых, наш ответ или вклад может не быть в киберпространстве, как таковом. В-третьих, наши структуры командования и управления дают очень полезную точку отсчета, от которой мы можем развивать комплексные стратегические штабы, которые координируют и направляют наши операции в киберпространстве. Это может быть осуществлено, только если Оборона продолжит инвестировать в интегрирование киберпространства, как угрозу и как возможность, в наши стратегии, доктрины и практику. И возвращаясь к вопросу, эффективный фьюжн можно осуществить только через практику, тренировки и испытания … пока он не станет второй природой.

## Отказ от ответственности

Выраженные здесь взгляды являются исключительно взглядами авторов и не отражают точку зрения Правительства ее Величества, Министерства обороны, Вооруженных сил ее Величества или любого ведомства Объединенного Королевства, Консорциума оборонных академий и институтов изучения безопасности ПрМ, участвующих организаций или редакторов Консорциума.

## Признательность

Том 19 журнала *Connections: The Quarterly Journal* публикуется при поддержке правительства Соединенных Штатов Америки.