Степени применения силы в боевом киберпространстве

Джозеф Бюссинг[*]

Введение

Каждое мгновение коммуникации по Интернету зависит от передачи конфиденциальной, легко доступной и аутентичной информации. Если эта информация будет считана, изменена или сфальсифицирована каким бы то ни было образом, это подвергнет риску надежное и безопасное функционирование любого сервиса, зависящего от передачи данных. Таким образом, эксплуатация данных может быть использована в целях, которые могут иметь разрушительные последствия для современного общества. Основная проблема сетевого общества состоит в том, что международные конвенции об использовании силы не могут в достаточной степени защитить мир от нестабильностей, порождаемых компьютерными атаками. В этой статье сделана попытка улучшить ситуацию путем определения того, какие типы действий, совершаемых посредством компьютеризированных сетей, являются применением вооруженной силы или вооруженным конфликтом.

В этой статье международное право, существующее в период вооруженных конфликтов (МПВК), применено к трем случаям компьютерных атак, осуществленных национальными государствами. При рассмотрении этого вопроса целью было указать законодательные ограничения на действия, которые могут быть предприняты в ответ на компьютерные атаки. Первый рассматриваемый случай, это волна кибератак, которые имели место в войне в Южной Осетии между Россией и Грузией в 2008 году. Второй случай относится к тайной операции Соединенных Штатов под кодовым наименованием «Олимпийские игры». В этом случае анализ будет сфокусирован на компьютерной программе Stuxnet. В третьем случае МПВК используется для оценки актов цифрового шпионажа, осуществленных формированием 61398 Народно-освободительной армии Китая.

Применяя как правовую норму МПВК к этим трем случаям, можно прийти к выводу, что существуют три четкие интерпретации основанных на использовании компьютеров операций. Случай от 2008 года во время войны в Южной Осетии является ситуацией, в которой использование компьютеров для нападения на другую страну можно интерпретировать как применение силы и как акт вооруженного конфликта. Операция «Олимпийские игры» показывает, что компьютерные атаки можно считать использованием силы, но не актом вооруженного конфликта. Анализ действий подразделения 61398 демонстрирует вариант компьютерных атак, которые не являются ни применением силы, ни вооруженным конфликтом. Каждый из рассмотренных случаев отражает уникальные характеристики операций в киберпространстве. Поэтому, для того чтобы обосновать юридическое понимание

[*] Джозеф Бюссинг родился и вырос в Кремниевой долине в Калифорнии. Недавно он закончил магистерскую программу по международным отношениям Новой школы в Калифорнии. Он также является компьютерным программистом-самоучкой.

этих случаев, в анализе отдается предпочтение основанной на результате оценке кибератак, впервые предложенной Майклом Шмиттом и изложенной в Таллиннском руководстве по международному праву, применяемого к кибервойнам.[1]

Разработка правовой классификации кибератак с использованием подхода, основанного на их результатах

Основанные на использовании компьютеров атаки являются подмножеством действий, которые можно описать как информационные операции. Информационные операции (ИО) определяются как действия, предпринятые вооруженными силами во время мира или войны с целью оказать влияние на информацию и информационные системы противника, в то же время обеспечивая защиту собственной информации и информационных систем.[2] В широком смысле ИО связаны с созданием помех радиолокационным станциям, с применением психологических и электронных средств ведения операций. Одним из подмножеств электронных ИО являются компьютерно-сетевые операции (КСО). КСО – это операции, направленные на нападение, обман, деградирование, нарушение работоспособности, отрицание, использование и защиту электронной информации и инфраструктуры.[3] Двумя основными субэлементами КСО являются кибератаки и киберзащита. Сетевые компьютерные атаки – это действия, осуществляемые через компьютерные сети с целью разрушить, сорвать доступ, деградировать или уничтожить информацию в компьютерах и компьютерных сетях и/или сами компьютеры.[4] Если информация в компьютере, который управляет уровнем воды на ядерной электростанции, претерпевает какое бы то ни было нарушение потока данных, это может иметь разрушительные физические последствия.[5] Каждый из случаев, представленных в этой статье, является формой КСО, которая имеет свои специфические последствия. Последствия, проиллюстрированные в каждом из рассмотренных примеров, охватывают диапазон от отказа предоставления какого-нибудь сервиса и кражи информации, до физического разрушения.

---

1 Michael N. Schmitt, gen. ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge: Cambridge University Press, 2013).

2 Объединенный комитет начальников штабов, Совместная публикация 3-13, «Информационные операции» (13 февраля 2006), Gl-3; доступно на www.carlisle.army.mil/DIME/documents/jp3_13.pdf.

3 Ulhas Kirpekar, "Information Operations in Pursuit of Terrorists," Master's Thesis completed at the Naval Postgraduate School, Monterey, CA (September 2007), 63; доступно на http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.185.907&rep=rep1&type=pdf.
Смотри так же Объединенный комитет начальников штабов, Совместная публикация 3-13, «Информационные операции», II-9 для операций в киберпространстве.

4 Kirpekar, "Information Operations in Pursuit of Terrorists," 63.

5 World Nuclear Association, "Fukushima Accident 2011" (2013), доступно на http://www.world-nuclear.org/info/Safety-and-Security/Safety-of-Plants/Fukushima-Accident-2011/#.UXgxAIJAvIU.

Из-за сравнительно нового характера осуществляемых под покровительством государств международных кибератак, в этой статье рассматривается существующее международное договорное право, которое включает запреты на применение силы и право на самозащиту в смысле, в котором они сформулированы в Уставе Организации Объединенных Наций. Эти положения будут использованы для измерения степени, в которой компьютерные атаки могут считаться применением силы. Кроме того, будут использованы руководящие указания, основанные на подходе, базированном на оценке результатов, для формирования нормативной рамки, предназначенной для определения степени использования силы в каждом из случаев, рассмотренных в этой статье.

Статья 2(4) Устава ООН направлена на сохранение международного мира и порядка запретительными мерами. Статья предписывает «всем членам в их международных отношениях воздерживаться от угрозы использования или использования силы против территориальной целостности или политической независимости любого государства, или любым другим образом, несовместимым с целями Организации Объединенных Наций».[6]

Несмотря на добрые намерения этого заявления, туманная формулировка «использование силы» является вызовом при выполнении запретительных элементов Статьи 2(4). Эта идея была выдвинута в 1945 году на конференции в Сан-Франциско, когда бразильская делегация высказала мнение, что статья 2(4) должна включать и экономическое принуждение.[7]

Такая поправка к статье 2(4) никогда не стала реальностью, и невыясненное понятие силы далее было расширено в постановлении Международного суда по делу *Никарагуа против Соединенных Штатов* от 1986 года. Суд счел, что предоставление финансирования никарагуанским *контрас,* хотя и является вмешательством во внутренние дела Никарагуа, его нельзя квалифицировать как применение силы.[8] Это постановление предполагает, что инструменты силы следует оценивать на основе результатов их применения. К примеру, физическое принуждение с большой вероятностью может стать причиной уничтожения, нанесения ранений и эскалации, чем дипломатическое и экономическое принуждение. Поэтому, последствия применения вооруженной силы воспринимаются как более значимые, и поэтому вооруженные действия запрещены международным сообществом. По этим соображениям, применение силы разделено на спектр степеней тяжести, который охватывает случаи от использования вооруженной силы до случаев приме-

---

6 Устав Объединенных Наций, Статья 2, параграф 4.

7 Doc. 215, I/1/10, 6 U.N.I.C.O Docs. 559 (1945). See Doc. 784, I/1/27, 6 UNICO Docs. 334-35 (1945). Поправка, предложенная Бразилией, которая к запрету на угрозу применения силы прибавила бы слова «и от угрозы применения или применения экономических мер», была отвергнута 26 голосами против 2.

8 Военные и паравоенные действия (Никарагуа против США), 1986 M.C. 4,119 (27 июня 1986). В действительности Суд не применял статью 2(4); вместо этого при рассмотрении вопроса Суд использовал запрещение в обычном международном праве прибегать к использованию силы.

нения экономического принуждения. Таким образом, проблемой является расположение разнообразия компьютерных атак на шкале степеней использования силы.

Глава VII, статья 41 Устава ООН определяет спектр степеней применения силы, устанавливая конкретные действия, которые считаются использованием невооруженной силы. Случаи применения невооруженной силы включают «полный или частичный перерыв экономических отношений, железнодорожных, морских, воздушных, почтовых, телеграфных, радио или других средств сообщения».[9] Поскольку статья 41 использует формулировку «другие средства сообщения», она включает сетевые технологии в этот уровень невооруженной силы. Противоречие в этой легитимизации основанных на использовании компьютеров оружий появляется, когда сетевые технологии используются для действий, приводящих к физическим разрушениям.

Глава VII, статьи 39 и 51 Устава ООН дает разрешение на использование силы на основании конкретных критериев, установленных с целью сохранения мира и реализации права государств на самооборону. Статья 39 дает Совету Безопасности ООН «право определять существование любой угрозы миру, любого нарушения мира или акта агрессии».[10] Статья 51 разрешает использование силы формулировкой, что «Настоящий Устав ни в коей мере не затрагивает неотъемлемого права на индивидуальную или коллективную самооборону, если произойдет вооруженное нападение на Члена Организации».[11] В этой конструкции не используется понятие «применение силы». Вместо этого, формулировка «вооруженное нападение» дает государству право предпринимать ответные действия в целях самообороны.[12] В результате, Совет Безопасности является единственным органом, который может принимать решение о вооруженной реакции на события, которые угрожают миру. Государства, использующие разрешение на применение вооруженной силы по статье 51, должны дефинировать понятие «вооруженное нападение», прежде чем будут использовать какую бы то ни было силу. Для государств, предпринимающих действия в ответ на компьютерные атаки, трудность состоит в определении того, чем является компьютерная атака – угрозой миру, нарушением мира, актом агрессии или чем-то, что является прелюдией к предстоящему вооруженному нападению.

Компьютерные атаки являются вызовом для правовых рамок, касающихся запрета на использование силы и разрешений на ее применение в целях самообороны, поскольку они имеют широкий спектр последствий. Эти последствия варьируют от вызывания раздражения до физического разрушения. Одна из категорий компьютерных атак, которую определенно можно классифицировать как исполь-

[9] Устав Организации Объединенных Наций, статья 41.
[10] Устав Организации Объединенных Наций, статья 39.
[11] Устав Организации Объединенных Наций, статья 51.
[12] Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework,” *Columbia Journal of International Law* 37:3 (1999): 893.

зование силы, это атаки, которые напрямую становятся причиной нанесения физического ущерба.[13] Трудность состоит в том, к какой части диапазона степеней использования силы отнести компьютерные атаки, которые не приводят к физическому ущербу или ущербу для здоровья людей. Учитывая, что международное сообщество уже признает определенные действия использованием силы в определенной степени (например, экономическое принуждение или материальная поддержка повстанцев в чужом государстве), компьютерные атаки следует рассматривать подобным образом. Поэтому для описания разных порогов степени применения силы в конкретных атаках используются критерии Шмитта, основанные на характеристиках их последствий.

Для определения степени, в которой не приводящие к физическим разрушениям компьютерные атаки можно считать использованием силы, используются следующие характеристики: тяжесть, непосредственность, степень прямого действия, инвазивность, измеримость и предполагаемая легитимность.[14]

- Тяжесть указывает на то, приводит ли атака к физическим разрушениям или просто является дипломатическим принуждением. В этой характеристике учитывается определение в статье 2(4), которое включает влияние на территориальную целостность и политическую независимость государства.
- Непосредственность измеряет, насколько быстро осуществляется компьютерная атака. Для вооруженных нападений последствия наступают немедленно, как например, при взрыве бомб. Хотя компьютерные атаки осуществляются со скоростью распространения света, для проявления их последствий может быть необходимо время.
- Степень прямого действия измеряет то, как атака связана с ее последствиями. В случае традиционных вооруженных нападений ракеты причиняют разрушения. В случае экономического принуждения, например при манипулировании валютой, последствия атаки менее очевидны.[15]
- Инвазивность измеряет степень, в которой атака осуществляется внутри или вне страны. При традиционных вооруженных нападениях или в случаях использования силы, атаки осуществляются на территории страны.
- Измеримость подобна степени прямого действия, за исключением того, что она является мерой того, насколько легко измерить последствия определенного действия.

---

[13] Там же, 898.

[14] Там же, 898–99.

[15] Daniel Ikenson, *Appreciate This: Chinese Currency Rise Will Have a Negligible Effect on the Trade Deficit* (Washington, D.C.: CATO Institute, 2010), доступно на www.cato.org/publications/free-trade-bulletin/appreciate-chinese-currency-rise-will-have-negligible-effect-trade-deficit.

- И последнее, предполагаемая легитимность учитывает правовые нормы и соображения, которые являются основанием для принятия решения о проведении атаки.

Эта рамка полезна потому, что она дает комплексный набор принципов для анализа всех типов использования силы и всех типов нападений, в том числе и компьютерных атак. Эти шесть критериев особенно полезны при описании степени, в которой компьютерную атаку можно считать вооруженным или невооруженным использованием силы.

В случае компьютерных атак, уровень которых можно считать ниже порога применения силы или вооруженного нападения, в качестве дополнительной концепции к этой рамке рассматривается право на ответную реакцию в целях самообороны, которое основывается на следующих трех факторах:

- Атака является частью целостной операции, чья кульминация – это вооруженное нападение
- Атака является необратимым действием в предстоящем и неизбежном нападении
- Обороняющаяся сторона осуществляет ответную реакцию до нападения в последнем возможном временном окне возможностей.[16]

Эта вторая схема будет применена к случаям войны в Южной Осетии от 2008 года и действий подразделения 61398, так как в этих случаях не имели места физические разрушения. Поскольку при операции «Олимпийские игры» были физические разрушения, она будет оцениваться по критериям, основанным на последствиях, и в связи с ограничениями в законодательстве США и в международном праве на получение разрешения для таких действий. Кроме того, ответная реакция Ирана на эту КСО предполагает, что когда компьютеры причиняют физические разрушения, такие атаки можно рассматривать как применение силы ниже порога вооруженного конфликта.

Война в Южной Осетии 2008 года между Россией и Грузией

Самой большой проблемой, связанной с сетевыми компьютерными атаками, особенно с теми, что являются частью тайных операций, осуществляемых национальными государствами, является идентификация источника атаки. Даже если коммуникацию реально проследить до определенного компьютера, может оказаться невозможным доказать связь между этим компьютером и государством, на котором, как предполагается, лежит ответственность за осуществление атаки.[17] По этой причине, при анализе случая с войной 2008 года в Южной Осетии предполагается, что определенные подразделения органов российского государства спон-

[16] Schmitt, “Computer Network Attack and the Use of Force in International Law,” 908.

[17] Daniel Silver, “Computer Network Attack as a Use of Force under Article 2(4),” *International Law Studies* 76, специальное издание по теме “Computer Network Attack and International Law” (2002): 79.

сировали компьютерные атаки, направленные на грузинскую инфраструктуру. Сложность идентификации ответственного за это порождает проблему оценки легитимности компьютерных атак, которую можно обсуждать только *post facto*. Это приводит к такой ситуации, в которой оценку боевого киберпространства невозможно проводить в реальном времени.

В данном случае, предположение того, что источником атаки является Россия, основывается на нескольких соображениях. Первая причина – это то, что основной задачей этой статьи является рассмотрение покровительствуемых государством кибератак. Хотя Россия не взяла на себя ответственность за эти компьютерные атаки, но если приписать их России, то это будет прекрасным примером классифицирования КСА как вооруженного конфликта и применения силы. Вторая причина состоит в том, что когда компьютерная сетевая атака (КСА) используется для создания беспорядков в целевой стране, вероятность того, что виновник публично подтвердит свою причастность или что оставит следы, которые достоверно подтвердят его вину, мала.[18] Третьей причиной является то, что когда компьютеры используются в контексте традиционных военных операций, у государств нет мотивации начинать юридический спор только на основании компьютерных атак.[19] Это происходит потому, что военное нападение имеет гораздо более вопиющий характер, чем компьютерная атака. И последнее, когда государства осуществляют компьютерные атаки, скорее всего они попытаются скрыть свое участие или постараются, чтобы эти атаки выглядели инициированными хакерами, которые не имеют ничего общего с государством.[20]

Несмотря на то, что невозможно установить ответственного за такие атаки, увеличивается число свидетельств, что Россия развивает свои наступательные киберспособности. В марте 1998 года власти США нашли связь между попытками взломать компьютерные системы Пентагона, НАСА, Министерства энергетики США, частных университетов и исследовательских лабораторий. Все эти атаки исходили из компьютерной сети в России.[21] И еще раз, ответственность на этом поле сражений осталась неопределенной, а идентичность злоумышленников все еще неизвестна общественности. Другое событие, на этот раз в 2007 году, включало трехнедельную, политически направленную кибератаку против эстонских компьютеров. Как было установлено, компьютеры, с которых начались атаки, имели российские интернет-адреса и находились в государственных институциях.[22] Российские власти все так же отрицали свою причастность к этим атакам. В свете этих событий, в 1995 году российский генерал Владимир Слипченко за-

---

[18] Там же.

[19] Там же.

[20] Там же.

[21] "Cyber War; The Warnings?" *PBS Frontline* (2003); доступно на www.pbs.org/wgbh/pages/frontline/shows/cyberwar/warnings/.

[22] Timothy Thomas, "Nation-State Cyber Strategies: Examples From China and Russia," в *Cyberpower and National Security*, ed. Franklin D. Kramer, Stuart H. Starr, and Larry Wentz (Washington, D.C.: National Defense University Press, 2009), 475–76.

явил, что Академия генерального штаба сдвинула фокус работы от моделирования противоборства одних вооруженных сил против других, к моделированию противоборства одной системы с другой, что включает киберсистемы и некоторые другие, связанные с информацией системы.[23]

В августе 2008 года враждебные действия между Россией и Грузией по поводу отделившейся территории Южной Осетии достигли точки военного противоборства. 8 августа русские танки перешли границу Грузии. Однако, еще 7 августа были осуществлены компьютерные операции против компьютерных систем Грузии.[24] Целями кибератак были правительственные грузинские вебсайты и даже сайты посольств США и Соединенного Королевства. Первоначально атака исходила из русских IP адресов.[25] Даже если этот инцидент и не был напрямую связан с российскими государственными ведомствами и вооруженными силами, он привел к киберблокаде, которая очень удачно способствовала успешному наступлению российских вооруженных сил.[26] Поэтому эта кибератака рассматривается как акт вооруженного конфликта, поскольку она является элементом операции, который подготовил пространство боевых действий для российского вторжения в Грузию.

С точки зрения тяжести последствий результаты этой кибероперации были незначительными. Никто не был убит вследствие прямого результата операции, также не было нанесено никакого материального ущерба. КСА против Грузии во время конфликта в Южной Осетии точнее всего характеризуется понятием блокада дигитальной информации. Чтобы понять это в контексте международного права, можно обратиться к декларации 3314 ГА ООН, в которой сказано, что блокада портов или береговой линии считается актом агрессии.[27] В данном случае не препятствовалось поступлению в страну никаких физических товаров. Однако, дигитальная блокада прервала информационный поток и заменила его российской пропагандой в период, когда конфиденциальность, интегритет и наличие информации являются основными приоритетами.

В течение этой компьютерной атаки были повреждены вебсайты, содержащие важную информацию, и Интернет коммуникации были забиты с использованием технологии флуда (переполнения). Атаки привели в нерабочее состояние вебсайты

---

[23] Там же, 476.

[24] Енекен Тикк и др., «Кибератаки против Грузии: уроки в области права», доклад, опубликованный в Совместном центре повышения квалификации в области кибероборо-ны, Таллин, Эстония (ноябрь 2008), 4; доступен на http://www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf.

[25] Jeffrey Carr, "The Rise of the Non-State Hacker," в *Inside Cyber Warfare: Mapping the Cyber Underworld* (Sebastopol, CA: O'Reilly Media, 2009), 15–17.

[26] Richard A. Clarke and Robert K. Knake, "Why Cyber Warfare is Important," in *Cyber Warfare: The Next Threat to National Security and What to Do About It* (New York: HarperCollins, 2010), 18–21.

[27] Дефиниция агрессии, резолюция Генеральной ассамблеи ООН 29/3314, Аннекс, U.N. Doc. A/RES/29/3314/Annex (14 декабря 1974).

президента, парламента, правительства и министерства иностранных дел Грузии.[28] Отсутствие доступа к официальной информации, исходящей из правительства Грузии, ограничило жизненно важное распространение информации от государственных органов к обществу. Дополнительным элементом этой атаки стало то, что она заставила Национальный банк Грузии прервать предоставление электронных услуг на десять дней.[29]

Степень прямого действия кибератак в контексте военного вторжения России на территорию Грузии так же подкрепляет точку зрения, что эти атаки являются использованием вооруженной силы. Хотя единственным серьезным последствием КСА было нарушение коммуникаций, но оно случилось в такое время, когда коммуникация была жизненно важной для грузинского правительства.[30] Получилось так, что атаки продолжались всего несколько дней, начиная с 7 августа 2008.[31] Эта небольшая продолжительность, которая совершенно точно совпала с вторжением России в Южную Осетию, указывает на прямое действие, связывающее ущерб, нанесенный кибератакой, с ущербом, нанесенным российскими вооруженными силами. В любой другой момент такая дигитальная блокада была бы бессмысленной, но временная близость к реальным боевым действиям наводит на мысль, что это было дигитальным актом вооруженного конфликта. Другая точка зрения состоит в том, чтобы рассматривать кибератаку как часть военной операции, совершенно так же, как создание помех радарам или прерывание коммуникаций способствует целостному успеху операции.

Измеримость и инвазивность этой операции ограничены только в киберпространстве. Поскольку метод атаки состоял в нарушении сервисов и повреждении вебсайтов, единственное дигитальное «вторжение», которое имело место, существовало только на компьютерах, которые предоставляли хостинг следующим URL: www.president.gov.ge (вебсайт грузинского президента); www.nbg.gov.ge (Национальный банк Республики Грузия); и www.mfa.gov.ge (Министерство иностранных дел Республики Грузия).[32] Атаки типа отказ сервисов измеряются потоком информации к определенным вебсайтам. В качестве стандартного измерения, средний поток Mb/s для атак на компьютеры, которые были защищены программным обеспечением Kaspersky Labs, в 2011 году был 70 Mb/s.[33] Согласно информации фирмы, обеспечивающей компьютерную безопасность, которая наблюдает за Интернет трафиком, во время атак на грузинские вебсайты поток информации достиг среднего значения в 211.66 Mb/s, но имелись пики в 814.33 Mb/s, которые в среднем продолжались два часа и пятнадцать минут, но достигли пиковой про-

[28] Thomas, “Nation-State Cyber Strategies.”
[29] “Cyber War; The Warnings?”
[30] Там же.
[31] Там же.
[32] Там же.
[33] Yury Namestnikov, “DDos Attack in Q2 of 2011,” *Securelist* (29 August 2011); доступно на www.securelist.com/en/analysis/204792189/DDoS_attacks_in_Q2_2011.

должительности в шесть часов.[34] Сравнение измеренной интенсивности атак на Грузию со средней интенсивностью подобных атак наводит на мысль об исключительно хорошо организованных и рассчитанных действиях. И в заключении, параметры измеримости и инвазивности кибератаки против Грузии дают основание думать, что эта атака была осуществлена при полном согласовании с российскими вооруженными силами, и таким образом, является применением силы и квалифицируется как вооруженный конфликт.

Предполагаемая легитимность этой атаки напрямую связана с порогом применения силы, установленного в Уставе ООН. Текущее прочтение статьи 41 предполагает, что нарушение цифровых коммуникаций является международно признанным использованием невооруженной силы. Эта предположительная правовая рамка подразумевает, что поскольку компьютерная атака не привела к физическому ущербу, она не является актом применения вооруженной силы, а скорее актом использования невооруженной силы.

По причинам, упомянутым выше, критерии Шмита дают лучшее понимание использования невооруженной силы в контексте компьютерных атак. Действия, посредством которых российские власти дистанцировали себя от националистического хакерского сообщества, дали Кремлю возможность правдоподобно отрицать свою причастность, в то же время получая выгоду от пассивной поддержки и стратегических результатов действий хакеров.[35] Хотя согласно статье 41, акт компьютерной атаки является невооруженным использованием силы, непосредственность, степень прямого действия, инвазивность и измеримость данной атаки дают основание считать эту атаку актом вооруженного конфликта.

И в заключение, если кибератаки в 2008 году во время войны в Южной Осетии действительно исходили от российского правительства, их следует считать актом вооруженного конфликта. Атаки были рассчитаны на инвазивное действие, которое напрямую являлось информационной блокадой непосредственно накануне военной интервенции. При наличии таких характеристик, данная атака определенно нарушает запрет статьи 2(4) на использование силы и квалифицируется как акт вооруженного конфликта по смыслу статьи 51 о праве на самооборону.

Stuxnet – киберэквивалент ракет точного наведения

Лучшей тайной операцией является та операция, о которой никто, никогда, ничего не знает. Закон о национальной безопасности США от 1947 года дефинирует тайную операцию как действие или действия государственных органов Соединенных Штатов, направленные на оказание влияния на политические, экономические или военные условия за границей, при которых роль правительства США не будет

[34] Jose Nizario, "Georgia DDoS Attacks—A Quick Summary of Observations," Arbor Networks (12 August 2008); доступно на http://asert.arbornetworks.com/2008/08/georgia-ddos-attacks-a-quick-summary-of-observations/

[35] Thomas, "Nation-State Cyber Strategies."

очевидной или не будет публично подтвержденной.[36] Это определение находится в прямом конфликте с запретом на использование силы, сформулированном в статье 2(4) Устава ООН. Оказание влияния на политические, экономические или военные условия в другой стране по сути есть нарушение политического суверенитета государства, и как таковое является актом использования силы. Вооруженная это сила, или невооруженная, может быть предметом споров. Поэтому, высшей целью тайных операций, направленных на осуществление физических разрушений, это оставаться необнаруженными, или позволяющими правдоподобно отрицать причастность.

Как становится очевидным из определения Международного суда по делу Никарагуа против Соединенных Штатов, даже если тайные операции будут раскрыты, можно претендовать, что они находятся ниже порога вооруженного конфликта. Это означает, что несмотря на отсутствие ясности терминов «вооруженный» или «атака», государства соглашаются, что не все военные действия являются вооруженным конфликтом.[37] Можно сказать, что компьютерная атака Stuxnet относится к категории военных нападений, которые явным образом нарушают политический суверенитет государства, но не являются вооружённым конфликтом. Поэтому она является отличным примером для анализа тайных компьютерных операций, проводимых против национальных государств, поскольку это случай, при котором абсолютно точно известно, кто несет ответственность за нападение, и при котором кибератака является явным использованием силы.

Операция «Олимпийские игры» началась в 2006 году во время второго срока администрации Джорджа У. Буша и продолжалась до ноября 2010 года, в течение первого срока Обамы (хотя компьютерный код имел встроенную дату самоуничтожения 24 июня 2012).[38] Самые ранние этапы разработки Stuxnet-а включали слои проверки программного кода на предмет того, не нарушает ли это кибероружие международное право во время вооруженных конфликтов.[39] Кроме того, идея этой компьютерной программы была не только помешать ядерным амбициям Ирана; она была спроектирована для оказания воздействия на лучшие научные и военные умы Ирана.[40] Дизайнеры Stuxnet-а сделали ее так, чтобы проблемы, порожденные ее действием, выглядели как небрежный инжиниринг или отказ механического оборудования. Такие неясные причины подвергали стрессу и увеличивали нестабильность рабочего персонала Натанза.[41] Программа Stuxnet имела несколько разных вариантов, которые воздействовали на разные системы завода для обогащения урана и имели разные последствия. Разработчики Stuxnet постоянно

[36] SEC. 503 [50 U.S.C. §413b] (para e).
[37] Устав Организации Объединенных Наций, статья 39.
[38] David Sanger, *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power* (New York: Crown Publishers, 2012), 202.
[39] Там же, 193.
[40] Там же, 199.
[41] Там же.

меняли режимы атаки, создавая новые версии вируса.[42] Конечным результатом были физические разрушения и психологическое давление на иранское государство.

Основанные на результатах аналитические правила классификации дают две возможности для категоризации этой атаки. В зависимости от точки зрения результаты могут поддерживать или отвергать интерпретацию этого события как вооруженная атака. Масштаб физического ущерба, причиненного этой атакой, ограничен значительными повреждениями центрифуг для обогащения урана, находящихся на заводе для обогащения урана в Натанзе. Таким образом, согласно одной интерпретации, эта компьютерная атака являлась актом применения вооруженной силы, запрещенным статьей 2(4).

Червь Stuxnet был обнаружен на компьютерах по всему Ближнему Востоку и в таких удаленных странах, как Индонезия и Соединенные Штаты. Хотя работа компьютерных систем в этих странах была нарушена, никакого физического ущерба не последовало. Это означает, что проектировщики атаки сделали все возможное, чтобы ограничить деструктивные элементы червя только внутри Ирана. Дизайнеры встроили в программу автономную логику, которая инициировала деструктивный участок только при успешной идентификации правильного компьютера в правильной сети.

То, что эта программа была активна в течение четырех лет, предполагает уровень решимости использовать силу, соответствующий вооруженному конфликту. При принятии решения, является ли данное применение силы вооруженным конфликтом, критерий непосредственности предполагает, что это событие действительно является вооруженным нападением, поскольку оно продолжалось с конца второго срока администрации Буша и в начале срока администрации Обамы. Хотя фактор непосредственности предполагает, что использование Stuxnet было вооруженным конфликтом, другие элементы программы Stuxnet дают основание думать иначе.

Кинетические результаты атаки Stuxnet никоим образом не похожи на результаты использования ракет или бомб. Данная атака имела прямой результат, выражающийся в том, что в урановых центрифугах на ядерном сооружении Ирана появились неисправности. Несмотря на физический ущерб, причиненный вирусом, повреждения происходили таким образом, что никто из людей не пострадал. Скорость вращения центрифуг увеличивалась и уменьшалась в течение определенного времени месяца, что приводило к их повреждению, причем неисправности казались результатом того, что иранцы купили некачественное оборудование, или результатом неправильного монтажа устройств.[43] В этом смысле, боевая часть кибероружия использовала гуманные средства ниже порога традиционных кинетических вооруженных нападений.

---

[42] Там же.
[43] Там же, 199.

Эффект операции Stuxnet можно измерить двумя параметрами: распространением вспышки заражения и физическим ущербом, причиненным ею. Доклад по сетевой безопасности фирмы Symantec указывает на то, что из 100 000 зараженных этим вирусом компьютеров во всем мире 67 000 географически находились в Иране.[44] Этот факт подкрепляет мнение, что это было рассчитанное и целенаправленное использование силы. Кроме того, эта программа разрушила одну тысячу центрифуг в Натанзе (11 процентов от общего числа в то время) и вызвала хаос, который напряг инженерно-технический состав и, похоже, замедлил обогащение необходимого количества урана в период от 2006 до 2010 года.[45]

Основным является вопрос, было ли получено законным образом разрешение на проведение этой операции. Поскольку Stuxnet был совершенно очевидным случаем применения силы, следующий элемент анализа направлен на предполагаемую легитимность действий правовых структур США, которые разрешили проведение этой операции. Благодаря факту, что это была тайная операция, она попадала под действие правил и законов, регулирующих проведение таких действий. Глава V Закона о национальной безопасности от 1947 года дает описание процедур, обеспечивающих подотчетность разведывательной деятельности. Единственным субъектом, имеющим право разрешать проведение тайных операций, является президент Соединенных Штатов, и ему дано такое право только тогда, когда такие действия необходимы в поддержку идентифицируемых внешнеполитических целей США и необходимы для обеспечения национальной безопасности Соединенных Штатов.[46] Кроме того, каждое такое решение президента должно быть отражено в опубликованном документе, который соответствует следующим требованиям: письменный документ должен быть издан в рамках сорока восьми часов с момента принятия решения на проведение тайной операции; определение не может разрешать проведение тайной операции, которая уже была осуществлена; каждое такое определение конкретизирует ведомство, агентство или государственный субъект США, которым разрешено принимать участие; определение указывает, есть ли третья сторона, кроме правительства США, которой разрешено действовать; и последнее, такое определение не может разрешать какие бы то ни было действия, которые нарушали бы конституцию Соединенных Штатов.[47]

В случае с вирусом Stuxnet, предложения о проведении тайной операции против сооружения по обогащения урана в Иране исходили от Стратегического командования США и Агентства Национальной Безопасности. Президент Буш ощущал, что кибератака является лучшим вариантом для разрешения проблемы ядер-

---

[44] Nicolas Falliere, Liam O'Murchu, and Eric Chien, "W32.Stuxnet Dossier," Symantec Security Response (February 2011); доступно на www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf.

[45] Lukas Milevski, "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly* 63 (2011): 69.

[46] SEC. 503 [50 U.S.C. §413b] (para a).

[47] SEC. 503 [50 U.S.C. §413b] (para a), 1–5

ных амбиций Ирана, чем традиционные военные или дипломатические подходы.[48] Когда Барак Обама стал президентом, он решил передать контроль за операцией разведывательному сообществу и поэтому пересмотрел и актуализировал набор указаний, связанных с операцией Stuxnet так, чтобы они позволяли США оказывать влияние на политику, экономику и военное состояние другой страны в мирное время.[49] Поэтому, поскольку кибератака Stuxnet основывается на существующих правовых документах, регламентирующих проведение тайных операций, можно считать, что она законосообразна и соответствует правовым нормам вооруженного конфликта.

Stuxnet элемент тайной операции под кодовым названием «Олимпийские игры» можно считать азбучным примером использования компьютерной сетевой атаки, которая попадает в категорию, находящуюся ниже порога вооруженного нападения. Этот вывод неординарен, поскольку червь Stuxnet причинил физический ущерб заводу для обогащения урана другого суверенного государства, а ответной реакции или даже протеста не последовало. В ноябре 2010 года президент Ирана сделал заявление, что начало полноценной работы атомной электростанции в Бушере откладывается по техническим причинам. Stuxnet и Натанз вообще никогда не упоминались в этой связи.[50] Чтобы понять фундаментально новый характер этого случая, давайте заменим компьютерную атаку нападением ракет точного наведения. Различия между средством и результатами огромны. Отличие между этими двумя случаями применения силы состоит в том, что если были бы использованы ракеты, это привело бы к международному кризису, поскольку ракеты уничтожили бы не только центрифуги для обогащения урана. Результат компьютерной атаки имел две стороны. Она задержала осуществление программы по обогащению урана в заводе в Натанзе в Иране, и она ввела в практику новый способ применения силы через киберпространство.

Нерешенные проблемы – китайский шпионаж против бизнеса США

Существует разновидность кибератак, которая в настоящее время находится ниже уровня применения силы, запрещённого статьей 2(4), и гораздо ниже порога вооруженного конфликта. Это кибератаки в целях шпионажа. В данной работе в качестве примера для оценки цифрового шпионажа используются сведения о существовании подразделения 61398 Народно-освободительной Армии Китая. При рассмотрении этого случая предполагается, что не существует никаких правовых ограничений или запретов, относящихся к цифровому шпионажу. Международное право вооруженных конфликтов неприменимо к этой ситуации, поскольку акт цифрового шпионажа третируется таким же образом, как и традиционный шпио-

[48] SEC. 503 [50 U.S.C. §413b] (para e), 191.
[49] SEC. 503 [50 U.S.C. §413b] (para e).
[50] Gary D. Brown, "Why Iran Didn't Admit Stuxnet Was an Attack," *Joint Force Quarterly* 63 (2011): 70.

наж. В некоторых аспектах цифровой шпионаж поднимает такие же проблемы, как компьютерные преступления, совершаемые негосударственными акторами.

Хотя применение международного права вооруженных конфликтов к таким случаям ограничено, основанные на результатах критерии, перечисленные выше, проливают свет на диапазон и масштаб ущерба, наносимого кибершпионажем. Согласно одному докладу независимой компании по компьютерной безопасности «Мандиант», за семь лет подразделение 61398 украло информацию у 150 компаний и накопило более ста терабайтов данных.[51] Если двадцать терабайт отпечатать на бумаге, для перевозки эту бумагу надо будет загрузить на колонну больших фур длиной в двадцать миль.[52] Явление цифрового шпионажа находится под мониторингом уже продолжительное время и напрямую связывается Народно-освободительной Армией (НОА). Такая практика является кражей в особенно больших размерах интеллектуального капитала бизнеса США и подрывает его конкурентоспособность. Поэтому тяжесть можно оценивать только по характеру украденной информации и ее влиянию на прибыльность бизнеса.

Все факторы, основанные на результатах критериев, за исключением тяжести последствий, поддерживают точку зрения, что это вооруженное нападение. Используя уровни классификации информации, связанной с национальной безопасностью, Исполнительный приказ 12958 дает указания, которые позволяют измерить значение для США украденной информации:

- Атака типа 1 создает помехи или неудобства обороне или экономической безопасности Соединенных Штатов.
- Атака типа 2 причиняет ущерб обороне или экономической безопасности США.
- Атака типа 3 причиняет серьезный ущерб обороне или экономической безопасности США.
- Атака типа 4 причиняет исключительно большой ущерб обороне или экономической безопасности США.
- Атака типа 5 причиняет критически тяжелый ущерб обороне или экономической безопасности США.[53]

Таким образом, в какой степени шпионская атака категоризируется как вооруженное нападение, зависит от классификации украденной информации.

И тут снова возникает дилемма оценки *post facto*. Во-первых, надо найти ответственного за кибератаку, и затем надо определить степень применения силы. В

[51] Mandiant APT 1, “Exposing One of China’s Cyber Espionage Units” (2013); доступно на http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.

[52] Joel Brenner, *Calm Before the Storm*, Foreign Policy (2011), доступно на www.foreignpolicy.com/articles/2011/09/06/the_calm_before_the_storm.

[53] Mark B. Treadwell, “When Does an Act of Information Warfare Become an Act of War? Ambiguity in Perception,” U.S. Army War College Strategy Research Project (1998), 16–17; доступно на www.dtic.mil/cgi-bin/GetTRDoc?AD=ada345572.

случаях кражи информации оценка потенциального значения терабайтов украденной информации может быть длительным и сложным процессом, и в большинстве случаев кража информации не дотягивает до уровня вооруженного нападения. Если эти атаки не запрещены статьей 2(4) и не подлежат оценке по международному праву вооруженных конфликтов, тогда ничто не препятствует государствам принимать участие в таких действиях. Прецедент, созданный действиями подразделения 61398 предполагает, что цифровой шпионаж остается вне правого регулирования, поскольку он не является ни применением силы, ни актом вооружённого конфликта.

Заключение

При применении международного права вооруженных конфликтов всегда возникают три вопроса: Является ли данный акт вооруженным конфликтом? Что это за конфликт? И последнее, что из себя представляют участники конфликта? В этой статье ищется ответ на первый вопрос. Однако, при этом рассматривается только *jus ad bellum* (право на войну) при компьютерных сетевых операциях. Кроме того, каждый случай компьютерной атаки, который проходит без правовых или политических последствий, создает прецедент, согласно которому такая форма международного поведения становится приемлемой.

Существует множество неразрешенных вопросов, возникающих на этом новом поле сражений, в том числе и вопрос о правовой структуре, которая третирует *jus ad bellum* при компьютерных атаках. Принципы необходимости, определенности и пропорциональности в отношении автономно распространяющихся компьютерных программ являются огромным полем коллективной озабоченности. Что следует считать участниками войны при компьютерной атаке – компьютеры, программное обеспечение или программистов, и какими правами располагают эти объекты? Одним из основных методов для распространения компьютерного кода является использование умышленного обмана, что есть нарушение законов, запрещающих мошенничество. Поскольку киберпространство состоит из компьютеров, являющихся собственностью компаний, находящихся в других странах, несут ли эти компании ответственность за то, что они обеспечивают материальную поддержку кибератаки? Кроме того, следует ли считать киберконфликты международными или локальными конфликтами? Все эти вопросы остаются неразрешенными, и поскольку общества по всему миру во все большей степени зависят от информации и технологической инфраструктуры, которая ее поставляет, мы должны развивать конвенциональное понимание войны и международное право в целях разрешения вопросов и озабоченностей, порожденных покровительствуемыми государствами компьютерными атаками.

Литература

Brenner, Joel. *Calm Before the Storm*. Foreign Policy, 2011.

Brown, Gary D.. "Why Iran Didn't Admit Stuxnet Was an Attack." *Joint Force Quarterly* 63 (2011): 70.

Carr, Jeffrey. "*The Rise of the Non-State Hacker*." In *Inside Cyber Warfare: Mapping the Cyber Underworld*, 15-17. Sebastopol, CA: O'Reilly Media, 2009.

Clarke, Richard A., and Robert K. Knake. "*Why Cyber Warfare is Important*." In *Cyber Warfare: The Next Threat to National Security and What to Do About It*, 18-21. New York: HarperCollins, 2010.

Cyber War; The Warnings?. PBS Frontline, 2003.

Definition of Aggression, United Nations General Assembly.

Doc. 215 In *6 U.N.I.C.O Docs.*, 1945.

Doc. 784 In *6 UNICO Docs.*, 1945.

Exposing One of China's Cyber Espionage Units. Mandiant APT 1, 2013.

Falliere, Nicolas, Liam O'Murchu, and Eric Chien. *W32.Stuxnet Dossier*. Symantec Security Response, 2011.

Fukushima Accident 2011. World Nuclear Association, 2013.

Ikenson, Daniel. *Appreciate This: Chinese Currency Rise Will Have a Negligible Effect on the Trade Deficit*. Washington, D.C.: CATO Institute, 2010.

Information Operations In *Joint Pub*. Joint Chiefs Of Staff, 2006.

Kirpekar, Ulhas. *Information Operations in Pursuit of Terrorists* In *Naval Postgraduate School*. Monterey, CA, 2007.

Milevski, Lukas. "Stuxnet and Strategy: A Special Operation in Cyberspace?" *Joint Force Quarterly* 63 (2011): 69.

Military and Paramilitary Activities. Nicaragua v. U.S., 1986.

Namestnikov, Yury. *DDos Attack in Q2 of 2011* In *Securelist*., 2011.

Nizario, Jose. *Georgia DDoS Attacks—A Quick Summary of Observations* In *Arbor Networks*., 2008.

Sanger, David. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. New York: Crown Publishers, 2012.

Schmitt, Michael N.. "Computer Network Attack and the Use of Force in International Law: Thought on a Normative Framework." *Columbia Journal of International Law* 37, no. 3 (1999): 893.

Silver, Daniel. *Computer Network Attack as a Use of Force under Article 2(4)* In *International Law Studies* ., 2002.

Thomas, Timothy. "*Nation-State Cyber Strategies: Examples From China and Russia*." In *Cyberpower and National Security*, 475-76. Washington, D.C.: National Defense University Press, 2009.

Tikk, Eneken. *Cyber Attacks Against Georgia: Legal Lessons Identified*. Tallinn, Estonia : Cooperative Cyber Defense Center of Excellence, 2008.

Treadwell, Mark B.. *When Does an Act of Information Warfare Become an Act of War? Ambiguity in Perception* In *U.S. Army War College Strategy Research Project*., 1998.

United Nations Charter., 1945.