4 Государственная политика и управление: учебник: в 2 ч. /Л. В. Сморгунов, А. П. Альгин, И. Н. Барыгин [и др.]; под ред. Л. В. Сморгунова. –Ч. 1: Концепции и проблемы государственной политики и управления. – М.: РОССПЭН, 2006. – 381 с.

5 Конституция Республики Казахстан принята на республиканском референдуме 30 августа 1995 года/ Ведомости Парламента Республики Казахстан, 1996 г., N 4, ст. 217 с изм. и доп. от 01.01.2023//// https://adilet.zan.kz/rus/

6 Мухитдинов Е.Н. Правовые основы формирования и функционирования института омбудсмена (уполномоченного по правам человека) в Казахстане и за рубежом: международно-правовые аспекты. Дисс. PhD. Алматы, 2009. – 140 с.

7 Конституционный закон Республики Казахстан «Об Уполномоченном по правам человека в Республике Казахстан» от 5 ноября 2022 года № 154-VII ЗРК// https://adilet.zan.kz/rus/docs/Z2200000154#z190

ПРИМЕНЕНИЕ МЕЖДУНАРОДНОГО ПРАВА В КИБЕРПРОСТРАНСТВЕ: СОВРЕМЕННЫЕ ТЕНДЕНЦИИ КИБЕРБЕЗОПАСНОСТИ

Қадыржанова Т. С., магистрант ЕНУ имени Л.Н. Гумилева, г. Астана

В последние годы киберпространство ускорилось в направлении верховенства права, и роли международного права в управлении киберпространством уделяется все больше внимания. С 2013 года международное сообщество достигло важного принципиального консенсуса относительно применения международного права к киберпространству. Однако между сторонами все еще существует много различий в том, в отношении чего может применяться международное право и как его применять к киберпространству. Начало применения международных правил и предписаний, а также формирование и конструирование международного порядка на этой основе становится «новой нормой» в киберпространстве. Уникальные атрибуты киберпространства, а также различия между странами, особенно крупными державами, с точки зрения идеологии, ценностей и реальных национальных интересов определяют, что разногласия вокруг применения международного права к проблемам киберпространства неизбежно будут долгосрочными и сложными.

«Киберпространство» (cyberspace), в результате современной научно-технической революции, оказывает беспрецедентное влияние на человеческую жизнь. В этом «пятом пространстве» человеческой жизни за пределами суши, океана, воздушного пространства и космического пространства люди полагаются на мыши и экраны для реального обмена информацией и взаимных обменов, которые часто совпадают с реальным миром. Но, с другой стороны, виртуальная и глобальная природа киберпространства существенно отличает его от других традиционных пространств. Отсюда следует вопрос: какой кодекс поведения необходимо установить в этом пространстве? Кто должен сформулировать эти кодексы поведения? Что касается этого вопроса, то развитие концептуального понимания и практики прошло несколько этапов эволюции. С момента изобретения Интернета и до 1990-х годов доминирующей концепцией было рассматривать киберпространство как «автономную систему» невмешательства, выступать за «саморегулирование» киберпространства и выступать против распространения различных правительственных мер контроля в реальном мире на киберпространство. [1]

Однако с быстрым расширением базы пользователей сети и усложнением состава пользователей продолжают возникать различные незаконные действия и угрозы безопасности, такие как нарушение сетевых прав, сетевые вирусы и хакерские атаки, и состояние невмешательства в «саморегулирование» в киберпространстве стало неустойчивым. В этом контексте с конца 1990-х годов так называемое «возвращение государства» в киберпространство становится все более очевидным, и страны все

активнее участвуют в управлении киберпространством посредством разработки различного внутреннего законодательства и политики. [2]

Подобно тому, как сфера национальной деятельности распространилась на воздушное и космическое пространство, породив новые отрасли международного права, такие как право воздушного пространства и космическое право, существование государств в киберпространстве также должно регулироваться соответствующими нормами международного права. В последние годы ряд инцидентов, оказавших значительное международное влияние, таких как уход Google из Китая в 2010 году, инцидент с «Prism Gate» в 2013 году и судебное преследование правительством США пяти китайских солдат за участие в «киберэкономическом шпионаже» в 2014 году, вызвали вопрос о том, какой порядок и правила должны быть установлены в киберпространстве. Вопрос о том, какие правила следует применять. Можно сказать, что киберпространство, таким образом, вступило в новую стадию, когда постепенно укреплялось соответствующее международное законодательство и незаметно возникло международное верховенство права.

В вышеупомянутом процессе развития нетрудно увидеть четкую основную линию, то есть киберпространство все больше переходит от невмешательства к правилам и верховенству закона. Это связано с тем, что развитие киберпространства, особенно негативные и даже разрушительные последствия различных угроз кибербезопасности для реального мира, не позволяют стране продолжать оставаться в стороне от этого, и необходимо активно формулировать «правила игры», чтобы справиться с этим и продвигать киберпространство с беспорядочный к упорядоченному. С другой стороны, поскольку киберпространство, по сути, является глобальным пространством, ни одна страна не может решать смежные вопросы в области управления киберпространством в одиночку, что определяет, что соответствующие «правила игры» включают не только внутренние законы и нормативные акты, сформулированные каждой страной в отдельности, но и правила международного права, разработанный каждой страной в сотрудничестве. Суверенные государства вошли в киберпространство и стали важным субъектом кибердеятельности, так что международные отношения и международный порядок в реальном мире начали распространяться на киберпространство, что неизбежно требует, чтобы международное право играло важную роль в построении порядка в киберпространстве. В «Международной стратегии для киберпространства», опубликованной в 2011 году, правительство США впервые предложило концепцию «верховенства закона в киберпространстве» и подчеркнуло: «Давние международные нормы, которые определяют поведение государств в мирное время и в конфликтах, также применимы к киберпространству». [3]

Хотя вышеупомянутая позиция США исходит из перспективы защиты их собственных интересов, пропаганда применения международного права к киберпространству отражает объективные потребности построения международного порядка в киберпространстве. На этой основе Группа правительственных экспертов ООН по информационной безопасности в июне 2013 года достигла документа, оцененного как «эпохальный консенсус». [4] В документе указывается, что применение международного права, особенно Устава ООН, имеет важное значение для поддержания международного мира и стабильности, и содействия созданию открытой, безопасной, мирной и безбарьерной среды в области информационно-коммуникационных технологий. Вышеупомянутый консенсус был широко принят в ООН и на других международных форумах. В результате наведение порядка в киберпространстве неотделимо от применения международного права, которое стало общепринятой концепцией в международном сообществе. Соответствующий консенсус, достигнутый международным сообществом в отношении применения международного права к киберпространству, положил начало пути киберпространства к международному верховенству права, что, несомненно, приветствуется. Однако следует понимать, что по сравнению с

большинством областей международных отношений и международного права международное верховенство права в киберпространстве все еще находится в начальном состоянии, и у международного сообщества все еще есть большие разногласия по поводу того, какие нормы международного права могут применяться и как применять к киберпространству. Различия и конфликты между странами по поводу применения международного права к киберпространству касаются не только того, как существующее международное право применяется в киберпространстве, но и того, следует ли «адаптировать» новые нормы международного права к этому новому виртуальному пространству. [5]

США и другие западные страны впервые подняли вопрос о применении международного права в киберпространстве и в основном подчеркнули применение существующего международного права в киберпространстве. Например, в «Международной стратегии США по киберпространству» 2011 года предлагалось: «Разработка национальных норм поведения в киберпространстве не требует воссоздания обычного международного права и не сделает существующие нормы международного права устаревшими». [6] В сентябре 2012 года юрисконсульт Государственного департамента США, выступил с речью на тему «Международное право в киберпространстве», дополнительно разъяснив соответствующие позиции правительства США. [7]

В новой версии «Стратегии кибербезопасности ЕС», опубликованной в феврале 2013 года, ЕС также неоднократно выступал за применение норм, принципов и ценностей международного права в реальном пространстве к киберпространству, но не поддерживает разработку новых специальных международно-правовых документов. [8] Западные страны в основном делали упор на международное право в области прав человека и применение норм международного права, касающихся применения силы. В «Международной стратегии киберпространства» США 2011 года впервые было предложено, чтобы основные принципы, которые поддерживают нормы киберпространства, включали защиту основных свобод, уважение к частной жизни, свободу от преступности и право на самооборону. США сосредоточились на вопросах международного права, связанных с применением силы в киберпространстве, в том числе на том, может ли страна осуществлять право на самооборону от кибератак, а также на применении правил международного гуманитарного права к кибератакам. «Таллиннский справочник», подготовленный при поддержке НАТО и опубликованный в 2013 году, в основном изучает право на применение силы и правил международного гуманитарного права в киберпространстве. [9]

Акцент западных стран на вышеупомянутой системе международного права отражает отношение этих стран к тому, как строить международный порядок в киберпространстве, особенно к тому, как достичь надлежащего баланса между свободой и безопасностью. Например, западные страны всегда энергично выступали за «свободу Интернета» и выступали за применение международного права в области прав человека, особенно положений о защите свободы выражения мнений, в киберпространстве. Этот момент был четко выражен в «Стратегии кибербезопасности ЕС» 2013 года: «Для поддержания открытости и свободы киберпространства те нормы, принципы и ценности, которые поддерживаются ЕС в реальном обществе, также должны использоваться в киберпространстве. Основные права, демократия и верховенство закона должны быть защищены в киберпространстве». Пропаганда применения норм международного права в отношении применения силы соответствует политической тенденции западных стран полагаться на свою сильную политическую, экономическую и военную мощь (включая их ведущие преимущества в милитаризации сетевых технологий) и все больше придавать значение односторонним военным действиям для решения внешние киберугрозы и поддерживать свою собственную кибербезопасность. С этой целью, под флагом регулирования «кибервойны», эти страны, с одной стороны, используют право прибегать

к силе, особенно право на самооборону, предусмотренное в Уставе ООН, в качестве правовой основы для своих односторонних военных операций, а с другой стороны, используют международное гуманитарное право для сдерживания своих собственных возможных внешних кибератак. [10]

Следует признать, что применение существующего международного права в киберпространстве обладает определенной неизбежностью и рациональностью. Формирование киберпространства в основном основано на современных коммуникационных технологиях Интернета, и с юридической точки зрения некоторые виды деятельности, которыми люди занимаются с помощью этой новой технологии, принципиально не отличаются от аналогичных видов деятельности, которые осуществляются с помощью традиционных средств. Например, Интернет стал основным средством распространения и обмена современной информацией после газет, радио и телевидения. Поэтому трудно утверждать, что положения международного права в области прав человека о защите свободы распространения и обмена информацией (включая свободу выражения мнений) не применяются к распространению информации, осуществляемые через Интернет. С широким использованием сетевых технологий в военной области кибератаки стали часто используемым средством ведения боевых действий в современной войне. В этом случае, по-видимому, нет оснований утверждать, что положения международного гуманитарного права, ограничивающие средства и методы ведения войны, такие как принцип различения военных и гражданских целей во враждебных действиях не применимы к «кибервойне». Применение существующего международного права в киберпространстве должно быть всеобъемлющим и сбалансированным. Основные принципы национального суверенитета, невмешательства во внутренние дела и неприменения силы, признанные в Уставе ООН, являются не только краеугольными камнями существующего международного права и международных отношений, но и должны стать основой будущего международного порядка в киберпространстве. Особенно по мере того, как страны все активнее участвуют в управлении киберпространством, применение принципа национального суверенитета в киберпространстве является императивом. Вытекающий из этого принцип киберсуверенитета является важным краеугольным камнем применения международного права в киберпространстве.

По сравнению с вопросом о том, какие существующие международные нормы могут быть применены к киберпространству, вопрос о том, как эти нормы международного права могут быть применены к киберпространству является более сложным. Это связано с тем, что различные уникальные атрибуты киберпространства неизбежно поднимут много новых вопросов о применении международного права. Как указано в «Международной стратегии киберпространства» США: «Уникальные характеристики сетевых технологий требуют дальнейших усилий по разъяснению того, как применяются соответствующие нормы международного права, и какие другие понимания необходимы для дополнения соответствующих правил». [11]

В настоящее время существует множество глобальных, региональных и двусторонних механизмов консультаций и диалога, связанных с международным управлением в киберпространстве. Например, «Интернет-корпорация по присвоению имен и номеров» (ICANN), созданная в октябре 1998 года, в основном отвечает за распределение пространства IP-адресов, назначение идентификаторов протоколов, управление общими доменными именами верхнего уровня и национальными и региональными системами доменных имен верхнего уровня, а также управление системой корневых серверов. В настоящее время это одно из самых влиятельных учреждений в международном механизме управления Интернетом. Кроме того, «Лондонский процесс», инициированный британским правительством в 2011 году, к настоящему времени провел четыре международные конференции по киберпространству в Лондоне (2011), Будапеште (2012), Сеуле (2013) и Гааге (2015). Будучи единственной в мире программой многостороннего

диалога и дебатов, посвященной построению порядка в киберпространстве, Лондонский процесс окажет влияние на будущее международное управление киберпространством и даже на международные отношения в более широком смысле, что нельзя игнорировать. С глобальным развитием Интернета с 1990-х годов все больше и больше стран, особенно развивающихся, выражают недовольство ситуацией в распределении сетевых ресурсов и управлении ими несколькими крупными странами и настоятельно требуют соответствующих реформ, включая передачу ответственность за управление сетью перед межправительственными международными организациями, такими как ООН или Международный союз электросвязи. Фрагментация международных механизмов управления и платформ в киберпространстве затруднила конкретную и систематическую кодификацию и разъяснение норм международного права в киберпространстве, что, в свою очередь, привело к применению соответствующих норм международного права, также демонстрирующих все более очевидное состояние фрагментации. Главным проявлением является то, что даже при одинаковом поведении в киберпространстве страны часто расходятся во мнениях относительно применения соответствующих норм международного права. Например, кибератака, предпринятая хакером из страны *A* против страны *B*, может быть признана разными странами как акт киберпреступности, акт кибертерроризма, применение силы, упомянутое в пункте 4 статьи 2 Устава ООН, или акт силового нападения, упомянутый в статье 51. [12]

В настоящее время международное сообщество располагает большим числом глобальных, региональных и двусторонних механизмов консультаций и диалога, связанных с управлением киберпространством, все из которых способствуют созданию международного кодекса поведения в киберпространстве на различных уровнях и в различных областях. Например, новая группа правительственных экспертов Организации Объединенных Наций по информационной безопасности, созданная в 2014 году в соответствии с соответствующими резолюциями Генеральной Ассамблеи Организации Объединенных Наций, в июле 2015 года приняла новый консенсусный документ *A/70/174*, предлагающий 10 добровольных, рекомендательных и ответственных национальных норм поведения в киберпространстве, и на основе консенсусного документа *A/68/98* от 2013 года в нем дополнительно выдвинуто 6 мнений о том, как международное право применяется к использованию информационно-коммуникационных технологий, что позволяет добиться нового прогресса в применении международного права в сетевом пространстве. На основе обширных консультаций между странами Генеральная Ассамблея Организации Объединенных Наций приняла декларацию принципов кодекса поведения в киберпространстве, которая поможет продолжать добиваться консенсуса между странами и обеспечит руководство международным порядком в киберпространстве. Будучи учреждением, занимающимся постепенным развитием и кодификацией международного права, Комиссия международного права Организации Объединенных Наций также может играть важную роль в применении международного права к киберпространству.

Список литературы:

1. Джон Б. Декларация о независимости киберпространства http://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.

2. Инь Ц. Механизм управления сетевой информационной безопасностью США и его последствия // Исследование права и бизнеса № 2, 2013, стр. 138-145.

3. Белый дом: Международная стратегия киберпространства: процветание, безопасность и открытость в сетевом мире, 2011 http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

4. Джен С. Государственный департамент США, Заявление о консенсусе, достигнутом Группой правительственных экспертов ООН по вопросам кибербезопасности, 2013 г., // http://www.state.gov/r/pa/prs/ps/2013/06/210418.htm.

5. Группа правительственных экспертов ООН по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности, доклад от 24 июня 2013 года, Документ ООН A/68/98, п. 19. // https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/66/PDF/N1337166.pdf?OpenElement.

6. Белый дом: Международная стратегия киберпространства: процветание, безопасность и открытость в сетевом мире, 2011 // http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

7. Гарольд Х. Международное право в киберпространстве // USCYBERCOM Ft. Мид, Мэриленд, 2012 г. // https://harvardilj.org/wp-content/uploads/sites/15/2012/12/Koh-Speech-to-Publish1.pdf.

8. Резолюция Европейского парламента от 12 сентября 2013 года о Стратегии кибербезопасности Европейского Союза: открытое, безопасное и защищенное киберпространство (2013/2606(RSP)) // https://www.europarl.europa.eu/doceo/document/TA-7-2013-0376_EN.html.

9. США: Международная стратегия киберпространства: процветание, безопасность и открытость в сетевом мире (2011) // http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

10. Майкл Н. Атака на компьютерную сеть и применение силы в международном праве: размышления о нормативной базе // 37 COLUM. J. TRANSNAT'L L. – С. 885.

11. ASEAN Региональный форум, Краткий отчет сопредседателей, (2012) // http://aseanregionalforum.asean.org/files/library/ARF%20Chairman's%20Statements%20and%20Reports/The%20Nineteenth%20ASEAN%20Regional%20Forum,%202011-2012/10%20-%20Co-Chairs%20Summary%20Report%20.pdf.

12. Устав ООН // https://www.un.org/ru/about-us/un-charter/full-text.

НАУЧНО-ПРАКТИЧЕСКОЕ ОБОСНОВАНИЕ О ВАЖНОСТИ ФРАГМЕНТАЦИИ МЕЖДУНАРОДНОГО ПРАВА

Қапаров А.С., ассистент Высшей школы права, Университет КАЗГЮУ имени М.С. Нарикбаева, г. Астана

«*Ничто не стоит на месте все меняется, таков закон жизни и те кто смотрят только в прошлое или только на настоящее, бесспорно пропустят будущее*» - Джон Ф. Кеннеди. Приведенная цитата прекрасно описывает любые аспекты и вопросы, которые происходят в жизни нашего общества. В той или иной степени, данная цитата повествует современную ситуацию в международном праве, где научное сообщество разделилось на два лагеря по вопросу об актуальности такого явления как фрагментация международного права. Первый лагерь объясняет об опасности фрагментации и ее последующей тенденции, которая может вполне себе развить и модернизировать самостоятельность некоторых международно-правовых режимов, а также распространение постулатов международного права на те или иные сферы отношении, которые не то, чтобы рассматривались международным сообществом, а вовсе не признавались ими как подходящими для международно-нормативного регламентирования. Отмечается негативное влияние фрагментации в виде формировании специализации и дробленность международного права в ключевых сферах как права человека, международная торговля, образование новых международных организаций и к ведению конфронтации государств, норм и режимов. Второй лагерь видит фрагментацию международного права как доказательным фактом жизнестойкости и модернизации международного права. Создание