

Proceedings of IYSC, (2021), vol. 10

Journal homepage: <http://journals.sdu.edu.kz/index.php/iysw>

2021 International Young
Scholars' Conference



РАСПРОСТРАНЯЕТСЯ ЛИ СУВЕРЕНИТЕТ НА КИБЕРПРОСТРАНСТВО?

Миятова Сая

M. Narikbayev KAZGUU University

Абстракт

Ключевой идеей данной работы является анализ таких понятий как «государственный суверенитет» и «киберпространство». Особенности киберпространства и неоднозначность определения территории в международном праве затрудняют возможность определить, может ли киберпространство подпадать под юрисдикцию стран международного сообщества. В рамках статьи автором анализируются разные подходы и теории, касающиеся распространения суверенитета на киберпространство. Вместе с тем, автор делает предположения, касающиеся рисков и последствий при распространении суверенитета на изучаемое пространство. Автором были использованы такие методы научного исследования, как анализ и синтез, определение понятий, сравнение - сходство и различие, индуктивный метод. В статье также сформулирован вывод, указывающий на необходимость принятия международной конвенции в целях урегулирования отношений в киберпространстве.

Ключевые слова: *киберпространство, суверенитет, юрисдикция, интернет, экстратерриториальность, всеобщее достояние.*

Распространяется ли суверенитет на киберпространство?

1. Киберпространство и суверенитет

Суверенитет – это фундаментальный принцип международного права. Он является краеугольным камнем в осуществлении власти и распространении юрисдикции на всей территории суверенного государства. Как принято считать, территорией государства на сегодняшний день считаются сухопутное, водное и воздушное пространства. Но как насчет нового явления XXI века – киберпространства? Ведь оно неосвязаемо и виртуально.

На протяжении истории развития международного права понятия «территория», «территориальный суверенитет» менялись и усложнялись новыми явлениями. Между тем мнения ученых разделились: одни считают, что «киберпространство» не должно относиться ни к какому режиму и должно представлять из себя совершенно новое измерение, к которому не могут быть применены существующие нормы и правила, другие же утверждают, что несмотря на его децентрализованность и экстратерриториальность, оно нуждается в управлении и техники, поддерживающие деятельность Сети установлены на поверхности территории, на которую распространяется юрисдикция соответствующей страны. Усложняет ситуацию и то, что на данный момент киберпространство не регулируется каким-либо международным договором. Ввиду его технологических особенностей, действия, совершаемые в киберпространстве может охватывать сразу несколько стран. Тогда в каких случаях можно говорить о нарушении суверенитета? Ведь возможны случаи, когда для защиты своего суверенитета необходимо будет посягнуть на чужой. Однако, считаю, что прежде чем анализировать квалификацию нарушения суверенитета, необходимо определить, можем ли мы относить государственный суверенитет и к киберпространству, что и является целью данной статьи.

1.1. Территориальный суверенитет в международном праве

Территориальный суверенитет является основным концептом и понятием в международном праве. Судья Хубер в деле об острове Пальма отметил: «Sovereignty in the relations between States signifies independence. Independence in regard to a portion of the globe is the right to exercise therein, to the exclusivity of any other States, the functions of a State».¹ Территориальное верховенство составляет основу территориальной компетенции по осуществлению суверенной власти. Носитель территориального верховенства правомочен независимо осуществлять полную власть на соответствующей территории.² То есть, для того, чтобы юрисдикция государства распространялась на его территорию, в т.ч. на пользование, владение и распоряжение территорией, государство должно обладать суверенитетом. Вместе с тем, отмеченная юрисдикция распространяется на все субъекты и объекты, находящиеся на территории государства. Национальная юрисдикция осуществляется за пределами государственной территории только в случае, если данная территория не подпадает под исключительную территориальную юрисдикцию другого носителя власти или норма международного права не запрещает распространение юрисдикции.³ Это означает, что другие государства не могут осуществлять юрисдикцию и распространять суверенитет за пределами своей территории.

Что же входит в государственную территорию? И. Лукашук в своей работе определил следующий состав территории, на который распространяется суверенитет: сухопутная территория (поверхность суши), включая острова; водная территория (акватория), включающая внутренние воды и территориальное море; земные недра; воздушное пространство, расположенное над перечисленными пространствами.⁴

¹ Reports Of International Arbitral Awards 838. (1928). *Island of Palmas case*. UN. Max Huber.

² Витцтум, В. Г. (2015). *Международное право*. Москва: Инфотропик Медиа, 323-343.

³ Ibid. 343

⁴ Лукашук, И.И. (2005). *Международное право*. Казань: Волтерс Клувер, 406.

Суверенитет, распространяемый на каждое из этих пространств, различается особенностью регулирования. К примеру, согласно ст. 1 Конвенции о международной гражданской авиации «Договаривающиеся государства признают, что каждое государство обладает полным и исключительным суверенитетом над воздушным пространством над своей территорией»⁵. Вместе с тем, несогласованный пролет через воздушное пространство государства является серьезным нарушением международного права.⁶

Иная норма предусмотрена в Конвенции ООН по морскому праву: «Суверенитет прибрежного государства распространяется *за пределы* его сухопутной территории и внутренних вод»⁷. Более того, суда всех государств, как прибрежных, так и не имеющих выхода к морю, пользуются правом мирного прохода через территориальное море (при соблюдении условия Конвенции).⁸

Здесь мы замечаем, что понятие «территориального суверенитета» не является однозначным и ограниченным, и зависит от особенностей изучаемого пространства. Следовательно, анализируя вопрос распространения суверенитета на киберпространство нельзя забывать о неидентичности правового режима определенной среды.

1.2. Киберсуверенитет

В настоящее время, существуют несколько распространенных теорий на тему суверенитета в киберпространстве.

Сторонники независимости киберпространства – ученые, которые утверждают, что суверенитет не распространяется на киберпространство считают, что оно

⁵ Конвенция о международной гражданской авиации. Доступно по ссылке: https://www.un.org/ru/documents/decl_conv/conventions/pdf/chicago_conv.pdf.

⁶ Engvers, A. (2001). *The Principle of Sovereignty in the Air to what extent can it be upheld against aerial intruders?* Lund: Lund University Press, 54

⁷ 2 статья Конвенции ООН по морскому праву. Доступно по ссылке https://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_r.pdf

⁸ Ibid, 17 статья

относится к *res communis omnium* и не должно подпадать под какой либо суверенитет.⁹ Так, по мнению исследователей, киберпространство должно иметь статус территорий с международным режимом, иными словами, быть одним из всеобщего достояния человечества, коим считаются открытое море, космическое пространство, включая Луну и другие небесные тела на которых не распространяется территориальный суверенитет государств. Однако, стоит отметить, что на сегодняшний день отсутствует единое, официально закрепленное определение «всеобщего достояния» как такового. Это затрудняет задачу отнесения киберпространства в ряд *res communis omnium*. Организация экономического сотрудничества и развития определяет «всеобщее достояние» как «природные ресурсы за пределами национальной юрисдикции, такие как океаны, космическое пространство и Антарктика»¹⁰. Между тем, существует несколько причин, по которым киберпространство едва ли относится к кругу всеобщего достояния. Во-первых, как правило, они регулируются международными договорами¹¹, во-вторых, по каждому из этих пространств определено, что они не являются частью государственного суверенитета¹², более того, ни одно государство не имеет какой-либо власти над этими пространствами. Как известно, ввиду трансграничной сущности киберпространства, оно управляется не только государствами, но и межправительственными и некоммерческими организациями, как ICANN, Internet Society и др.¹³ Стоит отметить, что многие подобные организации и компании зарегистрированы в США, и гипотетически, при таком раскладе США имеет

⁹ Shmitt, N. and Vihul, L. (2017). Respect for Sovereignty in Cyberspace. *Texas law review*, 1645

¹⁰ United Nations Statistics Division, Global Commons Definition, Доступно по ссылке <https://stats.oecd.org/glossary/detail.asp?ID=1120#:~:text=Global%20commons%20are%20natural%20assets,Nations%2C%20New%20York%2C%201997.>

¹¹ Конвенция ООН по морскому праву, которая вступила в силу в 1994 году; Договор о принципах деятельности государств по исследованию и использованию космического пространства, включая Луну и другие небесные тела, вступивший в силу в 1967 году; и Договор об Антарктике от 1959 года. Известно, что на данный момент киберпространство не регулируется каким-либо всеобъемлющим договором.

¹² Например, ст.4 Договора об Антарктике, гласящая: «Никакие действия или деятельность ... не создают никаких прав суверенитета в Антарктике». Или ст.2 Договора о космическом пространстве (1967): «Космическое пространство, включая Луну и другие небесные тела, не подлежит национальному присвоению ни путем провозглашения на них суверенитета, ни путем использования или оккупации, ни любыми другими средствами».

¹³ Терентьева, Л.В. (2019) Принципы установления территориальной юрисдикции государства в киберпространстве. *МГЮА*, 124

большую власть над киберпространством. Однако США не являются сторонниками данной теории, что заметно из решений по делу *American Civil Liberties Union v. Reno*. В данном споре судом было постановлено, что Интернет соединяет 159 стран и более 109 млн. пользователей, следовательно, США не имеют суверенитета над ними, поскольку деятельность, имеющая место в киберпространстве, не ограничивается юрисдикцией США и распространяется за ее пределы.¹⁴

Еще одна из причин, по которой киберпространство не может быть свободным от суверенитета заключается в том, что на данный момент проблематично сделать зону сети Интернет предметом многостороннего соглашения, без ее разграничения на национальные сегменты, где бы осуществлялась юрисдикция каждого отдельного государства.¹⁵ В отношении территорий с международным режимом преимущественно действуют нормы и принципы международного права и, соответственно, реализуются публично-правовые отношения, тогда как киберпространство является площадкой не только публично-правовых, но и частноправовых интересов, подпадающих под национальную юрисдикцию того или иного государства.¹⁶

Исследователи, мнения которых противоположны упомянутой теории утверждают, что государства должны обладать киберсуверенитетом, поскольку данное пространство нуждается в регулировании и может существовать только при помощи управления определенных субъектов. Данные субъекты, в свою очередь, относятся к определенной территории и находятся под ее юрисдикцией.

Одним из главных проявлении суверенитета государства является его юрисдикция, поскольку именно юрисдикция определяет власть государства в пределах определенной территории. Дискуссия о внетерриториальности интернета и невозможности определения суверенитета государств по отношению к

¹⁴ *American Civil Liberties Union v. Reno*, 31 F.Supp. 2d 473, 484 (E. D. Pa. 1999).

¹⁵ *Ibid.* 13, 123

¹⁶ *Ibid.* 123

киберпространству породила такие доктринальные расхождения, как невозможность территориальных суверенов управлять киберпространством, для которого должна быть создана своя юрисдикция (или несколько юрисдикций)¹⁷; расхождение в определении государственных пространственных границ в связи с применением предписывающей, судебной и исполнительной юрисдикции в рамках киберпространства. Стоит отметить, что в соответствии с концептом «пространства» в международном праве, ученые Г.Еллинек, К.Фрикер отмечали, что теория пространства не означает, что территория является объектом собственности, а является пространством, в пределах которого государство осуществляет свою юрисдикцию.¹⁸ Пространство необязательно указывает территориальные единицы, но определяет *предел* территориальных границ. Следовательно, применение таких понятий как «территория государств», «территориальный суверенитет», «юрисдикция» не является противоречивым в том ключе, в котором они могут быть использованы в вопросах киберпространства, поскольку данные понятия регулярно обогащались и деформировались за счет выявления новых пространственных концептов в истории международного права. Развитие киберпространства способствовало тому, что на сегодняшний день понятие «территория государств» начала эволюционировать в виде включения новых пространственных единиц, не имеющих *территориального, осязаемого, плоскостного* аспекта.¹⁹ Следовательно, виртуальность киберпространства не является столь проблематичным для его включения в ряд территории, на которые распространяется территориальный суверенитет государств.

Вопрос распространения суверенитета на киберпространство отмечен и в Таллинском Руководстве 2.0. Правило №1.1 гласит, что хотя ни одно государство не может заявлять о своем суверенитете над киберпространством *per se*, они могут

¹⁷ Johnson, R.D. and Post, G. D. (1996). Law And Borders: The Rise of Law in Cyberspace. Stanford Law Review, 34

¹⁸ Каюмова, А. Р. (2016). *Уголовная юрисдикция в международном праве*. Казань: Волтерс Клувер, 48

¹⁹ Ibid.13, 127

осуществлять суверенные прерогативы в отношении любой кибер-инфраструктуры, расположенной на их территории, а также деятельности, связанной с этой кибер-инфраструктурой.²⁰ Кроме того, в ч.3 данного правила определено, что именно территориальный суверенитет дает возможность осуществлять юрисдикцию и над киберпространством, относящимся к территории определенного государства.

Апелляционный суд США в деле *Microsoft Corp. vs United States* постановил, что определяющее значение для разграничения территориальной и экстратерриториальной юрисдикции имеет место нахождения информации, к которой требуется осуществить доступ.²¹ Что касается способа определения, к какой территории относится киберпространство, М. Финнимор и Д. Холлис в своих трудах отметили, что одним из очевидных рычагов является то, что важнейшие элементы кибер-инфраструктуры являются физическими и осязаемы, как правило, закреплены на твердой земле.²² Серверы и подводные кабели, например, имеют осязаемое физическое существование; кабели закреплены, и находятся в определенной территории. Государства используют эти физические особенности киберпространства в целях определения, распространяется ли на него юрисдикция или нет.

Необходимо отметить и позицию КНР по данному вопросу – Китай признает распространение суверенитета на киберпространство, поскольку в Стратегии международного сотрудничества в киберпространстве от 2017 года КНР определила 4 основных принципов.²³ Это – принципы мира, суверенитета, совместного управления и общей пользы.

²⁰ Schmitt, M.N. (2017). Tallinn Manual 20 on the International Law Applicable to Cyber Operations. *Cambridge University Press*, Rule 1.1

²¹ *Microsoft Corp. v. United States* 829 F.3d 197 (2d Cir. 2016) Доступно по ссылке: <https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/>.

²² Finnemore, M. and Hollis, D.B. (2016). Constructing norms for global cybersecurity. *American journal of international law*, 460

²³ International strategy of cooperation on cyberspace (2017). Доступно по ссылке: http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm.

Заключая данную часть, стоит отметить, что, несмотря на существование расхождений по вопросам суверенитета в киберпространстве, нельзя отрицать следующие факты: для существования и функционирования, киберпространство должно контролироваться кем-то. Оно нуждается в физической структуре, как вышеуказанные серверы, кабели и ИКТ, которые установлены на территории государств; Любая информация и деятельность (например, финансовые операции) в киберпространстве регулируются законами в соответствующих странах. Например, Соединенные Штаты, наряду со многими другими странами, заявили о своей заинтересованности в предотвращении хранения и распространения детской порнографии, Франция заявила о своей заинтересованности в прекращении распространения нацистских памятных вещей, а Австралия заявила о своей заинтересованности в защите своих граждан от клеветнических заявлений.²⁴ В каждом из приведенных выше примеров судебные системы постановили, что информация, доступная лицу, находящемуся в этих соответствующих государствах через киберпространство, подпадает под действие законов этого соответствующего государства.²⁵ Следовательно, можно предположить, что суверенитет государства распространяется на киберпространство в той части, в которой оно находится на его территории и подпадает под его юрисдикцию.

2. Риски и последствия

Ввиду отсутствия всеобъемлющего договора, который регулировал бы киберпространство неизбежно противоречие «территориализации» киберпространства и фрагментации интернета.

Как отмечает К. Айкенсер, последствия неосязаемости данных бросают вызов традиционному международному праву в отношении юрисдикции. Международные

²⁴ Goldsmith, J. and Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World*. Oxford University Press, 147-161

²⁵ Ibid 24

юрисдикционные нормы в значительной степени основываются на суверенитете государств над определенной территорией и власти над людьми и вещами на ней, и они предполагают, что местоположение людей и вещей является конечным и познаваемым. Эра облачных вычислений - когда данные беспрепятственно пересекают границы, части одного файла могут существовать в нескольких юрисдикциях, а место хранения данных часто зависит от выбора частных компаний - поднимает новые и сложные вопросы для международного сообщества.²⁶

На сегодняшний день также неизвестно, какие явления и действия в киберпространстве могут нарушить суверенитет. Экспертная группа по подготовке Таллинского руководства считает, что квалификация нарушения суверенитета в киберпространстве зачастую основывается на понесенных ущербах. Однако они не смогли ответить на вопрос: «нарушается ли суверенитет в случае кибератак без какого-либо ущерба?» или «обязательно ли ущерб должен быть осязаемым и серьезным?». Поскольку в традиционном понимании нарушении суверенитета – его квалификация не всегда основывается на причиненном ущербе.

Экстратерриториальность киберпространства также является риском, поскольку в некоторых случаях обеспечение суверенитета одной страны может осуществляться только при его распространения за пределы суверенной территории.²⁷ К примеру, если информация о насильственной смене власти, которая может привести к массовым беспорядкам в одном государстве, находится на сервере другого государства. В таком случае в целях поддержания национальной безопасности государства могут посягнуть на суверенитет других стран.

²⁶ Eichensehr, K.E. (2017). Data extraterritoriality. *Texas law review*, 146.

²⁷ Шарифов, М. (2009). Суверенная власть в киберпространстве и в сетевом пространстве. *Современное право*, 42

Выводы

В заключение следует отметить, что детерриториальность киберпространства, несомненно, вызывает споры по отношению распространения на него суверенитета. Киберпространство **в целом** не может быть подчинено власти государств, поскольку по своей природе оно многогранно и в него вовлечены миллионы сетевых структур, которые расположены на самых разных частях мира. Более значим на данный момент вопрос разграничения этого пространства в реалиях территориальных юрисдикции. Исходя из анализа ясно, что киберпространство **на территории** суверенного государства нуждается в его регулировании и управлении. Отношения и деятельность в Сети попадают под юрисдикцию соответствующей страны, следовательно, киберпространство не независимо от суверенитета.

Таким образом, считается необходимой разработка международного договора в отношении основополагающих принципов и правил пользования киберпространством, который также будет разграничивать юрисдикцию и суверенную власть государств. Справедливо отмечают К. Браун и С. Кайа, что киберпространство не может быть предметом самостоятельного урегулирования ни в одном государстве, исходя только из существующих норм национального законодательства. Решить эту проблему можно лишь заключив соответствующий международный договор.²⁸

²⁸ Brown, K. and Kaye, S. (2006). The problems of International Finance Law And Electronic Commerce. *Sydney*, 56

Список использованной литературы:*Книги и научные статьи*

1. Витцтум, В. Г. (2015). Международное право. Москва: Инфотропик Медиа, 323-343.
2. Лукашук, И.И. (2005). Международное право. Казань: Волтерс Клувер, 406.
3. Engvers, A. (2001). *The Principle of Sovereignty in the Air to what extent can it be upheld against aerial intruders?* Lund: Lund University Press, 54
4. Goldsmith, J. and Wu, T. (2006). *Who Controls the Internet?: Illusions of a Borderless World.* Oxford University Press, 147-161
5. Brown, K. and Kaya, S. (2006). *The problems of International Finance Law And Electronic Commerce.* Sydney, 56
6. Shmitt, N. and Vihul, L. (2017). *Respect for Sovereignty in Cyberspace.* *Texas law review*, 1645
7. Каюмова, А. Р. (2016). *Уголовная юрисдикция в международном праве.* Казань: Волтерс Клувер, 48
8. Finnemore, M. and Hollis, D.B. (2016). *Constructing norms for global cybersecurity.* *American journal of international law*, 460
9. Eichensehr, K.E. (2017). *Data extraterritoriality.* *Texas law review*, 146.
10. Шарифов, М. (2009). *Суверенная власть в киберпространстве и в сетевом пространстве.* Современное право, 42
11. Терентьева, Л.В. (2019) *Принципы установления территориальной юрисдикции государства в киберпространстве.* МГЮА, 124
12. Johnson, R.D. and Post, G. D. (1996). *Law And Borders: The Rise of Law in Cyberspace.* Stanford Law Review, 34

Документы, кейсы и др.

13. Конвенция о международной гражданской авиации
14. Конвенция ООН по морскому праву
15. United Nations Statistics Division, Global Commons Definition. Доступно по ссылке:
<https://stats.oecd.org/glossary/detail.asp?ID=1120#:~:text=Global%20commons%20are%20natural%20assets,Nations%2C%20New%20York%2C%201997>
16. International strategy of cooperation on cyberspace (2017). Доступно по ссылке:
http://www.xinhuanet.com/english/china/2017-03/01/c_136094371.htm
17. Schmitt, M.N. (2017). Tallinn Manual 20 on the International Law Applicable to Cyber Operations. Cambridge University Press, Rule 1.1
18. Island of Palmas case [1928] 2 Reports Of International Arbitral Awards 838 (UN) (Max Huber). Доступно по ссылке https://legal.un.org/riaa/cases/vol_II/829-871.pdf
19. American Civil Liberties Union v. Reno, 31 F.Supp. 2d 473, 484 (E. D. Pa. 1999)
20. Microsoft Corp. v. United States 829 F.3d 197 (2d Cir. 2016) Доступно по ссылке:
<https://harvardlawreview.org/2016/12/microsoft-corp-v-united-states/>.