DOI 10.22394/1726-1139-2020-6-41-49

# Проблема определения объема суверенных полномочий государства в цифровую эпоху*

*Коростелёв С. В.*

Секретариат Совета Межпарламентской Ассамблеи государств — участников Содружества Независимых Государств, Санкт-Петербург, Российская Федерация, ksv1@iacis.ru

*РЕФЕРАТ*

Глобальная архитектура компьютерных сетей создает дилемму безопасности: в то время как современные информационно-коммуникационные технологии позволяют противникам оспаривать исключительную власть государств над «его собственным» киберпространством, следование традиционным представлениям о суверенитете, соответственно, может ограничивать возможности государств по активному противодействию вызовам и угрозам в глобальных сетях.

Целью исследования является определение возможных объемов применения традиционного территориального концепта суверенитета к деятельности государств в киберпространстве.

В статье раскрывается, что относительно деятельности государств и физических лиц в киберпространстве содержание принципа суверенитета определяется практическими императивами государств и зависит от затрагиваемой сферы межгосударственных и трансграничных взаимодействий. Так, например, для целей ведения боевых действий выделяются три уровня, на которых будут определяться объекты для поражения: физическая сеть, логическая сеть, пользователь сети. Для разработчиков, эксплуатантов и аналитиков сетей важны другие критерии, и, по ряду предложений, глобальная сеть может включать до семи уровней (физический, передачи данных, сетевой, транспортный, сеансовый, представления данных, приложений).

В работе показано, что, несмотря на исключительный характер правомочий и юрисдикции государства в отношении физического уровня киберпространства, его логический и социальный уровни открыты для трансграничных проявлений юрисдикции других государств на основе критерия близости. То есть для тех случаев, когда государства могут установить реальную связь с цифровыми объектами или онлайн-персонами, и, соответственно, осуществлять властные полномочия.

*Ключевые слова*: киберпространство; определение суверенитета; международное право; юрисдикция; публичный порядок; уровни киберпространства

**Для цитирования**: *Коростелёв С. В.* Проблема определения объема суверенных полномочий государства в цифровую эпоху // Управленческое консультирование. 2020. № 6. С. 41–49.

## The Problem of Shaping the Capacity of Sovereign Powers of a State in the Digital Age

*Stanislav V. Korostelev*

Secretariat of the Council of the Interparliamentary Assembly of the Commonwealth of Independent States, Saint-Petersburg, Russian Federation; ksv1@iacis.ru

*ABSTRACT*

The global architecture of computer networks poses a security dilemma: while modern information and communication technologies allow adversaries to challenge the exclusive power of states over “his own” cyberspace, following traditional notions of sovereignty, respectively,

* Статья подготовлена при поддержке гранта Российского фонда фундаментальных исследований (РФФИ) 19-011-00156 А «Легитимация вмешательства во внутренние вооруженные конфликты (международные правовые аспекты)».

may limit the ability of states to actively counter challenges and threats in global networks. The aim of the study is to determine the possible scope of application of the traditional territorial concept of sovereignty to the activities of states in cyberspace.

The article shows that regarding the activities of states and individuals in cyberspace, the scope of the principle of sovereignty is determined by the practical imperatives of states and depends on the sphere of interstate and cross-border interactions affected. Therefore, for example, for the purposes of warfare, there are three levels at which objects for destruction will be determined: physical network, logical network, network user. Other criteria are important for developers, operators and network analysts, and, according to a number of proposals, a global network can include up to seven levels (physical, data transfer, network, transport, session, data, applications).

The article demonstrates that despite the exceptional nature of the powers and jurisdictions of the state in relation to the physical level of cyberspace, its logical and social levels are open to cross-border manifestations of the jurisdiction of other states on the basis of the proximity criterion. That is, for those cases when states can establish a real connection with digital objects or online personalities, and, accordingly, exercise authority.

*Keywords*: cyberspace; determination of sovereignty; international law; jurisdiction; public order; levels of cyberspace

**For citing**: Korostelev S.V. The Problem of Shaping the Capacity of Sovereign Powers of a State in the Digital Age // Administrative consulting. 2020. No. 6. P. 41–49.

В настоящее время идет дискуссия о том, насколько широко могут толковаться пределы реализации суверенных компетенций в киберпространстве[1] и возможно ли проводить кибероперации, которые нарушают суверенитет другого государства.

Вопрос о том, как должно определять содержание термина «суверенитет» при расширяющемся взаимодействии в киберпространстве в настоящее время является одним из наиболее спорных вопросов современных международных отношений. Традиционное понимание суверенитета основано на постулате абсолютного контроля географически определенной территории, которая, очевидным образом, может быть делимитирована и демаркирована в процессе взаимодействий с другими суверенными акторами. Однако глобальная архитектура компьютерных сетей исключает расстояние и географию как факторы, абсолютно ограничивающие осуществление властных полномочий государствами, и деятельность не связанных с государствами субъектов. Это в свою очередь неизбежно создает дилемму безопасности: в то время как современные информационно-коммуникационные технологии (далее — ИКТ) позволяют противникам оспаривать исключительную власть государств над «его собственным» киберпространством, следование традиционным представлениям о суверенитете, соответственно, может ограничивать возможности государств по активному противодействию вызовам и угрозам в глобальных сетях. Также необходимо отметить, что нормативная концепция «суверенитета» является результатом взаимодействия моральной философии и теории права в отношении вопроса объяснения существования и функционирования правовых и политических систем. А юрисдикция — это эмпирическая концепция, которая описывает и объясняет процессуальные аспекты взаимодействий таких систем. В международном дискурсе эти два аспекта неизбежно рассматриваются совместно, но очень часто, по вине пропаганды, в общественном сознании происходит смешение понятий «суверенитет» и «юрисдикция».

[1] Впервые термин «киберпространство» был введен в оборот в 1984 г. в романе «Нейромант» Вильяма Гибсона, где раскрывалась попытка интеграции главного героя в киберпространство, где и руководители были ему неизвестны, для внесения в это пространство имеющейся у него информации. Концепция киберпространства раскрывалась через способ манипулирования общеизвестными фактами или опытом для получения новых смыслов. См.: [4].

Суверенные полномочия государств предоставляют им возможность устанавливать юрисдикцию в отношении лиц, совершающих преступления с трансграничными последствиями. Так, например, Уголовный кодекс Российской Федерации в ст. 11 устанавливает уголовную ответственность лиц, совершивших преступление на территории государства[1], а в ст. 12 — вне ее пределов[2], если преступление направлено против интересов Российской Федерации либо ее граждан или постоянно проживающих в России лиц без гражданства, а также в случаях против обязательств государства, закрепленных в международных договорах или иных документах международного характера в сфере уголовно-правовых отношений. Тем самым, государство заявляет о распространении своих властных полномочий за пределы физической территории, таким образом, оспаривая властные полномочия других субъектов международного права в пределах их собственной территории и в отношении подвластных им лиц. То есть происходит столкновение притязаний на осуществление суверенных правомочий.

Таким образом, можно согласиться с тем, что «компетенции государства определяются через присущее ему свойство суверенитета. В самом примитивном понимании «суверенитет» означает исключительную власть, осуществляемую государством в пределах своей территории и в отношении своего населения, и, которая, в некоторых случаях, может осуществляться экстерриториально. В более широком смысле «суверенитет» какого-либо государства следует понимать как меру согласия других участников международного общения с содержанием и способами реализации им своих властных полномочий» [2].

Для построения модели выхода из такой ситуации при защите национальных интересов предлагается исходить из двух крайних парадигм суверенитета [6]. Во-первых, обязанность уважения суверенитета является нормой международного права, нарушение которого является международно-противоправным деянием. В киберконтексте это может проявляться как посягательство на территориальный суверенитет в результате осуществления кибероперации органом государства или иными лицами, чье поведение может быть присвоено какому-либо государству, если физические последствия таких действий сказываются в пределах территориальной юрисдикции другого государства, например, в отношении критичных элементов инфраструктуры, в том числе информационно-коммуникационной инфраструктуры (далее — ИКИ), отдельных объектов, юридических или физических лиц. Так, например, посягательство на суверенитет имеет место при внедрении вредоносных программ в ИКИ другого государства.

Во-вторых, суверенитет по-прежнему является базовой правовой категорией, которая находится в основании организации современного международного порядка и обеспечивается нормами jus cogens, такими как запрет на применение силы, содержащийся в ст. 2 п. 4 и п. 7 Устава ООН, либо нормой обычного международного права о невмешательстве[3], с которой государства согласились как с со-

---

[1] В том числе в пределах территориального моря или воздушного пространства, на континентальном шельфе и в исключительной экономической зоне государства, на судне, приписанном к порту Российской Федерации, находящемся в открытом водном или воздушном пространстве вне пределов Российской Федерации, если иное не предусмотрено международным договором Российской Федерации, а также на военном корабле или военном воздушном судне Российской Федерации независимо от места их нахождения.

[2] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 02.12.2019) [Электронный ресурс]. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения: 21.12.2019).

[3] Принцип, касающийся обязанности в соответствии с Уставом ООН не вмешиваться в дела, входящие во внутреннюю компетенцию любого другого государства. Декларация о принципах международного права, касающихся дружественных отношений и сотрудничества между госу-

ставной частью вестфальского концепта суверенного равенства. Но в настоящее время запреты на применение силы и невмешательство во внутренние дела уже не обладают императивным характером jus cogens сами по себе вне единого контекста международной жизни, в основе которого лежит общий интерес безопасного сосуществования. Государство, конечно же, имеет право противодействовать угрозам, исходящим с территории других государств, для обеспечения собственной национальной безопасности. Такого рода деятельность может опираться на концепцию «суверенитет как обязанность»[1], впервые сформулированную в Докладе тысячелетия Генерального секретаря ООН[2], в котором поднимался вопрос соотношения международно-правовых принципов суверенитета и невмешательства.

Балансируя между этими двумя крайними воззрениями на концепцию суверенитета, можно выделять также ad hoc подходы к толкованию содержания суверенитета относительно деятельности государств и физических лиц в киберпространстве. С этой точки зрения суверенитет является принципом, содержание которого определяется практическими императивами государств и зависит от затрагиваемой сферы межгосударственных и трансграничных взаимодействий.

Но и в этом случае представляется очевидным, что проблема согласования интересов государств в киберпространстве, по существу, не является новой. На первый взгляд есть факт сосуществования юридически несопоставимых парадигм. Но если исходить из того, что нормы международного морского, воздушного и космического права также согласовывались, отталкиваясь от территориального аспекта концепции суверенитета, то и киберправо в значительной своей части также может быть описано и объяснено в тех же самых терминах.

В общем случае, органы государственной власти не делают выводов о том, что киберактивность сама по себе является нарушением суверенитета, даже если эти действия имеют место и/или их последствия сказываются в другом государстве, но только если при этом не затрагивается публичный порядок (не затрагиваются государственные функции государства-объекта вмешательства) и последствия такой активности в инфраструктуре и на территории другого государства не причиняют масштабного ущерба и вреда.

Именно покушение на публичный порядок (ordre public) и масштаб последствий определяют правовые и политические пороги для киберактивности в отношении конкретного государства.

Для определения таких порогов на государство возлагается политическое обязательство по публичному заявлению своих взглядов на то, как существующее международное право применимо к поведению акторов в киберпространстве.

Учитывая, что традиционное понимание суверенитета исторически доктринально связывается с осуществлением власти в географически определенном пространстве, сразу же возникает вопрос, в каком объеме его можно применить к киберпростран-

---

дарствами в соответствии с Уставом Организации Объединенных Наций. Резолюция Генеральной Ассамблеи ООН от 24 октября 1970 г. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/declarations/intlaw_principles.shtml (дата обращения: 16.12.2019); Декларация о недопустимости интервенции и вмешательства во внутренние дела государств. Резолюция 36/103 Генеральной Ассамблеи ООН от 9 декабря 1981 г. [Электронный ресурс]. URL: https://www.un.org/ru/documents/decl_conv/declarations/internal_affairs_decl.shtml (дата обращения: 03.12.2019).

[1] Сущность данной концепции заключается в том, что «суверенитет предполагает строгое соблюдение обязательств перед своим народом и наделение определенными международными привилегиями: государство, выполняющее основные обязательства по защите и обеспечивающее основные права человека, защищено от вторжения из-за рубежа». См.: [1].

[2] Мы, народы: роль Организации Объединенных Наций в XXI веке. Доклад Генерального секретаря, п.п. 215–219 [Электронный ресурс]. URL: http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N00/389/00/IMG/N0038900.pdf?OpenElement (дата обращения: 04.06.2015).

ству, в котором непрерывно осуществляются трансграничные взаимодействия. Не менее важным является вопрос, насколько эта деятельность подчиняется юрисдикции государств, если она осуществляется на основе технической инфраструктуры, не связанной с их территорией.

Киберпространство в некотором смысле является *res communis omnium* — общим достоянием человечества, в котором взаимодействия осуществляются на принципах взаимосвязанности, анонимности и простоты входа. Возможно, что как когда-то в международном морском праве были сформулированы принципы (свободы открытого моря), которыми руководствуются все участники деятельности в морских пространствах, в том числе, не имеющие выхода к морю, и установлен правовой режим для различных категорий морских пространств, сходным образом следует подходить к формированию правового режима киберпространства, состоящему из различных зон (слоев), объем правомочий государств в которых будет определяться в зависимости от масштаба связанности конкретной структуры интернета с территорией государства, — центрального элемента концепции суверенитета.

Сложность описания правового режима киберпространства коренится в его «многоуровневой» организации, где предмет описания, либо регулирования киберпространства, т. е. число таких назначаемых уровней зависит только лишь от целей обращения к нему. Киберпространство едино, но, например, для целей ведения боевых действий, выделяются три уровня, на которых будут определяться объекты для поражения: физическая сеть, логическая сеть, пользователь сети (cyber-persona)[1]. Для разработчиков, эксплуатантов и аналитиков сетей важны другие критерии, и, по ряду предложений, глобальная сеть может включать до семи уровней (физический, передачи данных, сетевой, транспортный, сеансовый, представления данных, приложений)[2].

Многоуровневая организация, в свою очередь, позволяет описать и объяснить особенности правового регулирования для деятельности в киберпространстве по сравнению с физическим географически определенным пространством: хотя технические компоненты, которые составляют основу глобальных компьютерных сетей, имеют уникальное физическое местоположение, оно само по себе лишь в исключительных случаях интересует пользователей киберпространства. Необходимость особого регулирования киберпространства формируют логический и социальный уровни, которые создают глобальную платформу для обмена информацией, услугами и осуществления практически безграничного числа видов деятельности без оглядки на границы между государствами. Но поскольку в международном сообществе все взаимодействия осуществляются относительно концепта государственного суверенитета, то возникает вопрос о применимости в киберпространстве традиционной нормы, содержащей абсолютный запрет каких-либо посягательств на территориальные правомочия государств, или необходимости ее толкования таким образом, чтобы была возможность учесть особенности организации киберпространства. В некоторых случаях в качестве точки отсчета для анализа структуры киберпространства и распределения властных полномочий акторов представляется возможным исполь-

---

[1] Joint Publication 3-12. Cyber Space Operations. Ch. I. 2. The Nature of Cyberspace [Электронный ресурс]. URL: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_12.pdf (дата обращения: 21.03.2020).

[2] Jerry C. Whitaker (ed), Systems Maintenance Handbook. 2nd edn. CRC Press LLC. 2002. Ch. 17 “Network Concepts” [Электронный ресурс]. URL: https://epdf.pub/electronic-systems-maintenance-handbook-second-edition.html (дата обращения: 15.12.2019); ГОСТ Р ИСО/МЭК 7498-4-99. Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Ч. 4. Основы административного управления. [Электронный ресурс]. URL: http://protect.gost.ru/v.aspx?control=8&baseC=-1&page=0&month=-1&year=-1&search=&RegNum=1&DocOnPageCount=15&id=124253&pageK=34DF434B-29DA-47D3-96C9-D7AB1D535D5D (дата обращения: 09.12.2019).

зование концепции «Человек в центре (Man-in-the-Middle)»[1], когда лицо, осуществляющее какие-либо действия вне зависимости от физического нахождения и осуществляемых функций, подчинено юрисдикции определенного государства.

В приведенных выше примерах, а также в аналогичных случаях мы видим разделение суверенных правомочий в отношении физически определенной территории государств (где могут храниться данные), и их правомочий в отношении данных. Хотя государство обладает юрисдикцией в отношении размещенной на его территории инфраструктуры и находящихся в ней данных, сами данные уже, как правило, не увязываются с его территорией. Как считает Комиссия Европейского союза, государства не обладают исключительными правами на регламентацию доступа к информации[2], в отличие от прав контроля государственной территории. Конечно же, это не относится к чувствительной правительственной информации. А собственно, правом на регулирование доступа к информации обладает государство, на территории которого предлагаются услуги и/или находятся пользователи информации.

В данном контекста очень полезным является рассмотрение проблемы реализаций суверенных правомочий в отношении ИКИ и данных правительством Эстонии. Предполагая, что ИКИ в пределах национальной территории может быть разрушена извне, правительство Эстонии реализовало концепцию «электронного посольства»[3]. В первом случае — это «физическое посольство», когда правительственная и иная важная для населения информация, например, о правах собственности, а также персональные данные хранятся на ресурсах, которые находятся на территориях дипломатических представительств Эстонии в дружественных государствах. Во-вторых, в случае «виртуального посольства» данные размещаются на частных облачных ресурсах.

Это положение свидетельствует о сосуществовании двух «параллельных» юрисдикций. Первая основана на принципе территориальности ИКИ, хранящей данные, другая — на территориальной доступности предлагаемых услуг и национальности или местожительства владельца данных. Поэтому подобно тому, как это сделано в морском праве, мы можем концептуализировать киберпространство как состоящее из разных зон — или слоев — суверенных полномочий, в зависимости от близости к сфере исключительной государственной власти, которая составляет ядро суверенитета.

Современная международная практика, равно как и национальное законодательство и судебные решения, касающиеся юрисдикции в отношении трансграничной деятельности, показывают, что, хотя государства подчеркивают исключительный

---

[1] См. например: [5].

[2] См. Предложения к правилам Европейского парламента и Совета по Европейскому ордеру о представлении и сохранности электронных доказательств в уголовных делах: «The data ordered through a European Production Order should be provided directly to the authorities without the involvement of authorities in the Member State where the service provider is established or represented. The Regulation also moves away from data location as a determining connecting factor, as data storage normally does not result in any control by the state on whose territory data is stored. Such storage is determined in most cases by the provider alone, on the basis of business considerations». Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on European Production and Preservation Orders for Electronic Evidence in Criminal Matters. COM/2018/225 final — 2018/0108 (COD). Chapter 1: Subject Matter, Definitions and Scope. Art. 1: Subject Matter [Электронный ресурс]. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN (дата обращения: 12.12.2019).

[3] Implementation of the Virtual Data Embassy Solution. Summary Report of the Research Project on Public Cloud Usage for Government, Conducted by Estonian Ministry of Economic Affairs and Communications and Microsoft Corporation [Электронный ресурс]. URL: https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf (дата обращения: 17.12.2019).

характер своих правомочий и юрисдикции в отношении физического уровня киберпространства в силу принципа территориальности, его логический и социальный уровни открыты для трансграничных проявлений юрисдикции других государств в силу самой структуры интернета. Можно утверждать, что киберпространства открыты для осуществления государственной власти на основе критерия близости, т. е. в тех случаях, когда государство может установить подлинную связь с цифровыми объектами или онлайн-персонами (пользователь сети (cyber-persona))[1], в отношении которых могут осуществляться властные полномочия.

Подобно критерию «подлинной связи», установленному Международным судом ООН в делах *Nottebohm*[2] и *Barcelona Traction*[3], используемому для определения того, может ли государство осуществлять экстерриториальную юрисдикцию, критерий близости описывает степень связи между данными или услугами, хранящимися за границей, и государством. Поэтому близость не устанавливает абсолютного критерия, а скорее относительного, в зависимости от конкретной ситуации и интересов соответствующих государств. Следующие критерии, установленные в случаях, касающихся экстерриториального доступа к данным, могут включать факторы для определения близости в случаях перекрывающихся притязаний на суверенитет: степень, в которой затрагиваются территория и интересы (последствия — вред, ущерб) конкретных государств, местоположение и национальность владельца данных, основная территория, с которой осуществляется доступ к данным, и на которую они адресуются, а в случае предоставления услуг — характер и масштабы связей поставщика услуг с конкретным государством. Существует точка зрения, что «неэффективность осуществления государственного контроля в сфере международного информационного обмена может быть связана с неадекватностью средств его осуществления, а не с отсутствием необходимости контроля. Нельзя не учитывать, что государственный контроль в той или иной области вводится в силу необходимости обеспечения реализации правовых норм, а не потому, что государство произвольно избирает область, в которой государственный контроль осуществлять будет несложно. В отношении международного информационного обмена необходимость государственного контроля обусловлена существованием запретов и ограничений на распространение информации» [3]. В этой позиции также подтверждается тезис о том, что пределы киберпространства и объем его регулирования и заявления суверенных правомочий определяются лишь самим затронутым государством самостоятельно путем заявления об этом через принятие нормативных актов и его возможностями по распространению своей юрисдикции вне национальной территории.

Неразвитость современного международного правового режима противодействия информационным угрозам и неопределенный объем суверенных полномочий государств в глобальных сетях объясняются тем, что международное сообщество обычно не ведет переговоры по разработке и заключению договоров для решения проблем до тех пор, пока их последствия, а не гипотетические возможности, не начнут ощущаться. Лишь проявление последствий какой-либо деятельности дает толчок к решению возникающих проблем. Так, например, «начало развития тяжелой воздушной авиации совпало с Первой мировой войной, во время которой была ясно продемонстрирована военная мощь самолетов для сбора разведывательных данных, нападения на наземные силы и бомбардировки вражеских городов. Результатом

[1] Joint Publication 3-12. Cyber Space Operations. Ch. I. 2. The Nature of Cyberspace.

[2] [Электронный ресурс]. URL: https://www.icj-cij.org/en/case/18/summaries (дата обращения: 16.12.2019).

[3] [Электронный ресурс]. URL: https://www.icj-cij.org/files/case-related/50/5389.pdf (дата обращения: 16.12.2019).

стал крайне ограниченный режим воздушного права, при котором любое вхождение в воздушное пространство страны без его разрешения следует рассматривать как серьезное нарушение ее суверенитета и территориальной целостности»[1]. Данное положение контрастирует с положениями космического права, которые определяют доступность космического пространства для использования всеми, поскольку в начале космической эпохи аппараты для исследования космоса не представляли угрозы для объектов на земле, в отличие от летательных аппаратов, несмотря на то, что и в одном и другом случае происходят пролеты над территорией государств. Именно отсутствие угрозы наземным объектам стало тем фактором, который определил, что находящиеся на орбите объекты находятся за пределами территориальных притязаний любой нации.

Что касается физического уровня киберпространства, то подконтрольность государству является абсолютно преобладающей по критерию территории в дискуссии об объеме суверенных правомочий. Это отражает международный консенсус о применимости международного права в киберпространстве, описанный Группой правительственных экспертов ООН в докладах за 2013[2] и 2015 гг.[3], в которых установлено, что суверенитет и правила юрисдикции государства применяются к ИКИ, расположенной на территории государства.

Так, например, п. «е» Правил поведения в области обеспечения международной информационной безопасности[4] подтверждает права и обязанности каждого государства, в соответствии с надлежащими нормами и правилами, в отношении законной защиты своего информационного пространства и критической информационной инфраструктуры от ущерба в результате угроз, вмешательства, атак и актов агрессии. То есть речь идет, прежде всего, о территориальных правомочиях государств. Очевидным образом следует предполагать, что суверенные правомочия государства не могут быть распространены на логический и социальные уровни интернета, и возможно говорить лишь о праве осуществления юрисдикции государства в ограниченном числе ситуаций, например, определенных в ст. 11 и 12 Уголовного кодекса России.

Государства регулярно отстаивают свое право на осуществление юрисдикции над компонентами физического уровня, например, устанавливая нормативные стандарты или требования безопасности. И также можно заявить, что какого-либо «информационного» суверенитета существовать не может вне пределов государственной территории. Не может же государство заявлять о праве устанавливать какие-либо правила в отношении информационного пространства, элементы инфраструктуры которого и, тем более, информация физически находятся вне его территориальной юрисдикции. Нельзя смешивать понятия «суверенитет» и «юрисдикция». И, следовательно, можно сделать вывод о том, что киберпространство едино, поскольку в противном случае государство не смогло бы присвоить ответственность за действия каких-либо международных акторов, если их действия осуществлялись в пределах физической территории другого государства, а последствия сказались на территории

---

[1] См.: U.S. Department of Defense Office of General Counsel. An Assessment of International Legal Issues in Information Operations. May 1999. P. 2 [Электронный ресурс]. URL: https://fas.org/irp/eprint/io-legal.pdf (дата обращения: 05.12.2019).

[2] Документ ООН A/68/98 [Электронный ресурс]. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N13/371/68/PDF/N1337168.pdf?OpenElement.

[3] Документ ООН A/70/174 [Электронный ресурс]. URL: https://undocs.org/ru/A/70/174 (дата обращения: 03.12.2019).

[4] Приложение к письму постоянных представителей Китая, Российской Федерации, Таджикистана и Узбекистана при Организации Объединенных Наций от 12 сентября 2011 года на имя Генерального секретаря. Документ ООН A/66/359 [Электронный ресурс]. URL: https://www.un.org/ga/search/view_doc.asp?symbol=A/66/359&Lang=R (дата обращения: 10.12.2019).

государства-объекта вмешательства. О том, что в этом вопросе существует согласие между большинством государств, даже теми из них, которые придерживаются совершенно полярных воззрений на объем прав и обязанностей государств в киберпространстве, можно найти подтверждение в практике государственных органов США и Китая.

## Литература


1. *Коростелёв С. В.* «Ответственность по защите» как политико-правовое обоснование актов применения силы в международных отношениях // Управленческое консультирование. 2015. № 8. С. 26–31.
2. *Коростелёв С. В.* К определению феномена терроризма: влияние наследия Нюрнбергского трибунала // Управленческое консультирование. 2018. № 5. С. 19–29.
3. *Талимончик В. П.* Обеспечение верховенства международного права в эпоху информационных технологий / Верховенство права на национальном и международном уровнях как приоритет деятельности ООН и суверенных государств: Материалы международной научно-практической конференции 6 сентября 2019 года / под ред. Е. М. Абайдельдинова, А. Х. Абашидзе, Р. К. Сарпекова, М. Ж. Куликпаевой. Нур-Султан, 2019. С. 206–217.
4. *Punday D.* The Narrative Construction of Cyberspace: Reading Neuromancer, Reading Cyberspace Debates. College English; Urbana. Vol. 63, 2. November 2000. P. 194–213.
5. *Li Cheng*. Cyberspace Reliabilities Revisit: New Challenges and Approaches. The College of William and Mary, ProQuest Dissertations Publishing, 2019. ProQuest Number: 13881565.
6. *Eric Talbot Jensen*. The Tallinn Manual 2.0: Highlights and Insights // Georgetown Journal of International Law. Vol. 48. 2017. P. 740–744.



***Об авторе:***

**Коростелев Станислав Валентинович**, Ответственный секретарь Объединенной комиссии при Межпарламентской Ассамблее государств — участников Содружества Независимых Государств по гармонизации законодательства в сфере безопасности и противодействия новым вызовам и угрозам, кандидат юридических наук, доцент; ksv1@iacis.ru


## References


1. Korostelev S. V. “Responsibility to Protect” as a political and legal justification for acts of use of force in international relations // Administrative consulting [Upravlencheskoe konsul’tirovanie]. 2015. N 8. P. 26–31. (In rus)
2. Korostelev S. V. To the definition of the phenomenon of terrorism: influence of the legacy of the Nuremberg Tribunal // Administrative consulting [Upravlencheskoe konsul’tirovanie]. 2018. N 5. P. 19–29. (In rus)
3. Talimonchik V. P. Ensuring the Rule of International Law in the Age of Information Technology / The Rule of Law at the National and International Levels as a Priority of the Activities of the UN and Sovereign States: Materials of the International Scientific and Practical Conference on September 6, 2019/ed. E. M. Abaideldinov, A. H. Abashidze, R. K. Sarpekov. Nur-Sultan, 2019. 712 p. P. 206–217. (In rus)
4. Punday D. The Narrative Construction of Cyberspace: Reading Neuromancer, Reading Cyberspace Debates. College English; Urbana. Vol. 63, 2. November 2000. P. 194–213.
5. Li Cheng. Cyberspace Reliabilities Revisit: New Challenges and Approaches. The College of William and Mary, ProQuest Dissertations Publishing, 2019. ProQuest Number: 13881565.
6. Eric Talbot Jensen. The Tallinn Manual 2.0: Highlights and Insights // Georgetown Journal of International Law. Vol. 48. 2017. P. 740–744.



***About the author:***

**Stanislav V. Korostelev**, Executive Secretary of the Joint Commission under the Interparliamentary Assembly of the Commonwealth of Independent States on Harmonization of Legislation in the Sphere of Security and Countering Emerging Threats and Challenges, PhD in Jurisprudence, Associate Professor; ksv1@iacis.ru