



Научная статья

УДК 34:004:342.3:004.9

EDN: <https://elibrary.ru/sywsrk>

DOI: <https://doi.org/10.21202/jdtl.2024.14>

Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств

Яссин Абдалла Абделькарим

Суд общей юрисдикции в Луксоре, Сохаг, Египет

Ключевые слова

государство,
граница,
кибербезопасность,
киберинтерес,
киберпространство,
киберсуверенитет,
национальный интерес,
право,
суверенитет,
цифровые технологии

Аннотация

Цель: обосновать существование национального киберсуверенитета как юридического понятия, наряду с которым путем введения инновационной детерминанты – концепции государственных киберинтересов – переосмыслить традиционные понятия национального суверенитета и государственных границ в условиях динамичной природы киберпространства и необходимости разработки гибридного механизма защиты киберграниц, основанного одновременно на праве и технологиях.

Методы: на основе доктринального метода выявлены принципиальные расхождения в представлениях ведущих ученых разной отраслевой принадлежности по концептуальным теоретико-методологическим и понятийно-категориальным вопросам, в том числе по вопросу обоснования единого алгоритма для установления границ в киберпространстве. Доктринальный метод дополнен анализом судебной практики разных стран, позволяющим рассмотреть распространение судами своей юрисдикции на споры, связанные с киберпространством.

Результаты: в исследовании представлено применение традиционных и современных правовых концепций суверенитета в новой, цифровой среде, результатом чего стало сочетание правовых и технологических подходов. Раскрыто функциональное значение концепции государственных киберинтересов для демаркации киберпространства и определения границ национального суверенитета. Показана адаптивность данной концепции к технически неопределенной природе киберпространства. Делается вывод об основных направлениях формирования концепции киберинтересов в киберпространстве, ее политических и правовых последствиях, основанных в том числе на практике судов разных стран по разрешению киберспоров.

© Абделькарим Я. А., 2024

Статья находится в открытом доступе и распространяется в соответствии с лицензией Creative Commons «Attribution» («Атрибуция») 4.0 Всемирная (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0/deed.ru>), позволяющей неограниченно использовать, распространять и воспроизводить материал при условии, что оригинальная работа упомянута с соблюдением правил цитирования.

Научная новизна: концепция государственных киберинтересов рассматривается в качестве инновационного метода определения киберграниц, что обуславливает трансформацию смысла традиционного понятия суверенитета и тесно связанного с ними понятия национальных интересов применительно к киберпространству в контексте обеспечения требований безопасности и активизации национальной защиты от киберугроз.

Практическая значимость: полученные результаты устраняют имеющиеся противоречия в определении суверенитета и его пространственных пределов в условиях развития современных технологий; способствуют выработке дисциплинарного стандарта киберсуверенитета на основе надежного демаркатора, необходимого для определения государственного суверенитета и границ в киберпространстве; адаптируют традиционные юридические понятия суверенитета и национальных интересов к глобальным современным кибервызовам; способствуют трансформации традиционных правовых институтов и норм в области суверенитета и границ в условиях киберпространства.

Для цитирования

Абделькарим, Я. А. (2024). Демаркация киберпространства: политико-правовые последствия применения концепции национальных интересов суверенных государств. *Journal of Digital Technologies and Law*, 2(2), 262–285. <https://doi.org/10.21202/jdtl.2024.14>

Содержание

Введение

1. Суверенитет и границы в киберпространстве: интегральное соответствие
 - 1.1. Эволюция границ и суверенитета в киберпространстве
 - 1.2. Тесная связь киберсуверенитета с национальными интересами
 - 1.3. Демаркация киберпространства: необходимость в детерминанте
2. Использование концепции государственных интересов для демаркации киберпространства
 - 2.1. Сущность концепции
 - 2.2. Политические и правовые последствия концепции государственных киберинтересов
 - 2.3. Судебные интерпретации концепции государственных киберинтересов
3. Пригодность концепции государственных интересов для демаркации киберпространства
 - 3.1. Основания пригодности
 - 3.2. Практические основы демаркации

Заключение

Список литературы

Введение

С появлением Интернета перед человечеством открылась безграничная сфера взаимодействия, которая распространяется на весь мир. Сегодня киберпространство связывает самые отдаленные уголки планеты. Это позволяет обмениваться разнонаправленными потоками данных между государствами, передавая разнообразную информацию и осуществляя международное кибервзаимодействие между людьми.

Безграничность киберпространства бросает вызов традиционным правовым нормам в области суверенитета и границ. Эти нормы необходимы для установления государственного контроля над национальной территорией с целью предотвращения экстерриториального ущерба, который могут нанести многочисленные незаконные кибердействия извне. Таким образом, требования безопасности предполагают переосмысление этих понятий в киберпространстве для активизации национальной защиты против киберугроз. Разрабатывая эти понятия в киберпространстве, ученые стремятся дать им четкое определение и разработать стандарты их проявления в киберпространстве. Однако отсутствие единой методологии порождает противоречия в определении суверенитета и границ в киберпространстве. В зависимости от сферы своей деятельности ученые расходятся в представлении требуемой детерминации.

Данное исследование призвано восполнить этот пробел путем введения новой детерминанты суверенитета и границ в киберпространстве. Этой детерминантой является понятие государственных киберинтересов. В работе отмечается, что национальные интересы в киберпространстве являются основной мотивацией для вмешательства государства; именно они побуждают государства действовать для защиты своих суверенных интересов.

Для достижения цели исследования в статье рассматривается соответствующая научная литература по проблемам суверенитета и границ в киберпространстве. Автор доказывает целостную взаимосвязь между этими понятиями и их тесную связь с идеей национальных интересов. Показано отсутствие дисциплинарного стандарта демаркации в киберпространстве; это практический пробел в знаниях, который данное исследование призвано восполнить. Затем автор объясняет концепцию государственных интересов, рассматривает ее последствия и использование судами разных стран при разрешении киберспоров. Наконец, в работе с помощью юридической аргументации доказана функциональность концепции государственных киберинтересов для установления границ в киберпространстве и предложены практические основы для ее реализации.

1. Суверенитет и границы в киберпространстве: интегральное соответствие

Суверенитет как политико-правовая концепция – это неоднозначное понятие, которое юристы и политики разрабатывают с XVI в. Это важнейший фактор организации межгосударственных отношений и всех взаимодействий на глобальном, общечеловеческом, уровне. Выдающиеся западные ученые, такие как Боден¹ и Гоббс²,

¹ Жан Боден (1530–1596), французский политический деятель и философ.

² Томас Гоббс (1588–1679), английский философ и историк.

представляли суверенитет как высшую власть короля принимать решения в пределах государства³. Согласно их взглядам, суверенитет – это политическая детерминанта государственной власти над территорией страны; ограничение национальной власти, которое налагает на государства фактическое обязательство взаимно уважать национальные суверенитеты друг друга. У Руссо эта политическая категория превратилась в понятие общественного договора⁴. Впоследствии философы и юристы разрабатывали различные теории суверенитета. Независимо от толкования понятия, суверенитет остается основным фактором, определяющим власть государства над своей территорией. Согласно Вестфальской доктрине, суверенитет означает верховную власть государства на своей территории (McLean & McMillan, 2009). Это традиционное определение суверенитета в юридических и политических науках, которое соответствует характеру межгосударственных взаимодействий в реальном мире. Таким образом, государства используют традиционные методы демаркации для установления государственных границ, регулирования полномочий и взаимодействий.

Однако появление киберпространства как современной сферы человеческих отношений и взаимодействий подразумевает распространение традиционных понятий на кибердеятельность. Этот факт потребовал от юристов и ученых переосмысления существующих понятий и теорий в контексте киберпространства. Таким образом, начала складываться концепция суверенитета в киберпространстве для организации государственной власти и отслеживания незаконной деятельности. Из-за очевидных различий между киберпространством и реальным миром необходимы значительные усилия со стороны ученых и законодателей для уточнения понятия суверенитета в условиях динамичной природы киберпространства. Этот процесс показал, что из-за особой природы киберпространства традиционные методы демаркации границ бесполезны. Необходимо разработать специальный инструментарий для установления киберграниц, определяющих государственный суверенитет в киберпространстве.

В первом разделе исследования мы опишем эволюцию научного знания в области концепций киберсуверенитета и киберграниц, а также изменения понятия суверенитета. Затем мы рассмотрим социальные и политические перспективы киберсуверенитета и его влияние на государственную и внутреннюю социальную политику, в частности, на законодательные аспекты этого явления. Наконец, мы проанализируем процесс демаркации в реальном мире и в киберпространстве и покажем проблемы в определении государственного суверенитета в киберпространстве.

1.1. Эволюция границ и суверенитета в киберпространстве

В 1983 г. благодаря изобретению протокола управления передачей данных (Transfer Control Protocol/Internet Protocol, TCP/IP) человечество обрело официальное открытое всемирное коммуникационное пространство – Интернет (ранее – онлайн-библиотека системы университетов штата Джорджия). С тех пор между пользователями Интернета – физическими, юридическими

³ Sovereignty. (2024, Mar. 12). Encyclopedia Britannica. <https://clck.ru/3A7Ttf>

⁴ Жан-Жак Руссо (1712–1778), французский философ.

лицами и правительствами – передаются огромные объемы данных. Развитие обмена данными требует анализа этой сферы взаимодействий с целью выявления ее особенностей.

Choucri и Clark (2013) отмечают, что в киберпространстве действительно отсутствует суверенитет; традиционное понятие суверенитета распространяется на киберпространство, но в такой форме, которая отвечает его безграничной природе. Подразумевается, что понятие суверенитета должно быть контекстуализировано в соответствии с технической сутью киберпространства. В этом решении проявляется попытка интегрировать юридическое понятие в технический контекст, чтобы преодолеть правовую неопределенность киберпространства.

Разработка понятия киберсуверенитета продолжилась, в результате чего была создана его строгая детерминанта. Исследователи сосредоточились на объяснении и уточнении того, как в киберпространстве проявляются границы. Границы являются логическим следствием суверенитета, поскольку они представляют собой его пределы. Понятия суверенитета и границ неразрывно связаны между собой; для определения суверенитета должны быть установлены и выверены границы. Эта логика распространяется и на киберпространство, поскольку точная интерпретация суверенитета требует разработки строгой детерминанты границ в киберпространстве.

Таким образом, началась научная разработка технических детерминант государственных границ в киберпространстве. Эти границы имеют те же признаки и функции, что и традиционные, поскольку позволяют государствам устанавливать свой суверенитет в киберпространстве. Соответственно, киберграницы были определены как «функциональный эквивалент границы, где данные поступают в первую реальную контрольную точку – сетевой маршрутизатор, компьютерный сервер, ПК или другие сетевые устройства» (Osborn, 2017). Это определение основано на моделях обмена данными, представленных в указанном исследовании. Как следствие, сотрудники государственных органов, например таможенники, могут наблюдать за потоком данных в киберпространстве, отслеживая нелегальные товары или облагая налогами другие киберматериалы, находящиеся в законном обороте. Значимость этого определения состоит в том, что для объяснения юридического понятия был использован чисто технический подход, что соответствует природе киберпространства. Osborn считал, что киберсуверенитет государства распространяется на первую точку, где поток данных затрагивает государственные интересы. Аналогичным образом Фанг при определении киберсуверенитета отдавал приоритет техническому аспекту, отмечая: «Суверенитет государства в киберпространстве основан на системах ИКТ (информационно-коммуникационные технологии), находящихся под юрисдикцией государства; его границами являются порты сетевых устройств государства, непосредственно подключенных к сетевым устройствам других государств; суверенитет киберпространства реализуется с целью защиты операций с данными посредством киберролей» (Fang, 2018). Автор соотносит кибертерриторию государства с сетью устройств в нем. Таким образом, карта всех устройств сети соответствует территории государства в киберпространстве. Кроме того, он отметил, что киберсуверенитет предоставляет государству те же полномочия в отношении своей территории, что и традиционный суверенитет, в частности возможности для обороны и сохранения независимости (Fang, 2018). Определение Фанга удачно сочетает в себе аспекты права и технологии, устанавливая государственную территорию в киберпространстве в соответствии с технической картой сетевых устройств и рассматривая права государства исходя из этой правовой концепции.

В связи с этим прокуратурой Египта был принят функциональный подход к вопросу о признании киберграниц. В официальном заявлении отмечается, что у государства есть виртуальные границы в киберпространстве; они составляют четвертую государственную границу на политической карте⁵. Таким образом, надзор в этой сфере представляет собой государственный интерес первостепенной важности. Хотя в заявлении не приводится определение киберграниц, их существование и функции признаны официально.

Широкое проникновение Интернета в современную жизнь сделало киберпространство неотъемлемой частью человеческих взаимоотношений и различного рода взаимодействий. Непрерывное развитие коммуникационных технологий в киберпространстве ставит под сомнение полномочия государств по регулированию деятельности в Интернете. Это побуждает ученых обратить пристальное внимание на правовые вопросы, возникающие при кибервзаимодействии. Аспекты государственного суверенитета и государственной власти над кибертерриторией занимают значительное место в научных дебатах. Кроме того, в рамках судебной практики был разработан ряд инструментов, позволяющих установить политические границы в киберпространстве.

Проблема киберсуверенитета не может ограничиваться физическим расположением сетевых устройств (Omar et al., 2022). Отсутствие традиционных границ в киберпространстве предполагает концептуализацию суверенитета с учетом технической неограниченности киберпространства. Поэтому в работе Omar с соавторами был введен термин «универсальный информационный суверенитет», обозначающий полномочия государства проводить операции по кибербезопасности для защиты своих национальных интересов в виртуальной реальности (Omar et al., 2022). Авторы показали, что определение границ государственного киберсуверенитета – это скорее политический, чем правовой процесс, поскольку каждое государство по-своему оценивает поток данных и его влияние на национальные интересы (Omar et al., 2022). Они осветили также практический аспект киберсуверенитета, выяснив его прямую связь с кибербезопасностью. Суверенитет – это легитимация операций по обеспечению кибербезопасности. Таким образом, это высшее проявление государственных интересов в киберпространстве.

Zekos отмечал, что глобальная природа Интернета переносит практику суверенитета с государств на рыночные силы, поскольку заменяет традиционную интерпретацию государственного суверенитета на понимание его как власти глобализованного рынка, обеспечивающей контроль капитала над киберпространством (Zekos, 2022). В связи с непрерывным ростом экономических выгод от глобализации киберпространства государства испытывают трудности с обеспечением своего традиционного суверенитета (Zekos, 2022). Таким образом, киберглобализация породила концепцию киберсуверенитета; это адаптация традиционного юридического понятия суверенитета в киберпространстве (Zekos, 2022). Следовательно, киберсуверенитет соответствует безграничности киберсферы, где традиционные территориальные границы полностью исчезают. Автор утверждает, однако, что государственный суверенитет в его правовой концепции тесно связан с территорией, поскольку это понятие позволяет государству устанавливать свою власть

⁵ The Egyptian Public Prosecution. (2020). Official Statement on Hanin Hossam's Case. <https://clck.ru/39rfJM>

в пределах национальных границ (Zekos, 2022). Соответственно, для установления суверенитета над государственной территорией в киберпространстве необходимо признание ее наличия. В условиях отсутствия традиционных территориальных границ автор предлагает для обеспечения государственного суверенитета применять современные методы географического цифрового отслеживания потоков данных в Интернете (Zekos, 2022). Кроме того, он приходит к выводу, что для признания своей территории в киберпространстве государствам следует использовать фактор эффекта (Zekos, 2022): любая деятельность, которая имеет какие-либо последствия на традиционной территории, устанавливает на ней государственный суверенитет. При таком толковании суды различных стран распространяют свою юрисдикцию на споры в киберпространстве. Распространение национального суверенитета на киберпространство оправдано связью между кибернетическим обществом и государством, независимо от отличий киберпространства (Zekos, 2022). Следовательно, государства могут установить свой суверенитет над электронными транзакциями и взаимодействиями, которые затрагивают их интересы. Это доказывает существование киберсуверенитета как юридического понятия.

По мнению Simmons и Hulvey, установление киберграниц облегчает организацию и управление потоками данных между национальными киберпространствами и универсальным киберпространством с помощью национальных законов (Simmons & Hulvey, 2023). Таким образом, киберграницы отражают стремление правительств защищать национальное киберпространство от иностранного вмешательства (Simmons & Hulvey, 2023). Поэтому границы и суверенитет – это две стороны одной медали, которая представляет собой национальную безопасность в киберпространстве.

Соблюдение киберсуверенитета – главный принцип киберопераций. Он является продолжением традиционного суверенитета, который представляет собой необходимое условие мирного сосуществования (Japaridze, 2023). Киберсуверенитет дает государствам право отслеживать незаконную деятельность в Интернете и принимать соответствующие контрмеры для сохранения своей национальной целостности в виртуальном пространстве (Japaridze, 2023). Таким образом, киберсуверенитет помогает защитить граждан от киберугроз. Однако крайние взгляды на киберсуверенитет могут привести к дроблению киберпространства до мельчайших областей (Japaridze, 2023), что противоречит первоначальному предназначению этой глобальной сферы. Поэтому суверенитет необходим в киберпространстве как определяющий фактор государственной власти для организации глобального взаимодействия.

Также стоит отметить точку зрения на киберсуверенитет как «подчинение киберпространства государственным интересам и ценностям» (Zein, 2022). Это определение говорит о наличии у государства высших полномочий по контролю и надзору за киберпространством и отражает очевидную связь между суверенитетом в киберпространстве и государственной властью. Оно также подразумевает усилия по демаркации киберпространства. Автор утверждает, что киберпространство де-факто является «универсальным всеобщим», подобно открытому морю и культурному наследию человечества (Zein, 2022). Поэтому сложно установить над ним суверенитет конкретной страны. Однако государства могут формировать свой национальный киберсуверенитет путем введения технических мер для ограничения потока данных, наблюдения за подозрительной деятельностью других государств и использования неопределенности киберпространства для противодействия этим явлениям (Zein, 2022). Кроме того, правовые последствия традиционного

суверенитета распространяются и на киберсуверенитет, поскольку государства должны обеспечивать взаимное уважение национального суверенитета при работе в киберпространстве, избегать незаконного вмешательства во внутренние дела других стран и поддерживать целостность территориального киберсуверенитета против незаконных кибератак, направленных на критическую инфраструктуру (Zein, 2022). Следует отметить, что автор подчеркивает тесную связь киберсуверенитета с безопасностью и благополучием страны, поэтому утверждает главенство политических мотивов над стремлением распространить суверенитет в его традиционной юридической интерпретации на новое инновационное киберпространство. В этом контексте А. Zhuk считает, что суверенитет в киберпространстве является чисто виртуальным и подразумевает установление государственного контроля над цифровой инфраструктурой, расположенной в пределах национальной виртуальной территории (Zhuk, 2023). Это исключительная особенность онлайн-сообществ, не имеющая связи с традиционной физической территорией.

Итак, поскольку суверенитет узаконивает действия государства по защите национальных интересов, ученые стремятся подробно описать, как эта концепция проявляется в киберпространстве. Если раньше спорили о самом существовании киберсуверенитета, то современная литература свидетельствует о его глобальном признании. Это признание проявляется в попытках интерпретировать данное понятие в техническом контексте киберпространства. Важно отметить, что при объяснении киберсуверенитета ученым удалось выделить его функциональные аспекты. Согласно определениям, суверенитет – это метод легитимизации действий государства в киберпространстве для представления своих национальных интересов. Более того, отсутствие четкого определения суверенитета может спровоцировать глобальный киберконфликт из-за пересечения полномочий между государствами. Это угрожает стабильности, необходимой для развития универсальных взаимодействий в киберпространстве. Поэтому разработка дисциплинарной детерминанты киберсуверенитета является обязательным условием для предотвращения возможных тяжелых последствий.

1.2. Тесная связь киберсуверенитета с национальными интересами

С момента своего появления в XVIII в. национальные интересы стали главным фактором, определяющим отношение государств к территориям. Государствам удавалось контролировать свои территории на основе понимания национальных интересов. Koulos утверждал, что страны, чтобы реализовать свои полномочия на определенной территории, начинают процесс ее национализации (Koulos, 2022). По мнению Сох, национальные интересы – это «совокупность убеждений, шаблонов и практик, ориентированных на народ, проживающий на ограниченной территории, и воплощенных в политических требованиях самоидентифицирующегося народа, которые могут быть или не быть реализованы в националистическом движении и самосознании» (Cox, 2021). Из этого определения можно понять, что национальные интересы некоторое время были ограничены традиционными территориальными пространствами. Однако появление Интернета устранило традиционные границы между государствами и позволило осуществлять транснациональное взаимодействие. Таким образом, национальные интересы стали завоевывать киберпространство, поскольку государства начали реализовывать планы по национализации киберпространства. В этом

аспекте необходимо изучить тесную связь между суверенитетом и национальными интересами в киберпространстве как рубеж, доказывающий необходимость демаркации киберсуверенитета государств и поиска детерминант киберграниц государств. Кроме того, необходимо исследовать некоторые государственные правила кибербезопасности, чтобы выявить отношение государства к демаркации киберпространства.

Понимание национальных интересов не препятствует применению этого понятия в реальном мире; в Интернете некоторые взаимодействия также мотивированы национальными интересами. Неограниченная универсальная природа киберпространства породила ряд областей цифрового соперничества, управляющим фактором которого являются национальные интересы. Поэтому, несмотря на двойственную природу киберпространства, государства стремились включить его в свои национальные концепции (Koulos, 2023). Иными словами, режимы разных стран пытались подчинить киберпространство своим политическим амбициям. Например, конечный адрес URL обычно указывает на государство, в котором находится владелец домена, например, .fr для Франции, .us для США и .eg для Египта. Koulos приводит этот пример в доказательство национализации киберпространства. Глобальное изменение ценностей привело к космополитическому пониманию национальных интересов (Cox, 2021). Глобализация пробудила политические амбиции стран на доминирование в киберпространстве. Отныне, указывает Сох, безграничная сфера Интернета разжигает бурную конкуренцию между странами под флагом национальных интересов (Cox, 2021). Более того, границы в киберпространстве формируются для защиты суверенитета на национальной территории. При этом для установления национальных киберграниц государства используют соответствующие методы. Эти механизмы отвечают специфической технической неопределенности киберпространства, что отличает их от традиционных методов демаркации границ. Интенсивная глобализация киберпространства заставляет государства концентрироваться на его территориализации, чтобы защитить свои национальные интересы от политической напряженности⁶. Национальные интересы являются главным оправданием их политики.

Поскольку киберпространство – это богатый источник информации, сверхдержавы стремятся установить над ним контроль, руководствуясь понятием киберсуверенитета⁷. Государства используют специальные технологии, чтобы укрепить контроль над национальной кибертерриторией. Они устанавливают национальный суверенитет в киберпространстве с помощью механизмов наблюдения и сбора данных, чтобы сохранить киберпревосходство для обеспечения целей экономики и безопасности (St-Hilaire, 2020). Государства могут осуществлять политическое давление на интернет-гигантов, чтобы использовать их технические возможности в политических конфликтах⁸.

⁶ Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. <https://clck.ru/3A7YMR>

⁷ Там же.

⁸ Blenkinsop, Ph. (2022, March 3). EU bars 7 Russian banks from SWIFT, but spares those in energy. Reuters. <https://clck.ru/3A7Yt8>

Более того, киберпространство стало значительным полем межгосударственного противостояния из-за разнообразных противоречивых интересов, на которые влияют потоки данных (Manshu & Chuanying, 2021). Если не урегулировать эти киберконфликты, они могут вызвать тяжелые политические последствия. На практике мы видим, что такие государства, как Китай и Россия, вкладывают огромные средства в технологии для установления своего суверенитета в киберпространстве, чтобы укрепить свою кибербезопасность против доминирования западных стран. Хотя их политика может привести к дроблению киберпространства, что противоречит принципу свободной передачи данных, эти государства ставят во главу угла свои национальные интересы (St-Hilaire, 2020). Именно национальные интересы выступают двигателем этой политики, что свидетельствует об их тесной связи с киберсуверенитетом. Ярким примером связи между киберсуверенитетом и национальными интересами является обещание Хиллари Клинтон ликвидировать цифровой железный занавес, установленный Китаем для контроля потока данных в Интернете (St-Hilaire, 2020). Это соревнование между странами за господство в киберпространстве мотивировано национальными интересами и направлено на обеспечение киберпревосходства страны. Кроме того, в США был создан Штаб киберопераций – рабочая группа для защиты национальных интересов США в киберпространстве от иностранных угроз⁹. После этого, в 2014 г., руководство Китая объявило об активизации работы по завоеванию господства в киберпространстве (Segal, 2014). Соревнования между странами за доминирование в киберпространстве представляют собой гонку вооружений между сверхдержавами за обладание этим важным ресурсом.

Следует отметить, что значимость киберпространства побуждает государства стремиться к доминированию в этой сфере. При этом они руководствуются идеями национального превосходства в киберпространстве. Этот факт подразумевает, что государства стремятся установить границы в киберпространстве для обеспечения национальных интересов и защиты суверенитета. Благодаря этому в киберпространстве представлена концепция национальных интересов, что доказывает ее тесную связь с понятием киберсуверенитета. Действительно, защита национальных киберграниц предполагает разработку механизма установления этих границ в киберпространстве.

1.3. Демаркация киберпространства: необходимость в детерминанте

Как следует из сказанного, судебная практика признает, что установление границ в киберпространстве необходимо для определения пределов национального суверенитета с целью предотвратить возможные конфронтации. Существование киберграниц является основой киберсуверенитета, что придает особую важность их демаркации. В реальном мире демаркация межгосударственных границ не является препятствием, поскольку государства используют традиционные инструменты, принятые и утвержденные международным правом. Более того, национальные интересы подразумевают установление четких государственных границ для обеспечения национальной обороны в киберпространстве. Однако из-за технически неоднозначной природы киберпространства процесс установления государственных границ существенно усложняется.

⁹ Command (2010), Our Mission and Vision. <https://clck.ru/3A7XsQ>

Общеизвестно, что территория государства является пространством его исключительной власти, которое ограничено признанными и четкими границами, представляющими собой государственные политические границы (Ahmed, 2021). Традиционно границы указывают на пределы, в которых государство может использовать свою власть. Таким образом, демаркация видимых границ между странами и территориями имеет решающее значение для стабильности и мирного сосуществования; она предотвращает незаконные вмешательства между государствами. Поскольку невозможно представить себе государство без территории, то и территория без границ существовать не может, так как целостность и признание территории зависят от установления ее очевидных и стабильных границ. На традиционных границах работают разрешительные правовые механизмы, обеспечивающие надзор за физическим перемещением людей и товаров, например, въездные и выездные визы, таможни, пограничные и береговые службы (Simmons & Hulvey, 2023).

Аналогичным образом, демаркация киберпространства занимает важное место в политике защиты государственных интересов. Страны имеют законное право устанавливать свой суверенитет против кибератак, направленных на национальную инфраструктуру. Кроме того, киберсуверенитет является одной из главных проблем уголовного правосудия, поскольку национальные судебные органы обязаны уважать суверенитет других стран при сборе доказательств в Интернете (Sallavaci, 2020). В целях сохранения киберсуверенитета трансграничное судопроизводство должно быть организовано на основе многосторонних или двусторонних договоров. Таким образом, ученые признают, что киберсуверенитет необходим для уголовного правосудия. Этот факт требует разработки соответствующего механизма установления границ в киберпространстве. Однако стремительная динамика киберпространства, обусловленная огромными потоками данных, затрудняет установление четких политических границ (Abdelrahman & Mekhiemer, 2022). В отличие от традиционных границ в киберпространстве ограничить территорию государства крайне сложно из-за отсутствия дисциплинирующей детерминанты. Следование традиционным межгосударственным границам стало нереалистичным из-за глобального характера киберпространства (Ahmed, 2021).

Чтобы маркировать свою кибертерриторию, государства используют традиционные метафоры для реагирования на иностранные киберугрозы (Simmons & Hulvey, 2023). Этот подход обусловлен территориальным мышлением государств в отношении киберпространства. Они рассматривают киберпространство как территорию, на которой можно доминировать и осуществлять суверенный контроль. Такие методы, как локализация данных, блокировка сайтов и судебные запросы о сотрудничестве, символизируют сочетание технологий и права для демаркации киберпространства. Это же отношение отражает определение киберграниц, данное Osborn. Однако опора на техническую составляющую для установления четких границ в киберпространстве может оказаться недостаточной из-за быстрого развития интернет-технологий, которое может столкнуться с медленным процессом внесения изменений в законодательство. Таким образом, становится актуальной разработка устойчивой детерминанты киберграниц. В данном исследовании представлена концепция государственных интересов как детерминанты киберграниц.

2. Использование концепции государственных интересов для демаркации киберпространства

2.1. Сущность концепции

Понятие «человеческий интерес» относится к потребностям, которые люди стремятся удовлетворить для своего благополучия. Эти потребности не являются чисто индивидуальными, они имеют социальные характеристики, обусловленные их вкладом в общественные отношения. Кроме того, они не являются абсолютными из-за ограничений производственных возможностей (Wang, 2022). Через свои основания интересы демонстрируют социальную трансформацию человеческих потребностей и тесную связь между людьми в определенном поле взаимодействий. Они являются детерминантами человеческих отношений, которые объединяют их в одних ситуациях и разделяют в других. Из-за разнообразия факторов интересы могут создавать противоречия между социальными группами, т. е. государствами (Wang, 2022). Интересы являются отправной точкой для создания политических, экономических и социальных связей внутри сообщества (Wang, 2022). Сох утверждал, что интересы стали главной осью общественных наук благодаря их вкладу в концепцию коллективных эмоций в сообществе (Cox, 2021). Таким образом, интересы – это эффективное выражение коллективной мотивации группы, которая побуждает государственную власть реагировать для их защиты.

Что касается государств, то их интересы как социальное явление означают национальные требования, которые удовлетворяют внутренние потребности в противовес интересам других государств. Поскольку страны могут различаться в установлении своих интересов, возникает конфликт интересов. Таким образом, интересы определяют, как ведут себя государства, чтобы обеспечить свои потребности. В приложении к киберпространству это означает, что каждое государство будет вести себя в Интернете так, чтобы удовлетворить свои национальные потребности; киберповедение государств будет соответствовать их интересам.

Государственные интересы – это общие интересы, поскольку они формируются на основе групповых потребностей (Wang, 2022). В киберпространстве понятие государственного интереса как общего интереса имеет следующие основные характеристики: публичность, реализация через цепочку поставок продукции, единство, включение фундаментальных ценностей и независимость (Wang, 2022). Это основные детерминанты государственных интересов как концепции.

2.2. Политические и правовые последствия концепции государственных киберинтересов

По мнению Fang, национальный суверенитет в киберпространстве – это политический интерес государства (Fang, 2018), и когда государство устанавливает свою власть над кибертерриторией, оно защищает национальные киберинтересы. Иными словами, установление политических границ в киберпространстве и утверждение национального суверенитета в их пределах отражает использование концепции государственных интересов для определения и поддержания киберграниц. Еще одним примером подчинения кибердипломатии государственным интересам является противоречие между США и Китаем. В то время как США борются за неограниченное киберпространство, поскольку достижение их национальных интересов требует

свободного потока данных, Китай стремится установить строгие киберграницы, чтобы защитить свою кибернезависимость (Fang, 2018). Этот пример подчеркивает критическое влияние концепции национальных интересов на киберполитику государств. Государство может ввести принудительную обработку данных, чтобы обеспечить легитимность обмена данными в пределах своих киберграниц и отслеживать незаконную кибердеятельность (Paice & McKeown, 2023). Такая практика способствует укреплению целостности национальной кибертерритории и реализации концепции киберсуверенитета. В этом выражается важнейшая роль концепции государственных интересов в обеспечении безопасности киберграниц. В частности, государственные интересы являются главной мотивацией в киберпространстве (Cox, 2021); когда киберинтересы страны оказываются под угрозой, вмешательство государства становится обязательным для защиты целостности национальных благ. Этот вывод соответствует сути суверенитета и национальных интересов в киберпространстве. Более того, угроза киберинтересам государств провоцирует кибервойну, которая включает в себя взаимные кибератаки через киберграницы для защиты своих экономических и военных объектов (Fang, 2018). Угрозы киберинтересам требуют срочной реакции государства, а противостояние им направлено на защиту национальных интересов.

В докладе Счетной палаты США от 2024 г. указывалось на острую необходимость разработки четких механизмов кибердипломатии для защиты государственных интересов в киберпространстве¹⁰. Тем самым правительство официально признало концепцию государственных киберинтересов и ее использование для планирования национальной дипломатии в киберпространстве. Таким образом, концепция государственных киберинтересов утвердилась в политике и дипломатии. Аналогичным образом ЕС использует совместную кибердипломатию, которая поддерживает совместные киберинтересы Евросоюза (Reiterer, 2022). Звучат призывы внедрять в ЕС самые передовые технологии для защиты киберинтересов Союза в условиях непрерывного развития конкурирующих кибердержав (Reiterer, 2022). Киберинтересы стали заметным элементом при разработке крупных национальных стратегий.

С юридической точки зрения общепризнано, что киберпространство – это виртуальная сфера глобальных взаимодействий, которая порождает реальные отношения между государствами. Кибервзаимодействие оказывает влияние на человеческие отношения в реальном мире. Этот факт вызывает необходимость регулирования киберпространства, обеспечивая правовые рамки для таких взаимодействий (Fang, 2018). Таким образом, государства внедряют свое законодательство в киберпространстве, чтобы защитить свои национальные интересы.

2.3. Судебные интерпретации концепции государственных киберинтересов

Контекстуализация концепции государственных киберинтересов представляет не только научный интерес. Изучение судебной практики, в том числе киберсудебных процессов, позволяет выяснить, как национальные судебные органы использовали эту концепцию для разрешения киберспоров.

¹⁰ US Government Accountability Office. (2024, January). Cyber Diplomacy. State's Efforts Aim to Support U.S. Interests and Elevate Priorities: Report to Congressional Addressees. <https://clck.ru/3A7Y99>

В деле *State v. Hunt* (2020) судебная система США занималась проблемой детской порнографии в Интернете. Важность решений по этому делу обусловлена угрозой эксплуатации несовершеннолетних. Так, по утверждению суда, в соответствии с 18 U.S.C. § 2252A, хранение порнографических материалов выражает преступное намерение обвиняемого просмотреть их. В решении отражено, что введение национального законодательства в киберпространстве стало следствием реализации государственных киберинтересов, а именно искоренения детской порнографии в Интернете. Аналогичным образом, в деле *People v. Jacobo* (2019) суд применил определение онлайн-торговли людьми и разрешение на преследование по составу этого преступления, установленное Законом штата Калифорния против сексуальной эксплуатации (*Californians Against Sexual Exploitation Act, CASE*) от 2012 г. таким образом, чтобы правоохранительные органы могли преследовать эту деятельность, если в нее вовлечен гражданин США. Это очевидное расширение киберграниц США, поскольку этого требуют государственные интересы. В деле *Democratic Nat'l Comm. v. Russian Fed'n* (2019) американский суд также встал на защиту целостности избирательного режима от зарубежных кибератак, которые угрожали демократической системе США. Кроме того, судебное разбирательство может быть возбуждено в экономических киберинтересах государства, как в деле *Regina v Cory Aguilar* (2018); суд Великобритании счел, что вред, нанесенный истцу мошеннической деятельностью ответчика в Интернете, достаточен для признания его виновным и заключения в тюрьму. Дело *Regina v Stephen Brownlee* (2020) было посвящено противодействию контрабанде через Интернет. Судебные органы Великобритании одобрили преследование неназванных веб-сайтов, которые использовались контрабандистами в качестве платформ для обмена нелегальными товарами. Эти сайты были признаны точками нарушения государственных границ и приговорены к уничтожению для защиты национальных интересов.

В делах *Lifestyle Equities CV v Amazon UK Services Ltd.* (2021) и *Tunein Inc v Warner Music UK Limited, Sony Music Entertainment UK Limited* (2021) судебные органы Великобритании встали на защиту творческой сферы своей страны, противостоя незаконной онлайн-торговле нелегальными материалами и произведениями искусства. Несомненно, такие материалы наносят моральный и финансовый ущерб владельцам авторских прав, защита которых представляет собой важнейший государственный интерес в соответствии с Законом Великобритании об авторском праве, промышленных образцах и патентах от 1988 г.

Американский судья О'Сканлиан в деле *Robins v. Spokeo* (2017) счел, что неверный отчет о бизнесе в Интернете нарушает Закон США об объективной кредитной отчетности (*US Fair Credit Reporting Act*), давая истцу право на компенсацию. Аналогичным образом суд Великобритании признал то же право в деле *Ghannouchi v Middle East Online Ltd & Anor.* Таким образом, суд борется с распространением неверной информации на веб-сайтах и защищает достоверность национальных СМИ.

В заключение отметим, что, согласно рассмотренным решениям, судебные органы признают существование концепции киберграниц и связывают ее с концепцией государственных интересов. Такая функциональная интерпретация означает, что государственные киберграницы устанавливаются в соответствии с государственными интересами в киберпространстве; если имеется интерес, то государство может расширять свой киберсуверенитет для его защиты. Однако судебные решения не содержат нормативного определения киберграниц; защищаемые интересы – это государственные киберграницы в соответствии с функциональной интерпретацией, которая согласуется с определением Osborn (2017) и Zein (2022).

3. Пригодность концепции государственных интересов для демаркации киберпространства

3.1. Основания пригодности

Нет нужды говорить о том, что в киберпространстве до сих пор нет четкого определения концепции границ. Государства используют различные механизмы для защиты своих национальных интересов. Разнообразие внутренней киберполитики противоречит универсальности киберпространства, стабильность которого требует единых норм. Отсутствие многосторонних конвенций о демаркации киберпространства, конкуренция политических киберинтересов, разнообразие национальных интерпретаций правовых понятий, проблемы установления авторства и ответственности в киберпространстве – вот главные препятствия на пути принятия концепции глобальной детерминанты киберграниц¹¹. В связи с отсутствием механизма правовой демаркации мы вводим понятие государственного интереса как необходимой детерминанты.

В качестве глобального всеобщего киберпространство требует введения общепризнанного стандарта для определения политических границ. Следует помнить, что чисто техническая природа киберпространства не препятствует контекстуализации правовых понятий в этой сфере. Традиционная концепция суверенитета распространяется на киберпространство, но в форме, соответствующей его технической природе (Choucri & Clark, 2013). Сочетание права и технологии стало основной проблемой, которая стояла перед учеными, пытавшимися разработать нормы для демаркации киберпространства. Эта проблема, как было показано ранее, побудила Osborn использовать чисто технический подход к определению киберграниц. Однако развитие науки дает нам возможность увязать концепции границ и суверенитета в киберпространстве с концепцией государственных интересов.

Ключом к успешной интеграции правового понятия в цифровую среду является адаптивность (Akhmatova & Akhmatova, 2020). Это вызов, который стоит перед легализацией киберпространства и управлением им. Адаптивность концепции государственных интересов к технически неопределенной природе киберпространства очевидна. Поскольку киберпространство удовлетворяет самые разные человеческие потребности, концепция интересов формируется через методы, принятые государствами для удовлетворения этих потребностей. Как указывает Wang (2022), интересы – это истинное выражение социальной жизни сообществ; они являются двигателем социальных взаимодействий между людьми. Поэтому они должны быть приоритетом при установлении границ между группами. Таким образом, концепция государственных интересов в киберпространстве эволюционирует, достигая пределов государственной киберполитики. Адаптивность ее компонентов к кибервзаимодействию позволяет использовать эту концепцию в качестве детерминанты государственной власти в киберпространстве.

¹¹ Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. <https://clck.ru/3A7ZPU>

Кроме того, главными мотивами вмешательства государств в киберпространство являются национальные интересы. Изучение китайского и западного подходов демонстрирует их поспешные попытки сформировать свой киберсуверенитет в соответствии с национальными интересами, которые они стремятся защищать в киберпространстве. В частности, четкое присутствие национальных интересов в киберпространстве побуждает государства использовать свои внутренние правовые инструменты для защиты своих киберинтересов. Согласно анализу Benabid¹² и Раисе и McKeown (2023), интересы государств являются активными двигателями национальной политики в киберпространстве. Эти факты доказывают приоритетность государственных киберинтересов на национальном уровне, что находит отражение в реализации этой концепции на политической арене.

С точки зрения судебной практики, решения национальных судов по киберспорам позволяют квалифицировать концепцию государственных интересов для определения киберграниц. Судебные органы США и Великобритании распространили свою юрисдикцию на киберпространство в тех случаях, когда существует угроза национальным интересам. Поскольку юрисдикция отражает суверенитет, национальные суды устанавливают национальный суверенитет в той степени, в которой затрагиваются государственные интересы. В этой интерпретации концепция государственных интересов используется в качестве детерминанты киберсуверенитета государства и, как следствие, его киберграниц.

3.2. Практические основы демаркации

После создания правовой основы для использования концепции государственных киберинтересов для определения киберграниц необходимо разработать практическую базу для этого процесса. В статье представлено несколько методов использования этой концепции в качестве детерминанты границ.

Ввиду универсальности киберпространства предлагается через использование конвенций и других механизмов развивать обычное международное право, поддерживая адаптивность правовых понятий к технической природе киберпространства¹³. При этом государства должны вступать в соглашения о принятии концепции государственных интересов для установления киберграниц. Регулирование киберпространства требует универсальных механизмов, поскольку односторонняя политика может поставить под угрозу глобальные усилия по регулированию. Кроме того, многосторонние договоренности обеспечивают международный консенсус в отношении принятия государственных киберинтересов для демаркации киберпространства. Как следствие, концепция государственных киберинтересов приобретет дисциплинарный характер, что повысит ее вклад в управление киберпространством.

¹² Benabid, M. (2022, August). The Territorialization of Cyberspace and GAFAM Geopolitics: Driving Forces and New Risks in the Wake of the Ukrainian Crisis. Policy Brief. № 52/22. <https://clck.ru/3A7YMR>

¹³ Hollis, D. B. (2021, June). A Brief Primer on International Law and Cyberspace. Carnegie Endowment for International Peace. <https://clck.ru/3A7ZPU>

Ключом к преодолению технико-юридических дилемм должны стать инновации (Linden & Shirazi, 2023). Ученым необходимо углублять традиционное понимание правовых понятий, адаптируя их к техническим контекстам, таким как киберпространство. Кроме того, инновации являются основой современных киберопераций, поскольку они предоставляют государствам выгодные возможности в киберпространстве (Soare, 2023). Что касается судебной сферы, то в попытке преодолеть техническую природу киберспоров суды разных стран используют технические инструменты наряду с традиционными правовыми понятиями. Этот уникальный механизм защиты киберграниц основан одновременно на праве и технологиях. Такая гибридная структура обеспечивает этому механизму гибкость, позволяющую адаптировать правовые концепции к техническому киберпространству. Кроме того, гибкость повышает возможности национальных судов противостоять киберугрозам. Инновации – это ключ, который позволяет судам преодолеть технические трудности киберспоров и застой в законодательстве, объединив право и технологии.

Стремительные, скачкообразные изменения дискурса предполагают преодоление препятствий за счет выхода за пределы существующей реальности. Опора исключительно на реалистичные логические рассуждения при разрешении технико-правовой дилеммы ставит юристов в тупик. В этом случае важнейший вклад в развитие правовой доктрины вносит воображение. В правовом аспекте именно воображение предоставляет ученым впечатляющие, убедительные и инновационные возможности для преодоления традиционных трудностей (d'Aspremont, 2022). Правовое воображение представляет собой мощный инструмент против юридической бюрократии; это «мышление о невозможном ради преодоления» (d'Aspremont, 2022). Кроме того, воображение, с точки зрения права, расширяет возможности юристов по переосмыслению существующих норм в гибких технологических средах, где изменения происходят быстро и неупорядоченно (Pollicino, 2020). Таким образом, воображение юриста позволяет изменять традиционные правовые понятия в соответствии с быстро развивающимися техническими сферами, такими как киберпространство. Следует отметить, что концепции границ и суверенитета также родились когда-то в воображении, а затем успешно интерпретированы и включены в реалистичные правовые контексты с помощью инновационных технико-правовых принципов, заложенных в эти решения и интерпретации. Аналогичным образом, концепция государственных киберинтересов, благодаря правовому воображению, может быть эффективно контекстуализирована в киберпространстве для установления границ и суверенитета. В вышеупомянутых судебных решениях эта концепция использовалась для определения объема национальной юрисдикции, что прямо подразумевает государственный суверенитет в пределах национальных границ. Следовательно, можно сделать вывод, что государственные киберграницы распространяются на каждую точку киберпространства, где затрагиваются государственные интересы. Такая интерпретация отражает гибкость концепции государственных интересов, соответствуя неопределенной природе киберпространства, где технически сложно соблюсти жесткие нормы. Таким образом, воображение позволяет воссоздать традиционные правовые понятия в киберпространстве, наделив их эффективным свойством адаптации к киберпространству – гибкостью.

Заключение

Суммируя вышесказанное, следует отметить, что киберпространство оказалось неспособным противостоять установлению границ с помощью традиционных методов демаркации, принятых для обозначения границ в реальном мире. Попытки ученых описать суверенитет и границы в киберпространстве с разных точек зрения породили противоречивое понимание этих понятий. Указанные противоречия дестабилизируют универсальные отношения в киберсфере. Для преодоления этой дилеммы нами предпринята попытка разработать современный правовой механизм определения суверенитета и границ в киберпространстве.

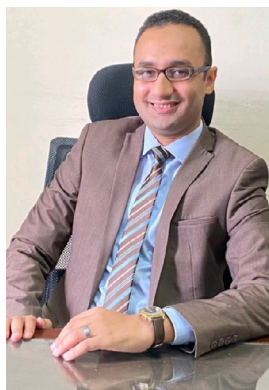
В отличие от других научных работ в данном исследовании для определения технического понятия используется чисто юридическая концепция. В качестве инструмента демаркации киберпространства в нем представлена концепция государственных киберинтересов. Эта концепция подразумевает установление связи между национальным суверенитетом в киберпространстве и любым воздействием на национальные интересы. Что касается функциональности концепции государственных интересов, в исследовании показана ее адаптируемость к технической природе киберпространства, что позволяет преодолеть традиционные препятствия на пути интеграции юридического понятия в техническую среду. Кроме того, в работе предложены механизмы, обеспечивающие применимость данной гипотезы.

Список литературы

- Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, 16(15), 423–443. (In Arabic). <https://doi.org/10.21608/jocu.2022.134235.1172>
- Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, 2(6), 632–646. (In Arabic).
- Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, 5, 6. <https://doi.org/10.1186/s41018-020-00076-2>
- Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, 69(5), 21–31. <https://doi.org/10.1177/0096340213501370>
- Cox, L. (2021). *Nationalism: Themes, Theories, and Controversies*. Palgrave Macmillan. <https://doi.org/10.1007/978-981-15-9320-8>
- d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, 35(4), 1017–1027. <https://doi.org/10.1017/s0922156521000637>
- Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. <https://doi.org/10.1007/978-981-13-0320-3>
- Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13
- Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, 1, 119. <https://doi.org/10.12688/openreseurope.14010.2>
- Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, 9, 22. <https://doi.org/10.1186/s40854-022-00432-8>
- Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, 3, 97–114. <https://doi.org/10.1007/s42533-021-00079-7>
- McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. <https://doi.org/10.1093/acref/9780199207800.001.0001>
- Omar, M. O., AlDajani, I. M., Juwaihian, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

- Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.
- Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity*, Springer, Singapore. https://doi.org/10.1007/978-981-19-6414-5_1
- Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online*. Edward Elgar Publishing. <https://doi.org/10.4337/9781788976688.00009>
- Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacific. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action*. New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2
- Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1
- Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.
- Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship*, 3158.
- Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. <https://doi.org/10.4324/9781003284093-6>
- St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. <https://doi.org/10.1007/978-3-030-61386-0>
- Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. <https://doi.org/10.1007/978-981-19-3963-1>
- Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, 3(3), 679–738. <https://doi.org/10.21608/ijdl.2022.138565.1159> (In Arabic).
- Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. <https://doi.org/10.1007/978-3-030-94736-1>
- Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, 2, 45. <https://doi.org/10.1007/s44206-023-00067-x>

Сведения об авторе



Абделькарим Яссин Абдалла – судья, суд общей юрисдикции в Луксоре, Министерство юстиции Египта

Адрес: 82516, Египет, г. Сохаг, Мадинат Нассер, ул. Ахмим Сохаг, Нью Касалови Хотел

E-mail: yassinabdelkarim91@gmail.com

ORCID ID: <https://orcid.org/0000-0001-7388-1337>

Конфликт интересов

Автор сообщает об отсутствии конфликта интересов.

Финансирование

Исследование не имело спонсорской поддержки

Тематические рубрики

Рубрика OECD: 5.05 / Law

Рубрика ASJC: 3308 / Law

Рубрика WoS: OM / Law

Рубрика ГРНТИ: 10.15.41 / Государственный суверенитет

Специальность ВАК: 5.1.5 / Международно-правовые науки

История статьи

Дата поступления – 21 сентября 2023 г.

Дата одобрения после рецензирования – 12 октября 2023 г.

Дата принятия к опубликованию – 25 июня 2024 г.

Дата онлайн-размещения – 30 июня 2024 г.



Research article

UDC 34:004:342.3:004.9

EDN: <https://elibrary.ru/sywsrk>

DOI: <https://doi.org/10.21202/jdtl.2024.14>

Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests

Yassin Abdalla Abdelkarim

Luxor Elementary Court, Sohag, Egypt

Keywords

border,
cyber interest,
cyber security,
cyber sovereignty,
cyberspace,
digital technologies,
law,
national interest,
sovereignty,
state

Abstract

Objective: to substantiate the existence of national cyber sovereignty as a legal concept; by introducing the concept of state cyber interests as an innovative determinant, to review the traditional concepts of national sovereignty and state borders in the context of the dynamic nature of cyberspace and the need to develop a hybrid mechanism for cyber borders protection, based simultaneously on law and technology.

Methods: the doctrinal method was used to identify the basic discrepancies in the views of leading scientists in different fields on fundamental theoretical-methodological, conceptual and categorical issues, including the justification of a single algorithm for establishing borders in cyberspace. The doctrinal method is supplemented by the analysis of judicial practice of different countries, which allows considering the courts extending their jurisdiction to disputes related to cyberspace.

Results: the study presents the application of traditional and modern legal concepts of sovereignty in the new digital environment, resulting in a combination of legal and technological approaches. The author reveals functional significance of the concept of state cyber interests for demarcating cyberspace and defining the boundaries of national sovereignty. The adaptability of this concept to the technically uncertain nature of cyberspace is shown. The conclusion is made about the main directions in forming the concept of cyber interests in cyberspace and its political and legal implications, based, among other things, on the practice of courts of different countries in resolving cyber disputes.

© Abdelkarim Y. A., 2024

This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (CC BY 4.0) (<https://creativecommons.org/licenses/by/4.0>), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

Scientific novelty: the concept of state cyber interests is considered as an innovative method of defining cyber borders. It leads to the transformation of the traditional sovereignty concept and the close national interest concept in relation to cyberspace in the context of fulfilling security requirements and intensifying national defense against cyber threats.

Practical significance: the obtained results eliminate existing contradictions in the definition of sovereignty and its spatial limits under the modern technology development; contribute to the elaboration of a disciplinary standard of cyber sovereignty based on a reliable demarcator necessary for the definition of state sovereignty and borders in cyberspace; adapt traditional legal concepts of sovereignty and national interests to the global modern cyber challenges; contribute to the transformation of traditional legal concepts of sovereignty and national interests in cyberspace.

For citation

Abdelkarim, Y. A. (2024). Demarcation of Cyberspace: Political and Legal Effects of Applying the Concept of Sovereign States' Interests. *Journal of Digital Technologies and Law*, 2(2), 376–399. <https://doi.org/10.21202/jdtl.2024.20>

References

- Abdelrahman, M. A., & Mekhiemer, O. F. (2022). Cyberspace and its Impact on the Concepts of Power, Security and Conflict in International Relations. *Journal of Politics and Economy*, 16(15), 423–443. (In Arabic). <https://doi.org/10.21608/jocu.2022.134235.1172>
- Ahmed, B. S. (2021). The Role of the International Court of Justice in Resolving International Borders Disputes. *Humanitarian and Natural Sciences Journal*, 2(6), 632–646. (In Arabic).
- Akhmatova, D., & Akhmatova, M. (2020). Promoting Digital Humanitarian Action in Protecting Human Rights: Hope or Hype. *Journal of International Humanitarian Action*, 5, 6. <https://doi.org/10.1186/s41018-020-00076-2>
- Choucri, N., & Clark, D. D. (2013). Who Controls Cyberspace? *Bulletin of the Atomic Scientists*, 69(5), 21–31. <https://doi.org/10.1177/0096340213501370>
- Cox, L. (2021). *Nationalism: Themes, Theories, and Controversies*. Palgrave Macmillan. <https://doi.org/10.1007/978-981-15-9320-8>
- d'Aspremont, J. (2022). Legal imagination and the thinking of the impossible. *Leiden Journal of International Law*, 35(4), 1017–1027. <https://doi.org/10.1017/s0922156521000637>
- Fang, B. (2018). *Cyberspace Sovereignty: Reflections on Building a Community of Common Future in Cyberspace*. Science Press and Springer Nature Singapore Pte Ltd. <https://doi.org/10.1007/978-981-13-0320-3>
- Japaridze, T. (2023). Cyber Sovereignty: Should Cyber Borders Replicate Territorial Borders? In J. Berghofer, A. Futter, C. Häusler, M. Hoell, & J. Nosál (Eds.), *The Implications of Emerging Technologies in the Euro-Atlantic Space* (pp. 209–225). Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-24673-9_13
- Koulos, Th. (2022). A Digital Territory to be Appropriated: The State and the Nationalization of Cyberspace [version 2; peer review: 2 approved]. *Open Research Europe*, 1, 119. <https://doi.org/10.12688/openreseurope.14010.2>
- Linden, T., & Shirazi, T. (2023). Markets in Crypto-assets Regulation: Does it Provide Legal Certainty and Increase Adoption of Crypto-assets? *Financial Innovation*, 9, 22. <https://doi.org/10.1186/s40854-022-00432-8>
- Manshu, Xu, & Chuanying, Lu (2021). China – U.S. Cyber-Crisis Management. *China International Strategy Review*, 3, 97–114. <https://doi.org/10.1007/s42533-021-00079-7>
- McLean, I., & McMillan, A. (2009). *The Concise Oxford Dictionary of Politics* (3 ed.). Oxford University Press. <https://doi.org/10.1093/acref/9780199207800.001.0001>
- Omar, M. O., AlDajani, I. M., Juwaih, M., & Leiner, M. (2022). Cybersecurity in Sovereignty Reform. In I. M. AlDajani, & M. Leiner (Eds.), *Reconciliation, Heritage and Social Inclusion in the Middle East and North Africa* (pp. 109–128). Springer, Cham. https://doi.org/10.1007/978-3-031-08713-4_8

- Osborn, Ph. (2017, October). Cyber Border Security – Defining and Defending a National Cyber Border. *Homeland Security Affairs* 13, Article 5.
- Paice, A., & McKeown, S. (2023). Practical Cyber Threat Intelligence in the UK Energy Sector. In C. Onwubiko et al. (Eds.), *Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media, Springer Proceedings in Complexity*, Springer, Singapore. https://doi.org/10.1007/978-981-19-6414-5_1
- Pollicino, O. (2020). Metaphors and Judicial Frame: Why Legal Imagination (also) Matters in the Protection of Fundamental Rights in the Digital Age. In B. Petkova, & T. Ojanen (Eds.), *Fundamental Rights Protection Online*. Edward Elgar Publishing. <https://doi.org/10.4337/9781788976688.00009>
- Reiterer, M. (2022). EU Cyber Diplomacy: Value- and Interest-Driven Foreign Policy with New Focus on the Indo-Pacific. In G. Boulet, M. Reiterer, & R. P. Pardo (Eds.). *Cybersecurity Policy in the EU and South Korea from Consultation to Action*. New Security Challenges. Palgrave Macmillan, Cham. https://doi.org/10.1007/978-3-031-08384-6_2
- Sallavaci, O. (2020). Rethinking Criminal Justice in Cyberspace: The EU E-evidence Framework as a New Model of Cross-Border Cooperation in Criminal Matters. In H. Jahankhani, B. Akhgar, P. Cochrane, & M. Dastbaz (Eds.), *Policing in the Era of AI and Smart Societies, Advanced Sciences and Technologies for Security Applications* (pp 1–58). Springer, Cham. https://doi.org/10.1007/978-3-030-50613-1_1
- Segal, A. (2017, June 2). *Chinese Cyber Diplomacy in a New Era of Uncertainty*. Hoover Working Group on National Security, Technology, and Law. Aegis Paper Series, 1703.
- Simmons, B., & Hulvey, R. (2023). Cyber Borders: Exercising State Sovereignty Online. *All Faculty Scholarship*, 3158.
- Soare, S. R. (2023). Algorithmic power? The Role of Artificial Intelligence in European Strategic Autonomy. In F. Christiano, D. Broeders, F. Delerue, F. Douzet, & A. Géry (Eds.). *Artificial Intelligence and International Conflict in Cyberspace*, Routledge, London. <https://doi.org/10.4324/9781003284093-6>
- St-Hilaire, W. A. (2020). *Digital Risk Governance: Security Strategies for the Public and Private Sectors*. Springer Nature Switzerland. <https://doi.org/10.1007/978-3-030-61386-0>
- Wang, P. (2022). *Principle of Interest Politics: Logic of Political Life from China's Perspective*. Peking University Press. Springer. <https://doi.org/10.1007/978-981-19-3963-1>
- Zein, M. (2022), The Effect of the New State Sovereignty Concepts on the Jurisdictions of Cybercrime. *International Journal of Doctrine, Judiciary, and Legislation*, 3(3), 679–738. <https://doi.org/10.21608/ijdl.2022.138565.1159> (In Arabic).
- Zekos, G. I. (2022). *Political, Economic and Legal Effects of Artificial Intelligence: Governance, Digital Economy and Society*. Springer Nature Switzerland. <https://doi.org/10.1007/978-3-030-94736-1>
- Zhuk, A. (2023), Virtual Sovereignty: Examining the Legal Status of Micronations in Cyberspace Through the Case of the Republic of Errant Menda Lerenda. *Digital Society*, 2, 45. <https://doi.org/10.1007/s44206-023-00067-x>

Author information



Yassin Abdalla Abdelkarim – Judge, Luxor Elementary Court, Egyptian Ministry of Justice

Address: New Casalovy Hotel Street, Akhmim Sohag Street, Madinat Nasser, 82516, Sohag, Egypt

E-mail: yassinabdelkarim91@gmail.com

ORCID ID: <https://orcid.org/0000-0001-7388-1337>

Conflicts of interest

The author declares no conflict of interest.

Financial disclosure

The research had no sponsorship.

Thematic rubrics

OECD: 5.05 / Law

PASJC: 3308 / Law

WoS: OM / Law

Article history

Date of receipt – September 21, 2023

Date of approval – October 12, 2023

Date of acceptance – June 25, 2024

Date of online placement – June 30, 2024